aws

Panduan Pengguna

Amazon Elastic Compute Cloud

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Elastic Compute Cloud: Panduan Pengguna

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan kekayaan masing-masing pemiliknya, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau mungkin tidak.

Table of Contents

Apa itu Amazon EC2? 1
Fitur 1
Layanan terkait 2
Mengakses EC2 4
Harga 5
Estimasi, penagihan, dan optimalisasi biaya 6
Sumber daya 7
Mulai tutorial 8
Langkah 1: Luncurkan instans 10
Langkah 2: Hubungkan ke instans Anda 12
Langkah 3: Bersihkan instans Anda 15
Langkah selanjutnya 16
Praktik terbaik 17
Amazon Machine Image 20
Karakteristik AMI 22
Izin peluncuran 22
Tipe volume root 23
Identifikasi tipe volume root AMI 24
Tipe virtualisasi 26
Temukan AMI 28
Parameter Systems Manager 31
Parameter publik Systems Manager 35
Dibayar AMIs di AWS Marketplace 37
Jual AMI Anda di AWS Marketplace 39
Mencari AMI berbayar 39
Membeli AMI berbayar 41
Ambil kode produk 42
Menggunakan dukungan berbayar 43
Tagihan untuk dibayar dan didukung AMIs 44
Mengelola langganan Anda 44
Siklus hidup AMI 45
Membuat AMI 47
Buat AMI yang didukung Amazon S3 56
Buat AMI menggunakan Windows Sysprep 96

Menyalin AMI 114
Menyimpan dan memulihkan AMI 132
Nenek moyang AMI 142
Penggunaan AMI 148
Usangkan AMI 172
Menonaktifkan AMI 178
Membatalkan pendaftaran AMI 184
Mode boot 191
Persyaratan untuk mode boot UEFI 192
Parameter mode boot AMI 194
Mode boot tipe instans 196
Mode boot instans 199
Mode boot sistem operasi 200
Mengatur mode boot AMI 202
Variabel UEFI 209
UEFI Secure Boot 210
Enkripsi AMI 227
Skenario peluncuran instans 227
Skenario penyalinan gambar 231
Berbagi AMIs 233
Penyedia AMI terverifikasi 234
Temukan bersama AMIs 235
Bersiaplah untuk menggunakan shared AMIs untuk Linux 238
Diizinkan AMIs 239
Jadikan AMI Anda Publik 259
Blokir akses publik untuk AMIs 263
Bagikan AMI dengan organisasi dan unit organisasi 273
Bagikan AMI dengan AWS akun tertentu 285
Membatalkan berbagi AMI dengan akun Anda 289
Rekomendasi untuk membuat Linux bersama AMIs 291
Memantau peristiwa AMI 297
Detail peristiwa 298
Peristiwa available 299
Peristiwa failed 299
Peristiwa deregistered 300
Peristiwa disabled 301

Memahami penagihan AMI 301
Bidang penagihan AMI 302
Mencari informasi penagihan AMI 304
Memverifikasi biaya AMI pada tagihan Anda 306
Kuota AMI 307
Minta kenaikan kuota untuk AMIs 308
Instans 310
Tipe instans 311
Tipe instans yang tersedia 312
Spesifikasi perangkat keras 313
Jenis hypervisor 313
Tipe virtualisasi AMI 314
Prosesor 314
Menemukan tipe instans 317
Pencari jenis instans EC2 325
Rekomendasi Compute Optimizer 327
Perubahan jenis instans 330
Instance performa yang dapat melonjak 339
Instans GPU 393
Instans Mac 408
Optimisasi EBS 459
Opsi CPU 562
AMD SEV-SNP 812
Kontrol status prosesor 820
Instans terkelola 824
Penagihan untuk instans terkelola 824
Identifikasi instance terkelola 825
Memulai instans terkelola 827
Virtualisasi bersarang 827
Cara kerjanya 827
Pertimbangan-pertimbangan 828
Luncurkan instance baru dengan virtualisasi bersarang diaktifkan 828
Konfigurasikan instance yang ada untuk menggunakan virtualisasi bersarang 829
Opsi penagihan dan pembelian 831
Instans Sesuai Permintaan 832
Instans Terpesan 835

Instans Spot 905
Host Khusus 1009
Instans Khusus 1072
Reservasi Kapasitas 1079
Templat peluncuran 1227
Pembatasan 1228
Izin 1229
Kontrol instans peluncuran 1236
Buat 1239
Modifikasi (kelola versi) 1255
Delete 1259
Luncurkan sebuah instans 1262
Tutorial 1265
Referensi parameter instance 1289
Luncurkan menggunakan wizard peluncuran instans 1304
Meluncurkan menggunakan templat peluncuran 1307
Luncurkan dari instance yang ada 1314
Peluncuran dari AWS Marketplace AMI 1316
Terhubung ke instans Anda. 1318
Prasyarat koneksi umum 1320
Hubungkan ke instans Linux Anda, menggunakan SSH. 1326
Hubungkan ke instans Windows Anda menggunakan RDP 1342
Terhubung menggunakan Session Manager 1353
Connect menggunakan IP publik dan EC2 Instance Connect 1354
Connect menggunakan IP pribadi dan EC2 Instance Connect Endpoint 1391
Perubahan status instans 1425
Penagihan berdasarkan status instans 1426
Contoh yang tertunda 1428
Contoh yang dihentikan 1428
Contoh hibernasi 1429
Mem-boot ulang instance 1429
Instance yang dihentikan 1430
Perbedaan antara status instance 1430
Berhenti dan mulai 1433
Hibernasi 1453
Boot ulang 1483

Mengakhiri ... 1485
Pensiun ... 1503
Pemulihan instans otomatis ... 1508
Konsep kunci pemulihan instans otomatis ... 1510
Perbedaan antara pemulihan otomatis yang disederhanakan dan pemulihan berbasis CloudWatch tindakan ... 1512
Membangun sistem yang tangguh ... 1513
Verifikasi apakah pemulihan otomatis terjadi ... 1513
Pemulihan otomatis yang disederhanakan ... 1515
CloudWatch pemulihan berbasis tindakan ... 1520
Metadata instans ... 1524
Kategori metadata instans ... 1526
Kategori data dinamis ... 1541
Akses metadata contoh ... 1542
Konfigurasikan opsi IMDS ... 1584
Menjalankan perintah saat peluncuran ... 1622
Contoh: Nilai indeks peluncuran AMI ... 1648
Mendeteksi apakah host adalah sebuah EC2 instance ... 1653
Memeriksa dokumen identitas instans ... 1653
Periksa sistem UUID ... 1653
Periksa pengenal pembuatan mesin virtual sistem ... 1655
Dokumen identitas instans ... 1660
Ambil dokumen identitas instance ... 1662
Verifikasi dokumen identitas instance ... 1664
Sertifikat publik ... 1675
Kepatuhan STIG ... 1736
Pengaturan STIG ... 1737
Unduh skrip STIG ... 1757
Terapkan pengaturan STIG dengan Systems Manager ... 1778
Sinkronisasi jam ... 1782
Stempel waktu paket perangkat keras ... 1782
Detik kabisat ... 1783
Gunakan Layanan Sinkronisasi Waktu Amazon lokal ... 1784
Gunakan Layanan Sinkronisasi Waktu Amazon publik ... 1797
Bandingkan stempel waktu untuk instans Linux Anda ... 1799
Ubah zona waktu instans Anda ... 1801

Manajer Kapasitas EC2 1803
Fitur Utama 1804
Mengaktifkan Manajer Kapasitas 1804
Mengatur data Anda 1817
Menavigasi Manajer Kapasitas di konsol 1825
Mengekspor data Anda 1828
Kelola driver perangkat 1832
Driver jaringan 1832
Driver grafis 1832
Driver perangkat penyimpanan 1833
Driver AMD 1833
Driver NVIDIA 1839
Instal driver ENA di Windows 1886
Driver Windows PV 1907
AWS NVMe driver 1943
Konfigurasikan instance Windows 1955
Pengaturan sistem khusus Windows 1955
AWS driver perangkat untuk instance Windows 1956
Agen peluncuran Windows 1957
Peluncuran Cepat EC2 untuk Windows 2119
Ubah kata sandi Administrator Windows 2144
Tambahkan komponen Sistem Windows 2145
Instal WSL di Windows 2150
Utilitas Windows 2152
Mutakhirkan instans Windows 2154
Lakukan pemutakhiran langsung 2155
Lakukan pemutakhiran otomatis 2160
Migrasi ke tipe instans berbasis Nitro 2171
Memecahkan masalah pemutakhiran 2180
Tutorial: Hubungkan instans EC2 ke database RDS 2181
Tujuan Tutorial 2181
Konteks 2181
Arsitektur 2182
Pertimbangan-pertimbangan 2183
Waktu untuk menyelesaikan tutorial 2184
Biaya 2184

Opsi 1: Terhubung secara otomatis menggunakan konsol EC2 2185
Opsi 2: Terhubung secara otomatis menggunakan konsol RDS 2197
Opsi 3: Hubungkan secara manual 2209
Armada 2219
Fitur dan manfaat 2219
Metode armada mana yang digunakan? 2220
Opsi konfigurasi 2222
Tipe permintaan 2223
Batas pengeluaran 2253
Pemilihan tipe instans berbasis atribut 2255
Pembobotan instans 2292
Strategi alokasi 2295
Penyeimbangan Ulang Kapasitas 2303
Reservasi Kapasitas 2309
Bekerja dengan Armada EC2 2310
Status permintaan Armada EC2 2311
Prasyarat Armada EC2 2312
Membuat Armada EC2 2317
Menandai Armada EC2 2326
Jelaskan Armada EC2 2328
Memodifikasi Armada EC2 2333
Hapus Armada EC2 2335
Bekerja dengan Armada Spot 2340
Status permintaan Armada Spot 2341
Izin Armada Spot 2342
Membuat Armada Spot 2353
Menandai Armada Spot 2362
Jelaskan Armada Spot 2372
Memodifikasi permintaan Armada Spot 2373
Membatalkan (menghapus) permintaan Armada Spot 2375
Penskalaan otomatis untuk Armada Spot 2378
Pantau armada Anda 2389
Pantau armada Anda menggunakan CloudWatch 2390
Pantau armada Anda menggunakan EventBridge 2393
Tutorial 2411
Tutorial: Konfigurasikan Armada EC2 untuk menggunakan pembobotan instance 2414

Tutorial: Konfigurasikan Armada EC2 untuk menggunakan Instans Sesuai Permintaan sebagai kapasitas utama ... 2418
Tutorial: Konfigurasikan Armada EC2 untuk meluncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas yang ditargetkan ... 2419
Tutorial: Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Blok Kapasitas 2426
Tutorial: Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Reservasi Kapasitas yang Dapat Diinterupsi ... 2429
Contoh konfigurasi CLI untuk Armada EC2 ... 2434
Contoh 1: Meluncurkan Instans Spot sebagai opsi pembelian default ... 2435
Contoh 2: Meluncurkan Instans Sesuai Permintaan sebagai opsi pembelian default ... 2435
Contoh 3: Meluncurkan Instans Sesuai Permintaan sebagai kapasitas primer ... 2436
Contoh 4: Luncurkan Instans Sesuai Permintaan menggunakan beberapa Reservasi Kapasitas ... 2436
Contoh 5: Luncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas ketika total kapasitas target melebihi jumlah Reservasi Kapasitas yang tidak digunakan ... 2440
Contoh 6: Luncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas yang ditargetkan ... 2444
Contoh 7: Konfigurasikan Penyeimbangan Kembali Kapasitas untuk meluncurkan Instans Spot pengganti ... 2448
Contoh 8: Luncurkan Instans Spot dalam armada yang dioptimalkan kapasitas ... 2450
Contoh 9: Luncurkan Instans Spot dalam armada yang dioptimalkan kapasitas dengan prioritas ... 2451
Contoh 10: Luncurkan Instans Spot di armada price-capacity-optimized ... 2452
Contoh 11: Konfigurasikan pemilihan tipe instans berbasis atribut ... 2454
Contoh konfigurasi CLI Spot Fleet ... 2455
Contoh 1: Availability Zone dengan harga terendah ... 2456
Contoh 2: Availability Zone dengan harga terendah dari daftar ... 2457
Contoh 3: Jenis instans dengan harga terendah dari daftar ... 2459
Contoh 4. Menimpa harga untuk permintaan ... 2460
Contoh 5: Gunakan strategi alokasi yang terdiversifikasi ... 2462
Contoh 6: Gunakan pembobotan contoh ... 2465
Contoh 7: Gunakan kapasitas On-Demand ... 2467
Contoh 8: Konfigurasikan Penyeimbangan Kembali Kapasitas ... 2468
Contoh 9: Gunakan armada yang dioptimalkan kapasitas ... 2469
Contoh 10: Gunakan armada yang dioptimalkan kapasitas dengan prioritas ... 2470
Contoh 11: Gunakan priceCapacityOptimized armada ... 2472

Contoh 12: Mengonfigurasi pemilihan tipe instans berbasis atribut 2473
Kuota armada 2474
Meminta peningkatan kuota untuk kapasitas target 2475
Jaringan 2477
Wilayah dan Zona 2478
Wilayah 2479
Zona Ketersediaan 2479
Zona Lokal 2481
Wavelength Zones 2482
AWS Outposts 2483
Pengalamatan IP instans 2485
IPv4 Alamat pribadi 2486
IPv4 Alamat publik 2487
Optimalisasi IPv4 alamat publik 2489
IPv6 alamat 2491
Beberapa alamat IP 2492
Nama host instans EC2 2493
Alamat link-lokal 2493
IPv4 alamat 2494
IPv6 alamat 2500
Alamat IP sekunder 2506
IPv4 alamat pada Windows 2510
Nama host dan domain instans EC2 2517
Memahami nama host dan domain instans EC2 2518
Jenis nama host 2518
Bawa alamat IP Anda sendiri 2533
Definisi BYOIP 2534
Persyaratan dan kuota 2535
Ketersediaan wilayah 2536
Ketersediaan Local Zone 2536
Prasyarat 2538
Di atas jangkauan alamat Anda 2547
Gunakan rentang alamat Anda 2556
Alamat IP elastis 2557
Harga alamat IP Elastis 2558
Dasar alamat IP Elastis 2558

Kuota alamat IP Elastis 2559
Kaitkan sebuah alamat IP Elastis 2560
Transfer alamat IP Elastis 2565
Merilis alamat IP Elastis 2571
Menggunakan DNS terbalik untuk aplikasi email 2572
Antarmuka jaringan 2576
Konsep antarmuka jaringan 2578
Kartu jaringan 2580
Alamat IP per antarmuka jaringan 2583
Membuat antarmuka jaringan 2585
Lampiran antarmuka jaringan 2591
Mengelola alamat IP 2595
Memodifikasi atribut antarmuka jaringan 2599
Beberapa antarmuka jaringan 2603
Antarmuka jaringan yang dikelola pemohon 2607
Delegasi awalan 2609
Menghapus antarmuka jaringan 2619
Bandwith jaringan 2620
Bandwidth instans yang tersedia 2621
Pembobotan bandwidth 2624
Memantau bandwidth instans 2656
Jaringan yang ditingkatkan 2657
Adaptor Jaringan Elastis (ENA) 2658
ENA Ekspres 2729
Intel 82599 VF 2761
Pantau kinerja jaringan 2774
Meningkatkan latensi jaringan di Linux 2786
Pertimbangan kinerja nitro 2790
Optimalkan kinerja jaringan pada Windows 2798
Elastic Fabric Adapter 2800
Dasar-dasar EFA 2801
Antarmuka dan pustaka yang didukung 2804
Tipe instans yang didukung 2804
Sistem operasi yang didukung 2818
Batasan EFA 2819
Harga EFA 2820

Memulai dengan EFA dan MPI 2820
Memulai dengan EFA dan NCCL 2838
Memulai dengan EFA dan NIXL 2860
Maksimalkan bandwidth jaringan 2881
Buat dan lampirkan EFA 2896
Lepaskan dan hapus EFA 2901
Memantau EFA 2902
Verifikasi penginstal EFA 2910
Catatan rilis 2923
Topologi EC2 2945
Cara kerjanya 2947
Prasyarat 2954
Contoh 2956
Grup penempatan 2972
Strategi penempatan 2973
Buat grup penempatan 2979
Ubah penempatan instance 2981
Menghapus grup penempatan 2982
Grup penempatan bersama 2983
Grup penempatan di AWS Outposts 2986
MTU Network 2987
Frame jumbo (9001 MTU) 2988
Path MTU Discovery 2989
Mengatur MTU untuk instans Anda 2990
Pemecahan Masalah 2996
Virtual private cloud 2997
Default Anda VPCs 2997
Tidak default VPCs 2998
Akses internet 2999
Subnet bersama 2999
IPv6-hanya subnet 3000
Jaringan Sekunder 3000
Apa itu Jaringan Sekunder? 3001
Konsep utama 3001
Arsitektur 3002
Pertimbangan tambahan 3002

Memulai ... 3002
Mengelola sumber daya Jaringan Sekunder ... 3004
Praktik terbaik desain jaringan ... 3005
Pemecahan masalah ... 3006
Kuota dan batas ... 3007
Keamanan ... 3008
Perlindungan data ... 3009
Keamanan data Amazon EBS ... 3010
Enkripsi saat tidak aktif ... 3011
Enkripsi saat bergerak ... 3012
Keamanan infrastruktur ... 3014
Isolasi jaringan ... 3014
Isolasi pada host fisik ... 3015
Mengontrol lalu lintas jaringan ... 3015
Ketahanan ... 3018
Validasi kepatuhan ... 3019
Manajemen identitas dan akses ... 3019
Kebijakan berbasis identitas ... 3020
Contoh kebijakan untuk API ... 3032
Kebijakan contoh untuk konsol ... 3078
AWS kebijakan terkelola ... 3092
Peran IAM ... 3101
Manajemen pembaruan ... 3114
Praktik terbaik untuk instans Windows ... 3115
Praktik terbaik keamanan tingkat tinggi ... 3115
Manajemen pembaruan ... 3116
Manajemen konfigurasi ... 3118
Manajemen perubahan ... 3119
Audit dan akuntabilitas untuk instans Windows Amazon EC2 ... 3120
Pasangan kunci ... 3121
Membuat pasangan kunci ... 3122
Jelaskan pasangan kunci Anda ... 3130
Menghapus pasangan kunci Anda ... 3135
Menambahkan atau mengganti kunci publik pada instance Linux Anda ... 3136
Verifikasi sidik jari ... 3138
Grup keamanan ... 3140

Ikhtisar ... 3141
Membuat grup keamanan ... 3142
Ubah grup keamanan untuk instans Anda ... 3145
Menghapus grup keamanan ... 3151
Pelacakan koneksi ... 3153
Aturan-aturan grup keamanan untuk kasus penggunaan yang berbeda ... 3159
NitroTPM ... 3166
Persyaratan ... 3167
Aktifkan AMI Linux untuk NitroTPM ... 3169
Verifikasi bahwa AMI diaktifkan untuk NitroTPM ... 3170
Aktifkan atau hentikan penggunaan NitroTPM ... 3172
Verifikasi bahwa instance diaktifkan untuk NitRotPM ... 3173
Ambil kunci dukungan publik ... 3174
Pengesahan instans EC2 ... 3176
Integrasi dengan AWS KMS ... 3178
Membuktikan lingkungan komputasi yang terisolasi ... 3179
AWS model tanggung jawab bersama ... 3179
Dapat dibuktikan AMIs ... 3179
Bersiaplah AWS KMS untuk pengesahan ... 3189
Dapatkan Dokumen Pengesahan NitroTPM ... 3190
Integrasi dengan AWS KMS ... 3198
Mengisolasi data dari operator Anda sendiri ... 3199
Credential Guard untuk instance Windows ... 3200
Prasyarat ... 3201
Luncurkan instance yang didukung ... 3201
Nonaktifkan integritas memori ... 3203
Aktifkan Credential Guard ... 3203
Verifikasi bahwa Credential Guard sedang berjalan ... 3205
AWS PrivateLink ... 3206
Membuat titik akhir VPC antarmuka ... 3207
Membuat kebijakan titik akhir ... 3207
Penyimpanan ... 3209
AWS Harga penyimpanan ... 3210
Amazon EBS ... 3210
Batas volume EBS ... 3211
Kartu EBS ... 3215

Penyimpanan instans Amazon EC2 3216
Persistensi data 3218
Batas volume penyimpanan instans 3220
Volume penyimpanan instans SSD 3224
Menambahkan volume penyimpanan instans 3229
Aktifkan volume swap untuk instans M1 dan C1 3236
Inisialisasi volume penyimpanan instance 3240
Statistik kinerja rinci volume penyimpanan instans 3241
Volume akar 3245
Instans dengan volume root Amazon EBS 3246
Instance dengan volume root penyimpanan instance (hanya instance Linux) 3248
Pertahankan volume root setelah penghentian instance 3249
Mengganti volume root 3253
Nama perangkat untuk volume 3264
Nama perangkat yang tersedia 3264
Pertimbangan nama perangkat 3267
Pemetaan perangkat blok 3269
Konsep pemetaan perangkat blok 3269
Tambahkan pemetaan perangkat blok ke AMI 3274
Tambahkan pemetaan perangkat blok ke instance 3278
Bagaimana volume dilampirkan dan dipetakan untuk instance Windows 3287
Peta disk NVME ke volume 3288
Petakan disk non-NVMe ke volume 3293
Pencegahan tumpang tindih 3303
Ukuran blok yang didukung 3304
Persyaratan 3305
Periksa dukungan instance 3306
Konfigurasikan beban kerja 3307
Cuplikan Windows VSS EBS 3309
Apa itu VSS? 3310
Cara kerja solusi snapshot Amazon EBS berbasis VSS 3311
Prasyarat VSS 3312
Membuat snapshot VSS 3325
Memecahkan masalah snapshot VSS 3335
Pulihkan opsi untuk solusi AWS VSS 3340
Riwayat versi 3341

Penyimpanan objek, penyimpanan file, dan caching file 3346
Amazon S3 3346
Amazon EFS 3349
Amazon FSx 3353
Cache File Amazon 3358
Kelola sumber daya 3359
Pilih Wilayah untuk sumber daya Anda 3359
Temukan sumber daya Anda 3361
Langkah-langkah konsol 3361
Contoh baris perintah 3370
Tampilan Global (lintas Wilayah) 3374
AWS Tampilan Global 3374
Tandai sumber daya Anda 3378
Dasar-dasar tag 3379
Tandai sumber daya Anda 3380
Pembatasan tanda 3381
Manajemen tanda dan akses 3382
Menandai sumber daya Anda untuk penagihan 3382
Tandai izin sumber daya 3383
Menambahkan dan menghapus tag 3387
Filter sumber daya berdasarkan tag 3391
Lihat tag menggunakan metadata contoh 3393
Kuota layanan 3399
Melihat kuota Anda saat ini 3399
Meminta peningkatan 3400
Pembatasan pada email yang dikirim menggunakan port 25 3401
Pantau sumber daya 3402
Memantau status instans Anda 3403
Pemeriksaan status 3404
Peristiwa perubahan status 3413
Peristiwa terjadwal 3415
Pantau instans Anda menggunakan CloudWatch 3454
Alarm contoh 3455
Kelola pemantauan terperinci 3457
CloudWatch metrik 3460
Instal dan konfigurasikan CloudWatch agen 3480

Statistik untuk metrik 3484
Lihat grafik pemantauan 3494
Membuat alarm 3495
Buat alarm yang menghentikan, mengakhiri, melakukan boot ulang, atau memulihkan instans 3496
Otomatisasi menggunakan EventBridge 3509
Jenis EC2 acara Amazon 3509
Log panggilan API menggunakan CloudTrail 3510
Acara manajemen EC2 API Amazon di CloudTrail 3512
Contoh acara Amazon EC2 API 3512
Koneksi audit dibuat menggunakan EC2 Instance Connect 3513
Pantau aplikasi.NET dan SQL Server 3515
Melacak penggunaan Tingkat Gratis Anda 3516
Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025 3516
Lacak penggunaan Tingkat Gratis untuk akun yang dibuat sebelum 15 Juli 2025 3518
Laporan penagihan dan penggunaan 3520
Contoh 3521
Instans bare metal 3522
Host Khusus 3522
Instans Khusus 3522
Optimisasi EBS 3523
Reservasi Kapasitas 3523
Inventarisasi EC2 instans Anda 3523
Lokasi geografis 3525
Spesifikasi perangkat keras 3526
Citra 3527
Alamat IP dan nama host DNS 3529
Aturan-aturan grup keamanan 3530
Data pengguna 3532
Sumber daya terkait 3533
Pemecahan Masalah 3534
Masalah peluncuran instans 3534
Nama perangkat tidak valid 3535
Batas instans terlampaui 3536
Kapasitas instans tidak cukup 3536

Konfigurasi yang diminta saat ini tidak didukung. Periksa dokumentasi untuk konfigurasi yang didukung. 3537
Instans langsung terhenti 3537
Izin tidak cukup 3539
Penggunaan CPU yang tinggi segera setelah Windows dimulai (hanya instance Windows) 3540
Meluncurkan instance IMDSv1 -enabled gagal 3541
Masalah berhenti contoh 3542
Paksa menghentikan sebuah instance 3543
(Opsional) Buat instance pengganti 3545
Masalah penghentian instans 3547
Instans langsung terhenti 3548
Penghentian instans yang tertunda 3548
Instans yang dihentikan masih ditampilkan 3550
Kesalahan: Instans mungkin tidak dihentikan. Memodifikasi atribut instance disableApiTermination " 3550
Instans diluncurkan atau dihentikan secara otomatis 3551
Contoh yang tidak dapat dijangkau 3551
Boot ulang instans 3551
Output konsol instans 3552
Mengambil tangkapan layar instans yang tidak dapat dijangkau 3553
Tangkapan layar umum untuk instance Windows 3554
Pemulihan instans saat komputer host gagal 3564
Instance muncul offline dan secara tak terduga di-boot ulang 3564
Masalah SSH contoh Linux 3565
Penyebab umum masalah koneksi 3566
Kesalahan saat menghubungkan instans Anda: Waktu koneksi habis 3568
Kesalahan: tidak dapat memuat kunci ... Mengharapkan: KUNCI PRIVAT APA PUN 3571
Kesalahan: Kunci pengguna tidak dikenali oleh server 3572
Kesalahan: Izin ditolak atau koneksi ditutup oleh [instans] port 22 3574
Kesalahan: File kunci privat yang tidak dilindungi 3576
Kesalahan: Kunci privat harus dimulai dengan “-----BEGIN RSA PRIVATE KEY-----” dan diakhiri dengan “-----END RSA PRIVATE KEY-----” 3578
Kesalahan: Verifikasi kunci host gagal 3578
Kesalahan: Server menolak kunci kami atau Tidak tersedia metode autentikasi yang didukung 3579
Tidak dapat melakukan ping pada instans 3580

Kesalahan: Server menutup koneksi jaringan secara tidak terduga 3580
Kesalahan: Validasi kunci host gagal untuk EC2 Instance Connect 3581
Tidak dapat terhubung ke instans Ubuntu menggunakan EC2 Instance Connect 3583
Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance saya? 3583
Pemeriksaan status gagal instance Linux 3590
Meninjau informasi pemeriksaan status 3591
Mengambil log sistem 3592
Memecahkan masalah kesalahan log sistem untuk instance Linux 3593
Kehabisan memori: hentikan proses 3594
KESALAHAN: mmu_update gagal (Pembaruan manajemen memori gagal) 3595
Kesalahan I/O (kegagalan perangkat blok) 3596
KESALAHAN I/O: bukan disk lokal maupun jarak jauh (Perangkat blok terdistribusi yang rusak) 3598
request_module: modprobe loop runaway (Melakukan loop modprobe kernel warisan pada versi Linux yang lebih lawas) 3599
“FATAL: kernel terlalu lawas” dan “fsck: Tidak ada file atau direktori tersebut saat mencoba membuka /dev” (Kernel dan AMI tidak cocok) 3600
“FATAL: Tidak dapat memuat /lib/modules" atau "BusyBox" (Modul kernel tidak ada) 3601
KESALAHAN Kernel tidak valid (kernel tidak kompatibel dengan EC2) 3603
fsck: Tidak ada file atau direktori tersebut saat mencoba membuka... (Sistem file tidak ditemukan) 3604
Kesalahan umum saat memasang sistem file (kegagalan pemasangan) 3606
VFS: Tidak dapat memasang fs root pada blok yang tidak diketahui (Sistem file root tidak cocok) 3609
Kesalahan: Tidak dapat menentukan major/minor jumlah perangkat root... (system/device Ketidakcocokan file root) 3610
XENBUS: Perangkat tanpa driver... 3611
... hari tanpa diperiksa, pemeriksaan paksa (Diperlukan pemeriksaan sistem file) 3613
fsck mati dengan status keluar... (Perangkat tidak ada) 3613
Perintah GRUB (grubdom>) 3615
Memunculkan eth0 antarmuka: eth0 perangkat memiliki alamat MAC yang berbeda dari yang diharapkan, mengabaikan. (Alamat MAC dengan hard-coding) 3618
Tidak dapat memuat SELinux Kebijakan. Mesin berada dalam mode pemberlakuan. Berhenti sekarang. (SELinux salah konfigurasi) 3619
XENBUS: Waktu menghubungkan ke perangkat habis (waktu habis Xenbus) 3621
Instans Linux melakukan booting dari volume yang salah 3622

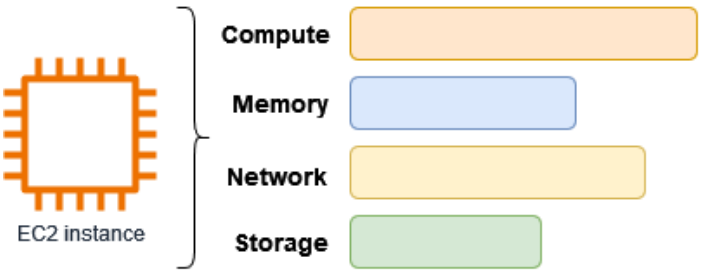
Masalah RDP contoh Windows 3624
Desktop Jarak Jauh tidak dapat terhubung ke komputer jarak jauh 3624
Kesalahan menggunakan klien RDP macOS 3626
RDP menampilkan layar hitam, bukan desktop 3626
Tidak dapat masuk dari jarak jauh ke sebuah instans dengan pengguna yang bukan administrator 3627
Memecahkan masalah Remote Desktop menggunakan AWS Systems Manager 3627
Aktifkan Desktop Jarak Jauh pada instans EC2 dengan registri jarak jauh 3631
Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance Windows? 3632
Masalah mulai instance Windows 3633
“Kata sandi tidak tersedia” 3633
“Kata sandi belum tersedia” 3634
“Tidak dapat mengambil kata sandi Windows” 3635
“Menunggu layanan metadata” 3635
“Tidak dapat mengaktifkan Windows” 3639
“Windows tidak asli (0x80070005)” 3641
“Tidak ada Server Lisensi Server Terminal yang tersedia untuk memberikan lisensi” 3642
“Beberapa pengaturan dikelola oleh organisasi Anda” 3642
Masalah instance Windows 3643
Tidak dapat menghubungkan AWS Systems Manager Sessions Manager ke instans Windows Server 2025 3643
Volume EBS tidak diinisialisasi di Windows Server 2016 dan 2019 3644
Lakukan boot instans Windows EC2 ke Directory Service Restore Mode (DSRM) 3645
Instans kehilangan konektivitas jaringan atau tugas terjadwal tidak berjalan saat diharapkan 3648
Tidak bisa mendapatkan output konsol 3649
Windows Server 2012 R2 tidak tersedia di jaringan 3649
Tabrakan tanda tangan disk 3649
Setel ulang kata sandi administrator Windows 3651
Setel ulang kata sandi menggunakan EC2 Launch v2 3652
Setel ulang kata sandi menggunakan EC2 Peluncuran 3657
Setel ulang kata sandi menggunakan EC2 Config 3663
Memecahkan masalah Sysprep 3669
EC2Penyelamatan untuk instance Linux 3671
Instal EC2 Rescue 3671
Jalankan perintah EC2 Penyelamatan 3676

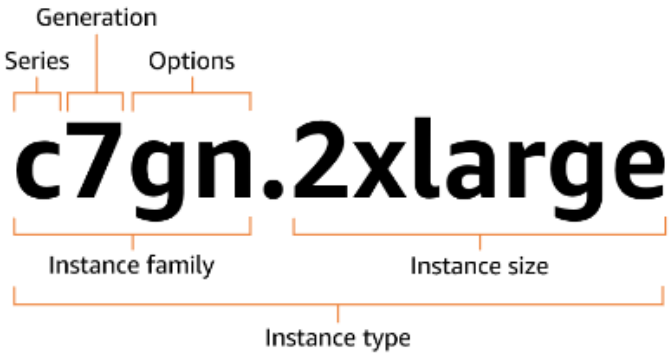
Kembangkan modul EC2 Penyelamatan 3678
EC2Rescue untuk instance Windows 3686
Memecahkan masalah menggunakan EC2 Rescue GUI 3687
Memecahkan masalah menggunakan EC2 Rescue CLI 3693
Memecahkan masalah menggunakan EC2 Rescue and Systems Manager 3702
Konsol Serial EC2 3706
Prasyarat 3706
Konfigurasikan akses ke Konsol Serial EC2 3714
Hubungkan ke Konsol Serial EC2 3724
Memutuskan koneksi dari Konsol Serial EC2 3734
Memecahkan masalah instans Anda menggunakan Konsol Serial EC2 3735
Kirim interupsi diagnostik 3744
Tipe instans yang didukung 3745
Prasyarat 3745
Kirimkan interupsi diagnostik 3748
Riwayat dokumen 3749
Sejarah untuk 2018 dan sebelumnya 3791
..... mmmdcccxviii

Apa itu Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) menyediakan kapasitas komputasi yang sesuai permintaan dan dapat diskalakan di Amazon Web Services (AWS) Cloud. Menggunakan Amazon EC2 akan mengurangi biaya perangkat keras sehingga Anda dapat mengembangkan dan melakukan deployment aplikasi lebih cepat. Anda dapat menggunakan Amazon EC2 untuk meluncurkan server virtual sebanyak atau sesedikit yang Anda butuhkan, mengonfigurasi keamanan dan jaringan, serta mengelola penyimpanan. Anda dapat menambahkan kapasitas (menaikkan skala) untuk menangani tugas-tugas berat komputasi, seperti proses bulanan atau tahunan, atau lonjakan lalu lintas situs web. Ketika penggunaan berkurang, Anda dapat mengurangi kapasitas (menurunkan skala) lagi.

Instans EC2 adalah server virtual di AWS Cloud. Saat Anda meluncurkan instans EC2, jenis instans yang Anda tentukan menentukan perangkat keras yang tersedia untuk instans Anda. Setiap jenis instans menawarkan keseimbangan sumber daya komputasi, memori, jaringan, dan penyimpanan yang berbeda. Untuk informasi selengkapnya, lihat Panduan Jenis Instans Amazon EC2.





Fitur-fitur Amazon EC2

Amazon EC2 menyediakan fitur-fitur tingkat tinggi berikut ini:

Instans

Server virtual.

Gambar Mesin Amazon (AMIs)

Templat yang telah dikonfigurasi untuk instans Anda yang mengemas komponen yang Anda butuhkan untuk server Anda (termasuk sistem operasi dan perangkat lunak tambahan).

Tipe instans

Berbagai konfigurasi CPU, memori, penyimpanan, kapasitas jaringan, dan perangkat keras grafis untuk instans Anda.

Volume Amazon EBS

Volume penyimpanan persisten untuk data Anda menggunakan Amazon Elastic Block Store (Amazon EBS).

Volume penyimpanan instans

Volume penyimpanan untuk data sementara yang dihapus saat Anda menghentikan, hibernasi, atau mengakhiri instans Anda.

Pasangan kunci

Amankan informasi login untuk instans Anda. AWS menyimpan kunci publik dan Anda menyimpan kunci pribadi di tempat yang aman.

Grup keamanan

Firewall virtual yang memungkinkan Anda menentukan protokol, port, dan rentang IP sumber yang dapat menjangkau instans Anda, serta rentang IP tujuan yang dapat terhubung ke instans Anda.

Amazon EC2 mendukung pemrosesan, penyimpanan, dan transmisi data kartu kredit oleh pedagang atau penyedia layanan, serta telah divalidasi sesuai dengan Standar Keamanan Data (DSS) Industri Kartu Pembayaran (PCI). Untuk informasi selengkapnya tentang PCI DSS, termasuk cara meminta salinan PCI AWS Compliance Package, lihat PCI DSS Level 1.

Layanan terkait

Layanan untuk digunakan dengan Amazon EC2

Anda dapat menggunakan instans lain Layanan AWS dengan instans yang Anda terapkan menggunakan Amazon EC2.

Amazon EC2 Auto Scaling

Membantu memastikan Anda memiliki jumlah instans Amazon EC2 yang tepat serta tersedia untuk menangani beban aplikasi Anda.

AWS Backup

Otomatiskan pencadangan instans Amazon EC2 Anda dan volume Amazon EBS yang dilampirkan padanya.

Amazon CloudWatch

Pantau instans dan volume Amazon EBS Anda.

Elastic Load Balancing

Mendistribusikan lalu lintas aplikasi yang masuk ke banyak instans secara otomatis.

Amazon GuardDuty

Deteksi penggunaan yang berpotensi tidak sah atau berbahaya dari instans EC2 Anda.

EC2 Image Builder

Otomatiskan pembuatan, pengelolaan, dan penyebaran gambar yang disesuaikan, aman, dan up-to-date server.

AWS Launch Wizard

Mengukur, mengonfigurasi, dan menyebarkan AWS sumber daya untuk aplikasi pihak ketiga tanpa harus mengidentifikasi dan menyediakan AWS sumber daya individual secara manual.

AWS Systems Manager

Lakukan operasi dalam skala besar pada instans EC2 dengan solusi end-to-end manajemen yang aman ini.

Layanan komputasi tambahan

Anda dapat meluncurkan instans menggunakan layanan AWS komputasi lain alih-alih menggunakan Amazon EC2.

Amazon Lightsail

Buat situs web atau aplikasi web menggunakan Amazon Lightsail, platform cloud yang menyediakan sumber daya yang Anda butuhkan untuk menyebarkan proyek Anda dengan cepat, dengan harga bulanan yang rendah dan dapat diprediksi. Untuk membandingkan Amazon EC2 dan Lightsail, lihat Amazon Lightsail atau Amazon EC2.

Amazon Elastic Container Service (Amazon ECS)

Melakukan deployment, mengelola, dan menskalakan aplikasi dalam kontainer pada klaster instans EC2. Untuk informasi selengkapnya, lihat Memilih layanan AWS kontainer.

Amazon Elastic Kubernetes Service (Amazon EKS)

Jalankan aplikasi Kubernetes Anda di AWS. Untuk informasi selengkapnya, lihat Memilih layanan AWS kontainer.

Akses Amazon EC2

Anda dapat membuat dan mengelola instans Amazon EC2 menggunakan antarmuka berikut:

Konsol Amazon EC2

Antarmuka web sederhana untuk membuat serta mengelola instans Amazon EC2 dan sumber daya. Jika Anda telah mendaftar untuk sebuah AWS akun, Anda dapat mengakses konsol Amazon EC2 dengan masuk ke Konsol Manajemen AWS dan memilih EC2 dari halaman beranda konsol.

AWS Command Line Interface

Memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Hal ini didukung di Windows, Mac, dan Linux. Untuk informasi tentang AWS CLI selengkapnya, lihat Panduan Pengguna AWS Command Line Interface. Anda dapat menemukan perintah Amazon EC2 di Referensi Perintah AWS CLI.

CloudFormation

Amazon EC2 mendukung pembuatan sumber daya menggunakan CloudFormation. Anda membuat template, dalam format JSON atau YAMAL, yang menjelaskan AWS sumber daya Anda, dan CloudFormation ketentuan serta mengonfigurasi sumber daya tersebut untuk Anda. Anda dapat menggunakan kembali CloudFormation template untuk menyediakan resource yang sama beberapa kali, baik di Region dan akun yang sama atau di beberapa Region dan akun. Untuk informasi tentang tipe sumber daya yang didukung dan properti pada Amazon EC2 selengkapnya, lihat referensi tipe sumber daya EC2 di Panduan Pengguna AWS CloudFormation .

AWS SDKs

Jika Anda lebih suka membangun aplikasi menggunakan bahasa khusus APIs daripada mengirimkan permintaan melalui HTTP atau HTTPS, AWS menyediakan pustaka, kode sampel, tutorial, dan sumber daya lainnya untuk pengembang perangkat lunak. Pustaka ini menyediakan fungsi dasar yang mengotomatiskan tugas-tugas seperti menandatangani permintaan Anda secara kriptografis, mencoba kembali permintaan, dan menangani respons kesalahan, sehingga memudahkan Anda untuk memulai. Untuk informasi selengkapnya, lihat Alat untuk Membangun di AWS.

AWS Tools for PowerShell

Satu set PowerShell modul yang dibangun di atas fungsionalitas yang diekspos oleh SDK for .NET. Alat untuk PowerShell memungkinkan Anda melakukan operasi skrip pada AWS sumber daya Anda dari baris PowerShell perintah. Untuk mulai, lihat Panduan Pengguna AWS Tools for PowerShell. Anda dapat menemukan cmdlet untuk Amazon EC2, di Referensi Cmdlet AWS Tools for PowerShell.

API Kueri

Amazon EC2 menyediakan API Kueri. Permintaan ini adalah permintaan HTTP atau HTTPS yang menggunakan parameter HTTP verbs GET atau POST dan parameter Kueri yang diberi nama `Action`. Untuk informasi tentang tindakan API untuk Amazon EC2 selengkapnya, lihat Tindakan di Referensi API Amazon EC2.

Harga untuk Amazon EC2

Amazon EC2 menyediakan opsi harga berikut:

Tingkat Gratis

Anda dapat memulai Amazon EC2 secara gratis. Untuk menjelajahi opsi Tingkat Gratis, lihat AWS Tingkat Gratis.

Instans Sesuai Permintaan

Bayar instans yang Anda gunakan dalam hitungan detik, dengan minimal 60 detik, tanpa komitmen jangka panjang atau pembayaran di muka.

Savings Plans

Anda dapat mengurangi biaya Amazon EC2 dengan membuat komitmen pada jumlah penggunaan yang konsisten, dalam USD per jam, untuk jangka waktu 1 atau 3 tahun.

Instans Terpesan

Anda dapat mengurangi biaya Amazon EC2 dengan membuat komitmen pada konfigurasi instans tertentu, termasuk tipe dan Wilayah instans, untuk jangka waktu 1 atau 3 tahun.

Instans Spot

Minta instans EC2 yang tidak digunakan, yang dapat mengurangi biaya Amazon EC2 Anda secara signifikan.

Host Khusus

Mengurangi biaya dengan menggunakan server EC2 fisik yang sepenuhnya didedikasikan untuk penggunaan Anda, baik On-Demand maupun sebagai bagian dari Savings Plans. Anda dapat menggunakan lisensi perangkat lunak terikat server yang ada dan mendapatkan bantuan untuk memenuhi persyaratan kepatuhan.

Reservasi Kapasitas Sesuai Permintaan

Cadangkan kapasitas komputasi untuk instans EC2 Anda di Zona Ketersediaan tertentu untuk durasi waktu apa pun.

Penagihan per detik

Menghapus biaya menit dan detik yang tidak terpakai dari tagihan Anda.

Untuk daftar lengkap biaya dan harga Amazon EC2 serta informasi tentang model pembelian selengkapnya, lihat harga Amazon EC2.

Estimasi, penagihan, dan optimalisasi biaya

Untuk membuat perkiraan untuk kasus AWS penggunaan Anda, gunakan AWS Kalkulator Harga.

Untuk memperkirakan biaya transformasi beban kerja Microsoft menjadi arsitektur modern yang menggunakan layanan open source dan cloud-native yang digunakan AWS, gunakan Kalkulator Modernisasi AWS untuk Beban Kerja Microsoft.

Untuk melihat tagihan Anda, buka Dasbor Manajemen Penagihan dan Biaya di konsol AWS Manajemen Penagihan dan Biaya. Tagihan Anda berisi tautan ke laporan penggunaan yang

memberikan detail tentang tagihan Anda. Untuk mempelajari lebih lanjut tentang penagihan AWS akun, lihat Panduan Pengguna AWS Billing and Cost Management.

Jika Anda memiliki pertanyaan tentang AWS penagihan, akun, dan acara, hubungi AWS Support.

Untuk menghitung biaya sampel lingkungan yang disediakan, lihat Pusat Ekonomi Cloud. Saat menghitung biaya lingkungan yang disediakan, ingatlah untuk menyertakan biaya insidental seperti penyimpanan snapshot untuk volume EBS.

Anda dapat mengoptimalkan biaya, keamanan, dan kinerja AWS lingkungan Anda menggunakan AWS Trusted Advisor.

Anda dapat menggunakan AWS Cost Explorer untuk menganalisis biaya dan penggunaan instans EC2 Anda. Anda dapat melihat data hingga 13 bulan terakhir, dan memperkirakan berapa banyak kemungkinan Anda akan menghabiskan untuk 12 bulan ke depan. Untuk informasi selengkapnya, lihat Menganalisis biaya dan penggunaan Anda AWS Cost Explorer di Panduan AWS Cost Management Pengguna.

Sumber daya

- Fitur Amazon EC2
- AWS Re: posting
- AWS Pembangun Keterampilan
- AWS Support
- Tutorial Langsung
- Web Hosting
- Windows aktif AWS

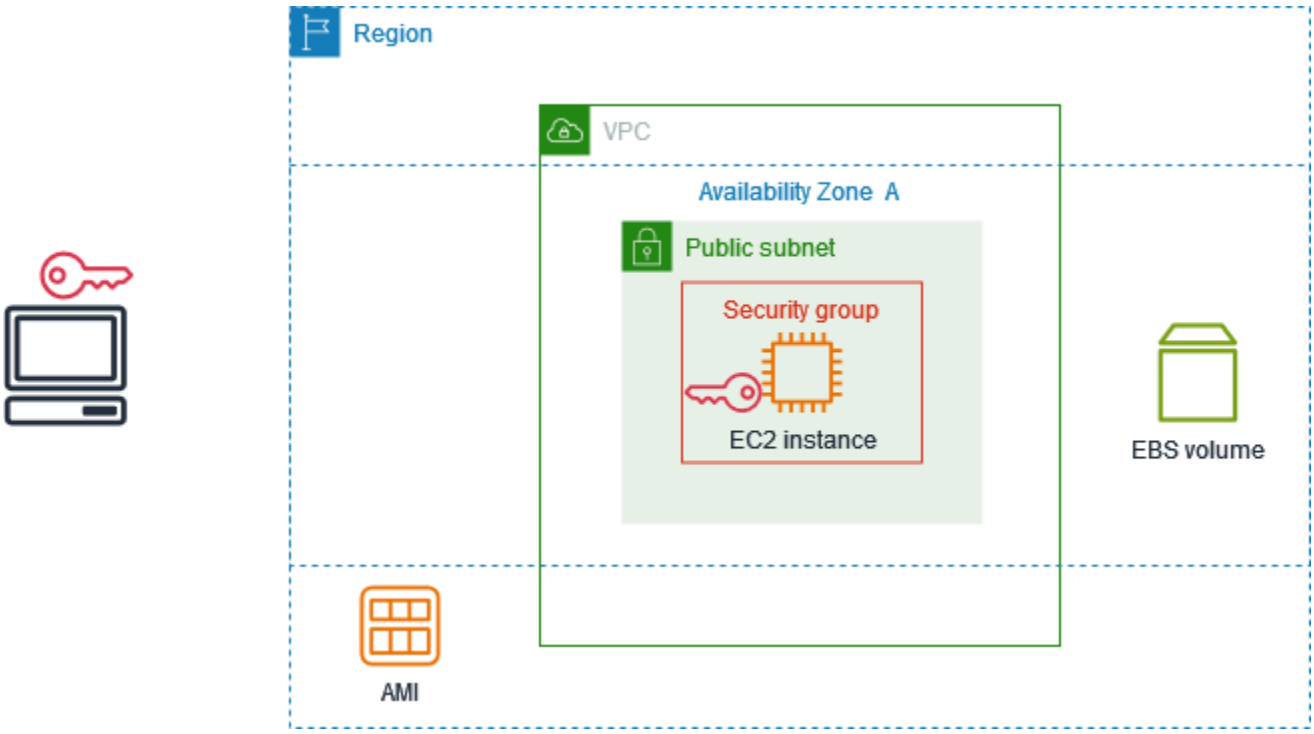
Memulai dengan Amazon EC2

Gunakan tutorial ini untuk memulai dengan Amazon Elastic Compute Cloud (Amazon EC2). Anda akan belajar cara meluncurkan dan terhubung ke sebuah EC2 instance. Instance adalah server virtual di AWS Cloud. Dengan Amazon EC2, Anda dapat mengatur dan mengonfigurasi sistem operasi dan aplikasi yang berjalan pada instans Anda.

Ikhtisar

Diagram berikut menunjukkan komponen kunci yang akan Anda gunakan dalam tutorial ini:

- Gambar — Template yang berisi perangkat lunak untuk dijalankan pada instance Anda, seperti sistem operasi.
- A key pair - Satu set kredenal keamanan yang Anda gunakan untuk membuktikan identitas Anda saat menghubungkan ke instans Anda. Kunci publik ada di instans Anda dan kunci pribadi ada di komputer Anda.
- Jaringan — Virtual Private Cloud (VPC) adalah jaringan virtual yang didedikasikan untuk Anda. Akun AWS Untuk membantu Anda memulai dengan cepat, akun Anda dilengkapi dengan VPC default di masing-masing AWS Region, dan setiap VPC default memiliki subnet default di setiap Availability Zone.
- Grup keamanan — Bertindak sebagai firewall virtual untuk mengontrol lalu lintas masuk dan keluar.
- Volume EBS — Kami memerlukan volume root untuk gambar. Anda dapat menambahkan volume data secara opsional.



Biaya untuk tutorial ini

Saat Anda membuat Akun AWS, Anda dapat memulai dengan Amazon secara EC2 gratis menggunakan AWS Tingkat Gratis.

Jika Anda membuat Akun AWS sebelum 15 Juli 2025, usianya kurang dari 12 bulan, dan Anda belum melampaui manfaat Tingkat Gratis untuk Amazon EC2, Anda tidak akan dikenakan biaya apa pun untuk menyelesaikan tutorial ini, karena kami membantu Anda memilih opsi yang ada dalam manfaat Tingkat Gratis. Jika tidak, Anda akan dikenakan biaya EC2 penggunaan Amazon standar sejak Anda meluncurkan instans (meskipun instans tetap menganggur) hingga Anda menghentikannya.

Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, usianya kurang dari 6 bulan, dan Anda belum menghabiskan semua kredit Anda, tidak akan dikenakan biaya apa pun untuk menyelesaikan tutorial ini, karena kami membantu Anda memilih opsi yang ada dalam manfaat Tingkat Gratis.

Untuk informasi tentang cara menentukan apakah Anda memenuhi syarat untuk Tingkat Gratis, lihatthe section called “Melacak penggunaan Tingkat Gratis Anda”.

Tugas

- Langkah 1: Luncurkan instans
- Langkah 2: Hubungkan ke instans Anda

- Langkah 3: Bersihkan instans Anda
- Langkah selanjutnya

Langkah 1: Luncurkan instans

Anda dapat meluncurkan EC2 instance menggunakan Konsol Manajemen AWS seperti yang dijelaskan dalam prosedur berikut. Tutorial ini dimaksudkan untuk membantu Anda meluncurkan instans pertama dengan cepat, jadi tutorial ini tidak mencakup semua opsi yang memungkinkan.

Untuk meluncurkan sebuah instans

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di bilah navigasi di bagian atas layar, kami menampilkan arus AWS Region - misalnya, Ohio. Anda dapat menggunakan Wilayah yang dipilih, atau secara opsional memilih Wilayah yang lebih dekat dengan Anda.
3. Dari dasbor EC2 konsol, di panel Launch instance, pilih Launch instance.
4. Di bawah Nama dan tanda, untuk Nama, masukkan nama deskriptif untuk instans Anda.
5. Di bawah Aplikasi dan Citra OS (Amazon Machine Image), lakukan hal berikut:
   a. Pilih Mulai Cepat, lalu pilih sistem operasi (OS) untuk instans Anda. Untuk contoh Linux pertama Anda, kami sarankan Anda memilih Amazon Linux.
   b. Dari Amazon Machine Image (AMI), pilih AMI yang ditandai Tingkat Gratis memenuhi syarat.
6. Di bawah Jenis instans, untuk tipe Instance, pilih jenis instans yang ditandai Tingkat Gratis memenuhi syarat.
7. Di bawah Key pair (login), untuk nama Key pair, pilih key pair yang ada atau pilih Create new key pair untuk membuat key pair pertama Anda.

   > **Warning**
   >
   > Jika Anda memilih Proceed without a key pair (Tidak disarankan), Anda tidak akan dapat terhubung ke instance Anda menggunakan metode yang dijelaskan dalam tutorial ini.

8. Di bawah Pengaturan jaringan, perhatikan bahwa kami memilih VPC default Anda, memilih opsi untuk menggunakan subnet default di Availability Zone yang kami pilih untuk Anda, dan mengonfigurasi grup keamanan dengan aturan yang memungkinkan koneksi ke instans Anda dari mana saja (). `0.0.0.0/0`

> **Warning**
>
> Jika Anda menentukan `0.0.0.0/0`, Anda mengaktifkan lalu lintas dari alamat IP manapun di dunia. Untuk protokol SSH dan RDP, Anda mungkin menganggap ini dapat diterima untuk waktu yang singkat di lingkungan pengujian, tetapi tidak aman untuk lingkungan produksi. Dalam produksi, pastikan untuk mengotorisasi akses hanya dari alamat IP individu atau rentang alamat yang sesuai.

Untuk contoh pertama Anda, kami sarankan Anda menggunakan pengaturan default. Jika tidak, Anda dapat memperbarui pengaturan jaringan Anda sebagai berikut:

- (Opsional) Untuk menggunakan subnet default tertentu, pilih Edit dan kemudian pilih subnet.
- (Opsional) Untuk menggunakan VPC yang berbeda, pilih Edit lalu pilih VPC yang ada. Jika VPC tidak dikonfigurasi untuk akses internet publik, Anda tidak akan dapat terhubung ke instans Anda.
- (Opsional) Untuk membatasi lalu lintas koneksi masuk ke jaringan tertentu, pilih Kustom alih-alih Di Mana Saja, dan masukkan blok CIDR untuk jaringan Anda.
- (Opsional) Untuk menggunakan grup keamanan yang berbeda, pilih Pilih grup keamanan yang ada dan pilih grup keamanan yang ada. Jika grup keamanan tidak memiliki aturan yang memungkinkan lalu lintas koneksi dari jaringan Anda, Anda tidak akan dapat terhubung ke instans Anda. Untuk contoh Linux, Anda harus mengizinkan lalu lintas SSH. Untuk contoh Windows, Anda harus mengizinkan lalu lintas RDP.

9. Di bawah Konfigurasi penyimpanan, perhatikan bahwa kami mengonfigurasi volume root tetapi tidak ada volume data. Ini cukup untuk tujuan pengujian.
10. Tinjau ringkasan konfigurasi instans di panel Ringkasan, dan ketika Anda siap, pilih Luncurkan instans.
11. Jika peluncuran berhasil, pilih ID instance dari notifikasi Sukses untuk membuka halaman Instans dan memantau status peluncuran.
12. Pilih kotak centang untuk instans. Keadaan instance awal adalah`pending`. Setelah instance dimulai, statusnya berubah menjadi`running`. Pilih tab Status dan alarm. Setelah instance Anda melewati pemeriksaan statusnya, instans siap menerima permintaan koneksi.

Langkah 2: Hubungkan ke instans Anda

Prosedur yang Anda gunakan tergantung pada sistem operasi instance. Jika Anda tidak dapat terhubung ke instans, lihat Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda untuk mendapatkan bantuan.

Instans Linux

Anda dapat terhubung ke instance Linux Anda menggunakan klien SSH apa pun. Jika Anda menjalankan Windows di komputer Anda, buka terminal dan jalankan `ssh` perintah untuk memverifikasi bahwa Anda telah menginstal klien SSH. Jika perintah tidak ditemukan, instal OpenSSH untuk Windows.

Untuk terhubung ke instans Anda menggunakan SSH

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Hubungkan.
4. Pada halaman Connect to instance, pilih tab SSH client.
5. (Opsional) Jika Anda membuat key pair saat meluncurkan instance dan mengunduh kunci pribadi (file.pem) ke komputer yang menjalankan Linux atau macOS, jalankan chmod perintah example untuk mengatur izin untuk kunci pribadi Anda.
6. Salin contoh perintah SSH. Berikut ini adalah contoh, di mana *key-pair-name* .pem adalah nama file kunci pribadi Anda, *ec2-user* adalah nama pengguna yang terkait dengan gambar, dan string setelah simbol @ adalah nama DNS publik dari instance.

   ```
   ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
   ```

7. Di jendela terminal di komputer Anda, jalankan ssh perintah yang Anda simpan di langkah sebelumnya. Jika file kunci pribadi tidak ada di direktori saat ini, Anda harus menentukan jalur yang sepenuhnya memenuhi syarat ke file kunci dalam perintah ini.

   Berikut adalah respons contohnya:

   ```
   The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
    (198-51-100-1)' can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```

8. (Opsional) Verifikasi bahwa sidik jari dalam peringatan keamanan cocok dengan sidik jari instance yang terdapat dalam keluaran konsol saat Anda pertama kali memulai instance. Untuk mendapatkan output konsol, pilih Tindakan, Monitor dan pemecahan masalah, Dapatkan log sistem. Jika sidik jari tidak cocok, seseorang mungkin mencoba menyerang. man-in-the-middle Jika cocok, lanjutkan ke langkah berikutnya.
9. Masukkan **`yes`**.

   Berikut adalah respons contohnya:

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

Instans Windows

Untuk terhubung ke instance Windows menggunakan RDP, Anda harus mengambil kata sandi administrator awal dan kemudian memasukkan kata sandi ini saat Anda terhubung ke instans Anda. Diperlukan beberapa menit setelah peluncuran instans sebelum sandi ini tersedia. Akun Anda harus memiliki izin untuk memanggil GetPasswordDatatindakan tersebut. Untuk informasi selengkapnya, lihat Contoh kebijakan untuk mengontrol akses API Amazon EC2.

Nama pengguna default untuk akun Administrator tergantung pada bahasa sistem operasi (OS) yang terkandung dalam AMI. Untuk menentukan nama pengguna yang benar, identifikasi bahasa OS, lalu pilih nama pengguna yang sesuai. Misalnya, untuk OS bahasa Inggris, nama pengguna adalah`Administrator`, untuk OS Prancis itu`Administrateur`, dan untuk OS Portugis itu`Administrador`. Jika versi bahasa OS tidak memiliki nama pengguna dalam bahasa yang sama, pilih nama penggguna`Administrator (Other)`. Untuk informasi selengkapnya, lihat Nama Lokal untuk Akun Administrator di Windows di situs web Microsoft.

Untuk mengambil kata sandi administrator awal

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Hubungkan.
4. Pada halaman Connect to instance, pilih tab klien RDP.
5. Untuk Nama Pengguna, pilih nama pengguna default untuk akun Administrator. Nama pengguna yang Anda pilih harus sesuai dengan bahasa sistem operasi (OS) yang terdapat dalam AMI yang

Anda gunakan untuk meluncurkan instance Anda. Jika tidak ada nama pengguna dalam bahasa yang sama dengan OS Anda, pilih Administrator (Lainnya).

6. Pilih Dapatkan kata sandi.
7. Pada halaman Dapatkan kata sandi Windows, lakukan hal berikut:

   a. Pilih Unggah file kunci pribadi dan arahkan ke file kunci pribadi (`.pem`) yang Anda tentukan saat meluncurkan instance. Pilih file dan pilih Buka untuk menyalin seluruh isi file ke jendela ini.

   b. Pilih Dekripsi kata sandi. Halaman Dapatkan kata sandi Windows ditutup, dan kata sandi administrator default untuk instance muncul di bawah Kata Sandi, menggantikan tautan Dapatkan kata sandi yang ditampilkan sebelumnya.

   c. Salin kata sandi dan simpan di tempat yang aman. Kata sandi ini diperlukan untuk terhubung ke instans.

Prosedur berikut menggunakan klien Remote Desktop Connection untuk Windows (MSTSC). Jika Anda menggunakan klien RDP yang berbeda, unduh file RDP dan kemudian lihat dokumentasi untuk klien RDP untuk langkah-langkah untuk membuat koneksi RDP.

Untuk terhubung ke instance Windows menggunakan klien RDP

1. Pada halaman Connect to instance, pilih Download file remote desktop. Setelah pengunduhan file selesai, pilih Batal untuk kembali ke halaman Instans. File RDP diunduh ke folder Anda`Downloads`.
2. Jalankan `mstsc.exe` untuk membuka klien RDP.
3. Perluas opsi Tampilkan, pilih Buka, dan pilih file.rdp dari folder Anda. `Downloads`
4. Secara default, Komputer adalah nama IPv4 DNS publik dari instance dan Nama pengguna adalah akun administrator. Untuk terhubung ke instance menggunakan IPv6 sebagai gantinya, ganti nama IPv4 DNS publik instance dengan IPv6 alamatnya. Tinjau pengaturan default dan ubah sesuai kebutuhan.
5. Pilih Hubungkan. Jika Anda menerima peringatan bahwa penerbit koneksi jarak jauh tidak diketahui, pilih Connect untuk melanjutkan.
6. Masukkan kata sandi yang Anda simpan sebelumnya, lalu pilih OK.
7. Karena sifat dari sertifikat yang ditandatangani sendiri, Anda mungkin mendapatkan peringatan bahwa sertifikat keamanan tidak dapat diautentikasi. Lakukan salah satu tindakan berikut:
   - Jika Anda mempercayai sertifikat, pilih Ya untuk terhubung ke instans Anda.

- [Windows] Sebelum Anda melanjutkan, bandingkan sidik jari sertifikat dengan nilai dalam log sistem untuk mengkonfirmasi identitas komputer jarak jauh. Pilih Lihat sertifikat lalu pilih Thumbprint dari tab Detail. Bandingkan nilai ini dengan nilai `RDPCERTIFICATE-THUMBPRINT` dalam Tindakan, Pantau dan pemecahan masalah, Dapatkan log sistem.
- [Mac OS X] Sebelum Anda melanjutkan, bandingkan sidik jari sertifikat dengan nilai dalam log sistem untuk mengonfirmasi identitas komputer jarak jauh. Pilih Tampilkan Sertifikat, perluas Detail, dan pilih SHA1 Sidik Jari. Bandingkan nilai ini dengan nilai `RDPCERTIFICATE-THUMBPRINT` dalam Tindakan, Pantau dan pemecahan masalah, Dapatkan log sistem.

8. Jika koneksi RDP berhasil, klien RDP menampilkan layar login Windows dan kemudian desktop Windows. Jika Anda menerima pesan kesalahan, lihatthe section called “Desktop Jarak Jauh tidak dapat terhubung ke komputer jarak jauh”. Ketika Anda selesai dengan koneksi RDP, Anda dapat menutup klien RDP.

Langkah 3: Bersihkan instans Anda

> **Warning**
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
> Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Setelah selesai dengan instans yang Anda buat untuk tutorial ini, Anda harus membersihkannya dengan mengakhiri instans tersebut. Jika Anda ingin melakukan lebih banyak hal dengan instans ini sebelum membersihkannya, lihat Langkah selanjutnya.

Anda akan berhenti dikenakan biaya untuk contoh tersebut atau penggunaan yang diperhitungkan terhadap batas Tingkat Gratis Anda segera setelah status instans berubah menjadi atau. `shutting down` `terminated` Untuk menyimpan instans Anda nanti, tetapi tidak dikenakan biaya atau penggunaan yang diperhitungkan terhadap batas Tingkat Gratis Anda, Anda dapat menghentikan

instans sekarang dan kemudian memulainya lagi nanti. Untuk informasi selengkapnya, lihat Hentikan dan mulai instans Amazon EC2.

Untuk mengakhiri instans Anda

1. Di panel navigasi, pilih Instans. Dalam daftar instans, pilih instans tersebut.
2. Pilih Instance state, Terminate (delete) instance.
3. Pilih Hentikan (hapus) saat diminta konfirmasi.

   Amazon EC2 menutup dan menghentikan instans Anda. Setelah Anda mengakhiri sebuah instans, instans akan tetap terlihat di konsol untuk beberapa saat, kemudian entri tersebut akan dihapus secara otomatis. Anda tidak dapat menghapus sendiri instans yang telah diakhiri dari tampilan konsol.

Langkah selanjutnya

Setelah memulai instans, Anda mungkin ingin menjelajahi langkah-langkah berikut:

- Jelajahi konsep EC2 inti Amazon dengan tutorial pengantar. Untuk informasi selengkapnya, lihat Tutorial untuk meluncurkan instans EC2.
- Pelajari cara melacak penggunaan Tingkat EC2 Gratis Amazon Anda menggunakan konsol. Untuk informasi selengkapnya, lihat the section called “Melacak penggunaan Tingkat Gratis Anda”.
- Konfigurasikan CloudWatch alarm untuk memberi tahu Anda jika penggunaan Anda melebihi Tingkat Gratis (untuk akun yang dibuat sebelum 15 Juli 2025). Untuk informasi selengkapnya, lihat Melacak AWS Tingkat Gratis penggunaan Anda di Panduan AWS Billing Pengguna.
- Tambahkan volume EBS. Untuk informasi selengkapnya, lihat Membuat volume Amazon EBS di Panduan Pengguna Amazon EBS.
- Pelajari cara mengelola EC2 instans Anda dari jarak jauh menggunakan Run perintah. Untuk informasi selengkapnya, lihat Run Command AWS Systems Manager di Panduan Pengguna AWS Systems Manager .
- Pelajari tentang opsi pembelian instans. Untuk informasi selengkapnya, lihat Opsi penagihan dan pembelian Amazon EC2.
- Dapatkan saran tentang tipe instans. Lihat informasi yang lebih lengkap di Dapatkan rekomendasi dari pencari tipe instans EC2.

Praktik terbaik untuk Amazon EC2

Untuk mendapatkan keuntungan maksimal dari Amazon EC2, kami menyarankan Anda untuk melakukan praktik terbaik berikut.

Keamanan

- Kelola akses ke AWS sumber daya dan APIs gunakan federasi identitas dengan penyedia identitas dan peran IAM bila memungkinkan. Untuk informasi selengkapnya, lihat Penyedia dan federasi identitas dalam Panduan Pengguna IAM.
- Terapkan aturan paling sedikit permisif untuk grup keamanan Anda.
- Lakukan patch, perbarui, serta amankan sistem operasi dan aplikasi pada instans Anda secara berkala. Untuk informasi selengkapnya, lihat Manajemen pembaruan. Untuk panduan khusus untuk sistem operasi Windows, lihatPraktik terbaik keamanan untuk instans Windows.
- Gunakan Amazon Inspector untuk secara otomatis menemukan dan memindai instans Amazon EC2 agar dapat memeriksa kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon Inspector.
- Gunakan AWS Security Hub CSPM kontrol untuk memantau sumber daya Amazon EC2 Anda terhadap praktik terbaik keamanan dan standar keamanan. Untuk informasi selengkapnya tentang menggunakan Security Hub CSPM, lihat kontrol Amazon Elastic Compute Cloud di Panduan Pengguna.AWS Security Hub CSPM

Penyimpanan

- Memahami implikasi dari tipe volume root untuk persistensi data, backup, dan recovery. Untuk informasi selengkapnya, lihat Tipe volume root.
- Gunakan volume Amazon EBS yang terpisah untuk sistem operasi versus data Anda. Pastikan bahwa volume dengan data Anda tetap ada setelah instans diakhiri. Untuk informasi selengkapnya, lihat Pertahankan data saat instans diakhiri.
- Gunakan penyimpanan instans yang tersedia untuk instans Anda agar dapat menyimpan data sementara. Perlu diingat bahwa data yang disimpan di penyimpanan instans akan dihapus saat Anda menghentikan, tidak mengaktifkan sementara, atau mengakhiri instans. Jika Anda menggunakan penyimpanan instans untuk penyimpanan basis data, pastikan bahwa Anda memiliki klaster dengan faktor replikasi yang menjamin toleransi kesalahan.

- Enkripsikan volume dan snapshot EBS. Untuk informasi selengkapnya, lihat enkripsi Amazon EBS di Panduan Pengguna Amazon EBS.

Manajemen sumber daya

- Gunakan tanda metadata instans dan sumber daya kustom untuk melacak dan mengidentifikasi sumber daya AWS Anda. Untuk informasi lebih lanjut, lihat Gunakan metadata instans untuk mengelola instans EC2 dan Tandai sumber daya Amazon EC2 Anda.
- Lihat batas Anda saat ini untuk Amazon EC2. Rencanakan untuk meminta kenaikan batas sebelum Anda membutuhkannya. Untuk informasi selengkapnya, lihat Kuota EC2 layanan Amazon.
- Gunakan AWS Trusted Advisor untuk memeriksa AWS lingkungan Anda, dan kemudian membuat rekomendasi ketika ada peluang untuk menghemat uang, meningkatkan ketersediaan dan kinerja sistem, atau membantu menutup kesenjangan keamanan. Untuk informasi selengkapnya, lihat AWS Trusted Advisor dalam Panduan Pengguna AWS Dukungan .

Pencadangan dan pemulihan

- Cadangkan volume EBS secara berkala menggunakan snapshot Amazon EBS, dan buat Amazon Machine Image (AMI) dari instans Anda agar dapat menyimpan konfigurasi sebagai templat untuk meluncurkan instans mendatang. Untuk informasi selengkapnya tentang AWS layanan yang membantu mencapai kasus penggunaan ini, lihat AWS Backupdan Amazon Data Lifecycle Manager.
- Deploy komponen penting aplikasi Anda di banyak Zona Ketersediaan, dan replikasi data Anda dengan tepat.
- Desain aplikasi Anda untuk menangani pembuatan alamat IP dinamis saat instans Anda dimulai ulang. Untuk informasi selengkapnya, lihat Pengalamatan IP instans Amazon EC2.
- Pantau dan respons peristiwa. Untuk informasi selengkapnya, lihat Pantau sumber daya Amazon EC2.
- Pastikan bahwa Anda siap menangani failover. Untuk solusi dasar, Anda dapat melampirkan antarmuka jaringan atau alamat IP Elastis ke instans pengganti secara manual. Untuk informasi selengkapnya, lihat Antarmuka jaringan elastis. Untuk solusi otomatis, Anda dapat menggunakan Amazon EC2 Auto Scaling. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon EC2 Auto Scaling.
- Uji proses pemulihan instans dan volume Amazon EBS Anda secara berkala untuk memastikan bahwa data dan layanan dipulihkan dengan sukses.

Jaringan

- Tetapkan nilai time-to-live (TTL) untuk aplikasi Anda ke 255, untuk IPv4 dan. IPv6 Jika Anda menggunakan nilai yang lebih kecil, ada risiko TTL akan kedaluwarsa saat lalu lintas aplikasi sedang bergerak, sehingga menyebabkan masalah jangkauan untuk instans Anda.

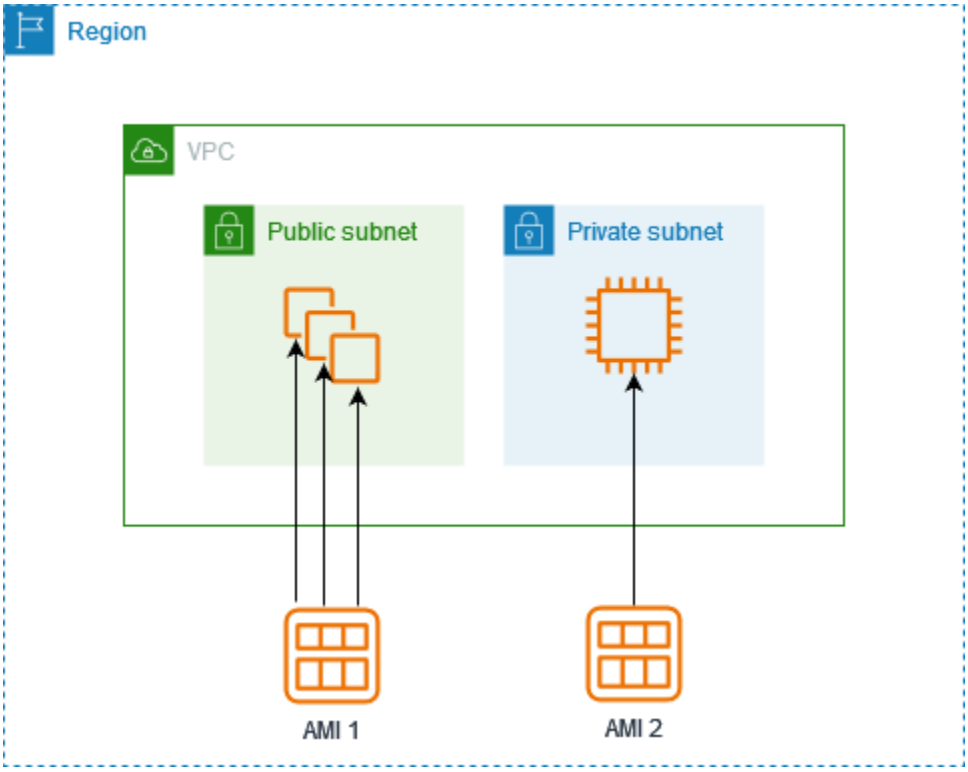
Gambar Mesin Amazon di Amazon EC2

Amazon Machine Image (AMI) adalah gambar yang menyediakan perangkat lunak yang diperlukan untuk mengatur dan mem-boot instans Amazon EC2. Setiap AMI juga berisi pemetaan perangkat blok yang menentukan perangkat blok untuk dilampirkan ke instance yang Anda luncurkan. Anda harus menentukan AMI saat meluncurkan instans. AMI harus kompatibel dengan jenis instans yang Anda pilih untuk instans Anda. Anda dapat menggunakan AMI yang disediakan oleh AWS, AMI publik, AMI yang dibagikan orang lain dengan Anda, atau AMI yang Anda beli dari AMI AWS Marketplace.

AMI khusus untuk yang berikut:

- Region
- Sistem operasi
- Arsitektur prosesor
- Tipe volume root
- Tipe virtualisasi

Anda dapat meluncurkan beberapa instans dari satu AMI jika Anda memerlukan beberapa instans dengan konfigurasi yang sama. Anda dapat menggunakan yang berbeda AMIs untuk meluncurkan instance ketika Anda memerlukan instance dengan konfigurasi yang berbeda, seperti yang ditunjukkan pada diagram berikut.



Anda dapat membuat AMI dari instans Amazon EC2 dan kemudian menggunakannya untuk meluncurkan instans dengan konfigurasi yang sama. Anda dapat menyalin AMI ke AWS Wilayah lain, dan kemudian menggunakannya untuk meluncurkan instance di Wilayah tersebut. Anda juga dapat membagikan AMI yang Anda buat dengan akun lain sehingga mereka dapat meluncurkan instance dengan konfigurasi yang sama. Anda dapat menjual AMI Anda menggunakan AWS Marketplace.

Daftar Isi

- Jenis dan karakteristik AMI di Amazon EC2
- Temukan AMI yang memenuhi persyaratan untuk EC2 instans Anda
- AMIs Dibayar AWS Marketplace untuk instans Amazon EC2
- Siklus hidup Amazon EC2 AMI
- Perilaku peluncuran instans dengan mode boot Amazon EC2
- Gunakan enkripsi dengan dukungan EBS AMIs
- Memahami penggunaan AMI bersama di Amazon EC2
- Pantau peristiwa AMI menggunakan Amazon EventBridge
- Memahami informasi penagihan AMI
- Kuota AMI di Amazon EC2

Jenis dan karakteristik AMI di Amazon EC2

Saat meluncurkan instance, AMI yang Anda pilih harus kompatibel dengan jenis instans yang Anda pilih. Anda dapat memilih AMI untuk digunakan berdasarkan karakteristik berikut:

- Wilayah
- Sistem operasi
- Arsitektur prosesor
- Izin peluncuran
- Tipe volume root
- Tipe virtualisasi

Izin peluncuran

Izin peluncuran menentukan siapa yang dapat menggunakan AMI untuk meluncurkan instance. Anda dapat menganggap izin peluncuran sebagai berbagi AMI —ketika Anda memberikan izin peluncuran, Anda membagikan AMI dengan pengguna lain. Hanya pemilik AMI yang dapat menentukan ketersediaannya dengan menentukan izin peluncuran. Izin peluncuran termasuk ke dalam kategori berikut.

Izin peluncuran	Deskripsi
publik	Pemilik memberikan izin peluncuran ke semua AWS akun.
eksplisit	Pemilik memberikan izin peluncuran ke AWS akun, organisasi, atau unit organisasi tertentu ()OUs.
implisit	Pemilik memiliki izin peluncuran implisit untuk AMI.

Amazon dan komunitas Amazon EC2 menyediakan banyak pilihan publik. AMIs Untuk informasi selengkapnya, lihat Memahami penggunaan AMI bersama di Amazon EC2. Pengembang dapat mengenakan biaya untuk mereka AMIs. Untuk informasi selengkapnya, lihat AMIs Dibayar AWS Marketplace untuk instans Amazon EC2.

Tipe volume root

Semua AMIs dikategorikan sebagai didukung oleh Amazon EBS atau didukung oleh Amazon S3.

- AMI yang didukung Amazon EBS-Backed — Volume root untuk instance yang diluncurkan dari AMI adalah volume Amazon Elastic Block Store (Amazon EBS) yang dibuat dari snapshot Amazon EBS. Didukung untuk Linux dan Windows AMIs.
- AMI yang didukung Amazon S3 — Volume root untuk instance yang diluncurkan dari AMI adalah volume penyimpanan instans yang dibuat dari template yang disimpan di Amazon S3. Didukung AMIs hanya untuk Linux. Windows AMIs tidak mendukung penyimpanan instance untuk volume root.

Untuk informasi selengkapnya, lihat Volume root untuk instans Amazon EC2.

> **Note**
>
> Dukungan Amazon S3 AMIs dianggap sebagai akhir masa pakai dan tidak direkomendasikan untuk penggunaan baru. Mereka hanya didukung pada jenis instans lama berikut: C1, C3, D2, I2, M1, M2, M3, R3, dan X1.

Tabel berikut merangkum perbedaan penting saat menggunakan kedua jenis. AMIs

Karakteristik	AMI yang didukung Amazon EBS	AMI yang didukung Amazon S3
Volume root	Volume EBS	Volume penyimpanan instans
Waktu boot untuk instans	Biasanya kurang dari 1 menit	Biasanya kurang dari 5 menit
Persistensi data	Secara default, volume root dihapus ketika instans berakhir.* Data di volume EBS lainnya tetap ada setelah pengakhiran instans secara default.	Data pada setiap volume penyimpanan instans hanya bertahan selama masa hidup instans.
Kondisi terhenti		

Karakteristik	AMI yang didukung Amazon EBS	AMI yang didukung Amazon S3
	Dapat berada dalam kondisi terhenti. Bahkan ketika instance dihentikan dan tidak berjalan, volume root tetap ada di Amazon EBS.	Tidak dapat berada dalam keadaan berhenti; instance sedang berjalan atau dihentikan.
Pengubahan	Tipe instans, kernel, disk RAM, dan data pengguna dapat diubah saat instans dihentikan.	Atribut instans tetap selama instan berlangsung.
Biaya	Anda dikenai biaya untuk penggunaan instans, penggunaa n volume EBS, dan penyimpanan AMI sebagai snapshot EBS.	Anda dikenai biaya penggunaan instans dan penyimpanan AMI di Amazon S3.
Pembuatan/pemaketa n AMI	Menggunakan perintah/panggilan tunggal	Memerlukan instalasi dan penggunaan alat AMI

* Secara default, volume root EBS memiliki tanda `DeleteOnTermination` diatur ke `true`. Untuk informasi tentang cara mengubah tanda ini sehingga volume tetap ada setelah pengakhiran, lihat Pertahankan volume root Amazon EBS setelah instans Amazon EC2 dihentikan.

** Hanya didukung dengan `io2` EBS Block Express. Untuk informasi selengkapnya, lihat Volume Blok Express IOPS SSD yang disediakan di Panduan Pengguna Amazon EBS.

Identifikasi jenis volume root yang ditentukan oleh AMI Anda

AMI yang Anda gunakan untuk meluncurkan instans EC2 menentukan jenis volume root. Volume root dari instans EC2 adalah volume EBS atau volume penyimpanan instans.

Instans berbasis nitro hanya mendukung volume root EBS. Jenis instans generasi sebelumnya berikut adalah satu-satunya tipe instans yang mendukung volume root penyimpanan instans: C1, C3, D2, I2, M1, M2, M3, R3, dan X1.

Console

Untuk mengidentifikasi jenis volume root yang ditentukan oleh AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs, dan pilih AMI.
3. Pada tab Detail, periksa nilai Tipe perangkat root sebagai berikut:
   - `ebs`— Instans yang diluncurkan dari AMI ini akan mendapatkan volume root EBS
   - `instance store`— Instans yang diluncurkan dari AMI ini akan mendapatkan volume root penyimpanan instance.

AWS CLI

Untuk mengidentifikasi jenis volume root yang ditentukan oleh AMI

Gunakan perintah describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].RootDeviceType
```

Berikut ini adalah output contoh.

```
ebs
```

PowerShell

Untuk mengidentifikasi jenis volume root yang ditentukan oleh AMI

Gunakan Get-EC2Imagecmdlet.

```
(Get-EC2Image `
    -ImageId ami-0abcdef1234567890).RootDeviceType.Value
```

Berikut ini adalah output contoh.

```
ebs
```

Tipe virtualisasi

Amazon Machine Image menggunakan salah satu dari dua tipe virtualisasi: paravirtual (PV) atau mesin virtual perangkat keras (HVM). Perbedaan utama antara PV dan HVM AMIs adalah cara mereka boot dan apakah mereka dapat memanfaatkan ekstensi perangkat keras khusus (CPU, jaringan, dan penyimpanan) untuk kinerja yang lebih baik. Windows AMIs adalah AMIs HVM.

Tabel berikut membandingkan HVM dan PV. AMIs

Karakteristik	HVM	PV
Deskripsi	AMI HVM disajikan dengan set perangkat keras virtual dan boot dengan menjalankan rekaman boot master perangkat blok root gambar Anda. Tipe virtualisasi ini menyediakan kemampuan untuk menjalankan sistem operasi secara langsung pada mesin virtual tanpa modifikasi apa pun, seolah-olah dijalankan di perangkat keras bare metal. Sistem host Amazon EC2 mengemulasi beberapa atau semua perangkat keras dasar yang disajikan kepada tamu.	AMIs Boot PV dengan boot loader khusus yang disebut PV-GRUB, yang memulai siklus boot dan kemudian rantai memuat kernel yang ditentukan dalam `menu.lst` file pada gambar Anda. Tamu Paravirtual dapat menjalankan perangkat keras host yang tidak memiliki dukungan virtualisasi secara eksplisit . Untuk informasi selengkapnya tentang PV-GRUB dan penggunaannya di Amazon EC2, lihat Kernel yang disediakan pengguna.
Tipe instans yang didukung	Semua jenis instance generasi saat ini mendukung AMIs HVM.	Jenis instans generasi sebelumnya berikut mendukung PV AMIs: C1, C3, M1, M3, M2, dan T1. Jenis instans generasi saat ini yang tidak mendukung PV AMIs.
Dukungan untuk ekstensi perangkat keras	Tamu HVM dapat memanfaatkan ekstensi perangkat keras	Tidak, mereka tidak dapat memanfaatkan ekstensi

Karakteristik	HVM	PV
	yang menyediakan akses cepat ke perangkat keras dasar di sistem host. Mereka diharuskan menggunakan jaringan yang disempurnakan dan pemrosesan GPU. Untuk melewati instruksi ke jaringan khusus dan perangkat GPU, OS harus memiliki akses ke platform perangkat keras asli, dan virtualisasi HVM menyediakan akses ini. Untuk informasi selengkapnya, lihat Jaringan yang disempurnakan di EC2 instans Amazon.	perangkat keras khusus seperti jaringan yang disempurnakan atau pemrosesan GPU.
Bagaimana menemukan	Verifikasikan bahwa jenis virtualisasi AMI diatur ke `hvm`, menggunakan konsol atau perintah describe-images.	Verifikasikan bahwa jenis virtualisasi AMI diatur ke `paravirtual` , menggunakan konsol atau perintah describe-images.

PV di HVM

Tamu paravirtual secara tradisional berkinerja lebih baik dengan penyimpanan dan operasi jaringan daripada tamu HVM karena mereka dapat memanfaatkan driver khusus untuk I/O menghindari overhead meniru jaringan dan perangkat keras disk, sedangkan tamu HVM harus menerjemahkan instruksi ini ke perangkat keras yang ditiru. Sekarang driver PV tersedia untuk tamu HVM, sehingga sistem operasi yang tidak dapat di-porting untuk berjalan di lingkungan paravirtualisasi masih dapat melihat keunggulan kinerja dalam penyimpanan dan jaringan dengan menggunakannya. I/O Dengan PV pada driver HVM ini, tamu HVM dapat memperoleh performa yang sama, atau lebih baik daripada tamu paravirtual.

Temukan AMI yang memenuhi persyaratan untuk EC2 instans Anda

AMI mencakup komponen dan aplikasi, seperti sistem operasi dan jenis volume root, yang diperlukan untuk meluncurkan sebuah instance. Untuk meluncurkan instance, Anda harus menemukan AMI yang memenuhi kebutuhan Anda.

Saat memilih AMI, pertimbangkan persyaratan berikut yang mungkin Anda miliki untuk instance yang ingin Anda luncurkan:

- AWS Wilayah AMI sebagai AMI IDs unik untuk setiap Wilayah.
- Sistem operasi (misalnya, Linux atau Windows).
- Arsitektur (misalnya, 32-bit, 64-bit, atau 64-bit ARM).
- Jenis volume root (misalnya, Amazon EBS atau penyimpanan instance).
- Penyedia (misalnya, Amazon Web Services).
- Perangkat lunak tambahan (misalnya, SQL Server).

Console

Anda dapat memilih dari daftar AMIs kapan Anda menggunakan wizard instance peluncuran, atau Anda dapat mencari semua yang tersedia AMIs menggunakan halaman Gambar.

Untuk menemukan AMI Mulai Cepat menggunakan wizard instance peluncuran

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Dari bilah navigasi, pilih Wilayah untuk meluncurkan instans Anda. Anda dapat memilih Wilayah yang tersedia untuk Anda, terlepas dari lokasi Anda. AMI IDs unik untuk setiap AWS Wilayah.
3. Dari dasbor konsol, pilih Luncurkan instans.
4. Di bawah Gambar Aplikasi dan OS (Gambar Mesin Amazon), pilih Mulai Cepat, pilih sistem operasi (OS) untuk instans Anda, dan kemudian, dari Amazon Machine Image (AMI), pilih dari salah satu yang umum digunakan AMIs dalam daftar. Jika Anda tidak melihat AMI yang ingin Anda gunakan, pilih Jelajahi lebih lanjut AMIs untuk menelusuri katalog AMI lengkap. Untuk informasi selengkapnya, lihat Aplikasi dan Gambar OS (Gambar Mesin Amazon).

Untuk menemukan AMI menggunakan AMIs halaman

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Dari bilah navigasi, pilih Wilayah untuk meluncurkan instans Anda. Anda dapat memilih Wilayah yang tersedia untuk Anda, terlepas dari lokasi Anda. AMI IDs unik untuk setiap AWS Wilayah.
3. Di panel navigasi, pilih AMIs.
4. (Opsional) Gunakan opsi filter dan pencarian untuk cakupan daftar yang ditampilkan AMIs untuk melihat hanya AMIs yang sesuai dengan kriteria Anda.

   Misalnya, untuk mencantumkan semua AMIs yang disediakan oleh AWS, pilih Gambar publik. Kemudian gunakan opsi pencarian untuk cakupan lebih lanjut daftar yang ditampilkan AMIs. Pilih bilah Pencarian dan, dari menu, pilih Alias pemilik, lalu operator =, lalu nilai amazon. Untuk menemukan AMIs yang cocok dengan platform tertentu, misalnya Linux atau Windows, pilih bilah Pencarian lagi untuk memilih Platform, lalu operator =, dan kemudian sistem operasi dari daftar yang disediakan.
5. (Opsional) Pilih ikon Preferensi untuk memilih atribut gambar mana yang akan ditampilkan, seperti jenis volume root. Atau, Anda dapat memilih AMI dari daftar dan melihat propertinya di tab Detail.
6. Sebelum memilih AMI, penting bagi Anda untuk memeriksa apakah ia didukung oleh penyimpanan instans atau Amazon EBS dan Anda mengetahui efek dari perbedaan ini. Untuk informasi selengkapnya, lihat Tipe volume root.
7. Untuk meluncurkan instans dari AMI ini, pilih dan pilih Peluncuran instans dari gambar. Untuk informasi selengkapnya tentang meluncurkan instans menggunakan konsol, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol. Jika Anda belum siap untuk meluncurkan instans, catatlah ID AMI untuk nanti.

AWS CLI

Gunakan perintah deskripsikan gambar untuk menemukan AMI yang memenuhi persyaratan Anda. Secara default, perintah ini mengembalikan semua AMIs yang bersifat publik, yang Anda miliki, dan yang dibagikan dengan Anda.

Untuk menemukan AMI yang dimiliki oleh Amazon

Gunakan perintah deskripsi-gambar dengan opsi. `--owners`

```
aws ec2 describe-images --owners amazon
```

Untuk menemukan AMI Windows

Tambahkan filter berikut untuk hanya menampilkan Windows AMIs.

```
--filters "Name=platform,Values=windows"
```

Untuk menemukan AMI yang didukung EBS

Tambahkan filter berikut untuk menampilkan hanya AMIs didukung oleh Amazon EBS.

```
--filters "Name=root-device-type,Values=ebs"
```

PowerShell

Gunakan Get-EC2Imagecmdlet untuk menemukan AMI yang memenuhi kebutuhan Anda. Secara default, cmdlet ini mengembalikan semua AMIs yang bersifat publik, yang Anda miliki, atau yang dibagikan dengan Anda.

Untuk menemukan AMI yang dimiliki oleh Amazon

Gunakan Get-EC2Imageperintah dengan `-Owner` parameter.

```
Get-EC2Image -Owner amazon
```

Untuk menemukan AMI Windows

Tambahkan filter berikut untuk hanya menampilkan Windows AMIs.

```
-Filter @{Name="platform"; Values="windows"}
```

Untuk contoh tambahan, lihat Menemukan Gambar Mesin Amazon Menggunakan Windows PowerShell di Panduan AWS Tools for PowerShell Pengguna.

Sumber daya terkait

Untuk informasi selengkapnya tentang AMIs sistem operasi tertentu, lihat berikut ini:

- Amazon Linux 2023 - AL2023 EC2 di Amazon di Panduan Pengguna Amazon Linux 2023
- Ubuntu - Amazon EC2 AMI Locator di situs web Canonical Ubuntu
- RHEL — Red Hat Enterprise Linux Images (AMI) Tersedia di Amazon Web Services (AWS) di situs web Red Hat
- Windows Server - Referensi AWS Windows AMI

Untuk informasi tentang AMIs itu, Anda dapat berlangganan di AWS Marketplace lihatAMIs Dibayar AWS Marketplace untuk instans Amazon EC2.

Untuk informasi tentang penggunaan Systems Manager untuk membantu pengguna menemukan AMI terbaru yang harus mereka gunakan saat meluncurkan instans, lihat berikut ini:

- Referensi AMIs menggunakan parameter Systems Manager
- Referensi terbaru AMIs menggunakan parameter publik Systems Manager

Referensi AMIs menggunakan parameter Systems Manager

Saat meluncurkan instance menggunakan wizard instans EC2 peluncuran di EC2 konsol Amazon, Anda dapat memilih AMI dari daftar, atau Anda dapat memilih AWS Systems Manager parameter yang mengarah ke ID AMI (dijelaskan di bagian ini). Jika menggunakan kode automasi untuk meluncurkan instans, Anda dapat menentukan parameter Systems Manager, bukan AMI ID.

Parameter System Manager adalah pasangan nilai-kunci yang ditentukan pelanggan yang dapat Anda buat di Penyimpanan Parameter System Manager. Penyimpanan Parameter menyediakan penyimpanan pusat untuk mengeksternalisasi nilai konfigurasi aplikasi Anda. Untuk informasi selengkapnya, lihat Penyimpanan Parameter AWS dalam Panduan Pengguna AWS Systems Manager .

Ketika Anda membuat parameter yang menunjuk ke sebuah ID AMI, pastikan Anda menentukan tipe data sebagai `aws:ec2:image`. Menentukan tipe data akan memastikan bahwa ketika parameter dibuat atau dimodifikasi, nilai parameter divalidasi sebagai ID AMI. Untuk informasi selengkapnya, lihat Dukungan parameter asli untuk Gambar Mesin Amazon IDs di Panduan AWS Systems Manager Pengguna.

Daftar Isi

- Kasus penggunaan
- Izin

- Batasan
- Meluncurkan instans menggunakan parameter Systems Manager

Kasus penggunaan

Bila Anda menggunakan parameter Systems Manager untuk menunjuk ke AMI IDs, akan lebih mudah bagi pengguna Anda untuk memilih AMI yang benar saat meluncurkan instance. Parameter Systems Manager juga dapat menyederhanakan pemeliharaan kode otomatisasi.

Lebih mudah bagi pengguna

Jika suatu instans perlu diluncurkan menggunakan AMI tertentu, dan AMI diperbarui secara rutin, kami sarankan Anda meminta pengguna untuk memilih parameter Systems Manager untuk mencari AMI. Mengharuskan pengguna memilih parameter Systems Manager memastikan AMI terbaru digunakan untuk meluncurkan instans.

Sebagai contoh, setiap bulan di organisasi, Anda dapat membuat versi AMI baru yang memiliki sistem operasi dan patch aplikasi terbaru. Anda juga memerlukan pengguna untuk meluncurkan instans menggunakan AMI versi terbaru Anda. Untuk memastikan pengguna menggunakan versi terbaru, Anda dapat membuat parameter Systems Manager (misalnya, `golden-ami`) yang menunjuk ke ID AMI yang benar. Setiap kali versi baru AMI dibuat, Anda memperbarui nilai ID AMI di parameter sehingga selalu mengarah ke AMI terbaru. Pengguna tidak perlu mengetahui pembaruan berkala untuk AMI karena mereka terus memilih parameter Systems Manager yang sama setiap saat. Penggunaan parameter Systems Manager untuk AMI Anda memudahkan mereka dalam memilih AMI yang benar untuk peluncuran instans.

Menyederhanakan pemeliharaan kode automasi

Jika menggunakan kode automasi untuk meluncurkan instans, Anda dapat menentukan parameter Systems Manager, bukan ID AMI. Setiap kali versi baru AMI dibuat, Anda memperbarui nilai ID AMI di parameter sehingga selalu mengarah ke AMI terbaru. Kode otomatisasi yang mengacu pada parameter tidak harus dimodifikasi setiap kali versi baru AMI dibuat. Hal ini menyederhanakan pemeliharaan otomatisasi dan membantu menurunkan biaya deployment.

> **Note**
>
> Instans yang berjalan tidak terpengaruh saat Anda mengubah ID AMI yang ditunjuk oleh parameter Systems Manager.

Izin

Jika Anda menggunakan parameter Systems Manager yang mengarah ke AMI IDs di wizard instans peluncuran, Anda harus menambahkan izin berikut ke kebijakan IAM Anda:

- `ssm:DescribeParameters`— Memberikan izin untuk melihat dan memilih parameter Systems Manager.
- `ssm:GetParameters`— Memberikan izin untuk mengambil nilai parameter Systems Manager.

Anda juga dapat membatasi akses ke parameter Systems Manager tertentu. Untuk informasi selengkapnya dan contoh kebijakan IAM, lihatContoh: Menggunakan wizard peluncuran instans EC2.

Batasan

AMIs dan parameter Systems Manager adalah Region spesifik. Untuk menggunakan nama parameter Systems Manager yang sama di seluruh Wilayah, buatlah parameter Systems Manager di setiap Wilayah dengan nama yang sama (misalnya, `golden-ami`). Di setiap Wilayah, arahkan parameter Systems Manager ke AMI di dalam Wilayah tersebut.

Nama parameter peka huruf besar/kecil. Garis miring terbalik untuk nama parameter hanya diperlukan jika parameter adalah bagian dari hierarki, misalnya, `/amis/production/golden-ami`. Anda dapat menghilangkan garis miring terbalik jika parameter bukan bagian dari hirarki.

Meluncurkan instans menggunakan parameter Systems Manager

Saat meluncurkan instance, alih-alih menentukan ID AMI, Anda dapat menentukan parameter Systems Manager yang menunjuk ke ID AMI.

Untuk menentukan parameter secara terprogram, gunakan sintaks berikut, di mana awalan standar dan `resolve:ssm` `parameter-name` merupakan nama parameter unik.

```
resolve:ssm:parameter-name
```

Parameter Systems Manager memiliki dukungan versi. Setiap iterasi parameter diberi nomor versi unik. Anda dapat mereferensikan versi parameter sebagai berikut, di `version` mana nomor versi uniknya. Secara default, versi terbaru parameter digunakan ketika tidak ada versi yang ditentukan.

```
resolve:ssm:parameter-name:version
```

Untuk meluncurkan instance menggunakan parameter publik yang disediakan oleh AWS, lihatReferensi terbaru AMIs menggunakan parameter publik Systems Manager.

Console

Untuk menemukan AMI menggunakan parameter Systems Manager

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Dari bilah navigasi, pilih Wilayah untuk meluncurkan instans Anda. Anda dapat memilih Wilayah yang tersedia untuk Anda, terlepas dari lokasi Anda.
3. Dari dasbor konsol, pilih Luncurkan instans.
4. Di bawah Gambar Aplikasi dan OS (Gambar Mesin Amazon), pilih Jelajahi lebih banyak AMIs.
5. Pilih tombol panah di sebelah kanan bilah pencarian, lalu pilih parameter Pencarian dengan Systems Manager.
6. Untuk Parameter System Manager, pilih parameter. ID AMI terkait akan muncul di bawah Saat ini memutuskan ke.
7. Pilih Pencarian. AMIs Yang cocok dengan ID AMI muncul dalam daftar.
8. Pilih AMI dari daftar, lalu pilih Pilih.

Untuk informasi tentang peluncuran instans menggunakan wizard peluncuran instans, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

AWS CLI

Untuk meluncurkan instance menggunakan parameter Systems Manager

Gunakan perintah run-instance dengan opsi. `--image-id` Contoh ini menggunakan parameter Systems Manager bernama**`golden-ami`**, yang menentukan ID AMI.

```
--image-id resolve:ssm:/golden-ami
```

Anda dapat membuat versi parameter Systems Manager. Contoh berikut menentukan versi 2 dari **`golden-ami`** parameter.

```
--image-id resolve:ssm:/golden-ami:2
```

PowerShell

Untuk meluncurkan instance menggunakan parameter Systems Manager

Gunakan New-EC2Instancecmdlet dengan parameter. `-ImageId` Contoh ini menggunakan parameter Systems Manager bernama**`golden-ami`**, yang menentukan ID AMI.

```
-ImageId "resolve:ssm:/golden-ami"
```

Anda dapat membuat versi parameter Systems Manager. Contoh berikut menentukan versi 2 dari **`golden-ami`** parameter.

```
-ImageId "resolve:ssm:/golden-ami:2"
```

Referensi terbaru AMIs menggunakan parameter publik Systems Manager

AWS Systems Manager menyediakan parameter publik untuk publik yang AMIs dikelola oleh AWS. Anda dapat menggunakan parameter publik saat meluncurkan instance untuk memastikan bahwa Anda menggunakan yang terbaru AMIs. Misalnya, parameter publik `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` tersedia di semua Wilayah dan selalu menunjuk ke versi terbaru Amazon Linux 2023 AMI untuk arsitektur arm64 di Wilayah tertentu.

Parameter publik tersedia dari jalur berikut:

- Linux – `/aws/service/ami-amazon-linux-latest`
- Windows – `/aws/service/ami-windows-latest`

Untuk informasi selengkapnya, lihat Bekerja dengan parameter publik di Panduan Pengguna AWS Systems Manager .

Daftar Amazon Linux AMIs

AWS CLI

Untuk daftar Linux AMIs di AWS Wilayah saat ini

Gunakan perintah berikut get-parameters-by-path. Nilai untuk `--path` parameter khusus untuk Linux AMIs.

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query "Parameters[].Name"
```

PowerShell

Untuk daftar Linux AMIs di AWS Wilayah saat ini

Gunakan Get- SSMParameters ByPath cmdlet.

```
Get-SSMParametersByPath `
    -Path "/aws/service/ami-amazon-linux-latest" | `
    Sort-Object Name | Format-Table Name
```

Daftar Windows AMIs

AWS CLI

Untuk membuat daftar Windows AMIs di AWS Wilayah saat ini

Gunakan perintah berikut get-parameters-by-path. Nilai untuk `--path` parameter khusus untuk Windows AMIs.

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query "Parameters[].Name"
```

PowerShell

Untuk membuat daftar Windows AMIs di AWS Wilayah saat ini

Gunakan Get- SSMParameters ByPath cmdlet.

```
Get-SSMParametersByPath `
    -Path "/aws/service/ami-windows-latest" | `
    Sort-Object Name | Format-Table Name
```

Luncurkan instance menggunakan parameter publik

Untuk menentukan parameter publik saat meluncurkan instance, gunakan sintaks berikut:`resolve:ssm:`*`public-parameter`*, di mana `resolve:ssm` awalan standar dan *`public-parameter`* merupakan jalur dan nama parameter publik.

AWS CLI

Untuk meluncurkan suatu instans menggunakan parameter publik

Gunakan perintah run-instance dengan opsi. `--image-id` Contoh ini menentukan parameter publik Systems Manager untuk ID gambar untuk meluncurkan instance menggunakan AMI Amazon Linux 2023 terbaru

```
--image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64
```

PowerShell

Untuk meluncurkan suatu instans menggunakan parameter publik

Gunakan New-EC2Instancecmdlet dengan parameter. `-ImageId` Contoh ini menentukan parameter publik Systems Manager untuk ID gambar untuk meluncurkan instance menggunakan AMI terbaru untuk Windows Server 2022.

```
-ImageId "resolve:ssm:/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base"
```

Untuk contoh selengkapnya yang menggunakan parameter Systems Manager, lihat Kueri untuk Amazon Linux AMI terbaru IDs Menggunakan AWS Systems Manager Parameter Store dan Query untuk AMI Windows Terbaru Menggunakan AWS Systems Manager Parameter Store.

AMIs Dibayar AWS Marketplace untuk instans Amazon EC2

AMI berbayar adalah AMI yang terdaftar untuk dijual di AWS Marketplace. AWS Marketplace Ini adalah toko online tempat Anda dapat membeli perangkat lunak yang berjalan AWS, termasuk AMI yang dapat Anda gunakan untuk meluncurkan instans EC2 Anda. AWS Marketplace AMIs Ini disusun ke dalam kategori, seperti Alat Pengembang, untuk memungkinkan Anda menemukan produk yang

sesuai dengan kebutuhan Anda. Untuk informasi lebih lanjut tentang AWS Marketplace, lihat situs AWS Marketplaceweb.

Anda dapat membeli AMIs AWS Marketplace dari pihak ketiga, termasuk AMIs yang datang dengan kontrak layanan dari organisasi seperti Red Hat. Anda juga dapat membuat AMI dan menjualnya AWS Marketplace ke pengguna Amazon EC2 lainnya. Membangun AMI yang aman, terjaga, dan dapat digunakan untuk konsumsi publik adalah hal yang cukup mudah jika Anda mengikuti beberapa langkah panduan sederhana. Untuk informasi tentang cara membuat dan menggunakan bersama AMIs, lihatMemahami penggunaan AMI bersama di Amazon EC2.

Meluncurkan instans dari AMI berbayar sama seperti meluncurkan instans dari AMI lainnya. Tidak perlu parameter tambahan. Instans dibebankan sesuai dengan tarif yang ditetapkan oleh pemilik AMI, serta biaya penggunaan standar untuk layanan web terkait, misalnya, tarif per jam untuk menjalankan jenis instans m5.small di Amazon EC2. Pajak tambahan mungkin juga berlaku. Pemilik AMI berbayar dapat mengonfirmasi apakah instans tertentu diluncurkan menggunakan AMI berbayar tersebut.

> **Important**
>
> Amazon DevPay tidak lagi menerima penjual atau produk baru. AWS Marketplace Sekarang menjadi platform e-commerce tunggal terpadu untuk menjual perangkat lunak dan layanan melalui AWS. Untuk informasi tentang cara menyebarkan dan menjual perangkat lunak AWS Marketplace, lihat Menjual di AWS Marketplace. AWS Marketplace mendukung AMIs didukung oleh Amazon EBS.

Daftar Isi

- Jual AMI Anda di AWS Marketplace
- Mencari AMI berbayar
- Beli AMI berbayar di AWS Marketplace
- Ambil kode AWS Marketplace produk dari instans Anda
- Gunakan dukungan berbayar untuk AWS Marketplace penawaran yang didukung
- Tagihan untuk dibayar dan didukung AMIs
- Kelola AWS Marketplace langganan Anda

Jual AMI Anda di AWS Marketplace

Anda dapat menjual AMI Anda menggunakan AWS Marketplace. AWS Marketplace menawarkan pengalaman berbelanja yang terorganisir. Selain itu, AWS Marketplace juga mendukung AWS fitur-fitur seperti Amazon EBS yang didukung AMIs, Instans Cadangan, dan Instans Spot.

Untuk informasi tentang cara menjual AMI Anda di AWS Marketplace, lihat Menjual di AWS Marketplace.

Mencari AMI berbayar

AMI berbayar adalah Amazon Machine Image (AMI) yang tersedia untuk dibeli. AMI berbayar juga memiliki kode produk. Anda dapat menemukan AMIs yang tersedia untuk pembelian di AWS Marketplace.

Console

Untuk menemukan AMI berbayar

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih Gambar publik untuk filter pertama.
4. Lakukan salah satu tindakan berikut:
   - Jika Anda mengetahui kode produk, pilih Kode Produk, lalu =, lalu masukkan kode produk.
   - Jika Anda tidak tahu kode produk, di bilah Pencarian, tentukan filter berikut: Owner alias=aws-marketplace. Tentukan filter tambahan sesuai kebutuhan.
5. Simpan ID AMI.

AWS CLI

Untuk menemukan AMI berbayar

Gunakan perintah deskripsi-gambar berikut.

```
aws ec2 describe-images --owners aws-marketplace
```

Outputnya mencakup sejumlah besar gambar. Anda dapat menentukan filter untuk membantu Anda menentukan AMI yang Anda butuhkan. Setelah Anda menemukan AMI, tentukan ID-nya dalam perintah berikut untuk mendapatkan kode produknya.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].ProductCodes[].ProductCodeId
```

Berikut ini adalah output contoh.

```
[
    "cdef1234abc567def8EXAMPLE"
]
```

Jika Anda mengetahui kode produk, Anda dapat memfilter hasilnya berdasarkan kode produk. Contoh berikut ini memberikan AMI terbaru dengan kode produk tertentu.

```
aws ec2 describe-images \
    --filters "Name=product-code,Values=cdef1234abc567def8EXAMPLE" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

PowerShell

Untuk menemukan AMI berbayar

Gunakan Get-EC2Imagecmdlet.

```
Get-EC2Image -Owner aws-marketplace
```

Outputnya mencakup sejumlah besar gambar. Anda dapat menentukan filter untuk membantu Anda menentukan AMI yang Anda butuhkan. Setelah Anda menemukan AMI, tentukan ID-nya dalam perintah berikut untuk mendapatkan kode produknya.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).ProductCodes
```

Berikut ini adalah output contoh.

```
ProductCodeId             ProductCodeType
```

```
-------------              ---------------
cdef1234abc567def8EXAMPLE marketplace
```

Jika Anda mengetahui kode produk, Anda dapat memfilter hasilnya berdasarkan kode produk. Contoh berikut ini memberikan AMI terbaru dengan kode produk tertentu.

```
(Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="cdef1234abc567def8EXAMPLE"} | sort CreationDate -Descending | Select-
Object -First 1).ImageId
```

Beli AMI berbayar di AWS Marketplace

Anda harus mendaftar (membeli) AMI berbayar sebelum dapat meluncurkan instans Amazon EC2 menggunakan AMI.

Biasanya, penjual AMI berbayar memberi Anda informasi tentang AMI, termasuk harga dan tautan tempat Anda dapat membelinya. Ketika Anda mengklik tautan, pertama-tama Anda diminta untuk masuk AWS, dan kemudian Anda dapat membeli AMI.

Membeli AMI berbayar menggunakan konsol

Anda dapat membeli AMI berbayar dengan menggunakan wizard peluncuran Amazon EC2. Untuk informasi selengkapnya, lihat Luncurkan instans Amazon EC2 dari AMI AWS Marketplace.

Berlangganan produk menggunakan AWS Marketplace

Untuk menggunakan AWS Marketplace, Anda harus memiliki Akun AWS. Untuk meluncurkan instans dari AWS Marketplace produk, Anda harus mendaftar untuk menggunakan layanan Amazon EC2, dan Anda harus berlangganan produk untuk meluncurkan instans. Anda dapat menggunakan salah satu metode berikut untuk berlangganan produk di AWS Marketplace:

- AWS Marketplace situs web: Anda dapat meluncurkan perangkat lunak yang telah dikonfigurasi sebelumnya dengan cepat dengan fitur penyebaran 1-Klik. Untuk informasi lebih lanjut, lihat produk berbasis AMI di. AWS Marketplace
- Wizard peluncuran Amazon EC2: Anda dapat mencari AMI dan meluncurkan instans langsung dari wizard. Untuk informasi selengkapnya, lihat Luncurkan instans Amazon EC2 dari AMI AWS Marketplace.

Ambil kode AWS Marketplace produk dari instans Anda

Anda dapat mengambil kode AWS Marketplace produk untuk instance Anda menggunakan metadata instance-nya. Jika instans memiliki kode produk, Amazon EC2 akan memberikannya. Untuk informasi selengkapnya tentang pengambilan metadata instans, lihat Akses metadata instans untuk instans EC2.

IMDSv2

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

Jalankan perintah berikut dari instance Windows Anda.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/product-codes
```

Gunakan dukungan berbayar untuk AWS Marketplace penawaran yang didukung

Amazon EC2 juga memungkinkan pengembang untuk menawarkan dukungan untuk perangkat lunak (atau turunan AMIs). Developer dapat membuat produk dukungan yang dapat Anda gunakan dengan mendaftar. Saat mendaftar untuk produk dukungan, developer memberi Anda kode produk, yang kemudian harus dikaitkan dengan AMI Anda sendiri. Hal ini memungkinkan developer untuk mengonfirmasi bahwa instans Anda memenuhi syarat untuk dukungan. Ini juga memastikan ketika Anda menjalankan instans produk, Anda dikenai biaya sesuai ketentuan untuk produk tertentu dari developer.

Batasan

- Setelah Anda mengatur atribut kode produk, itu tidak dapat diubah atau dihapus.
- Anda tidak dapat menggunakan produk dukungan dengan Instans Tercadang. Anda selalu membayar harga yang ditetapkan oleh penjual produk dukungan.

AWS CLI

Untuk mengaitkan kode produk dengan AMI Anda

Gunakan perintah modify-image-attribute.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --product-codes "cdef1234abc567def8EXAMPLE"
```

PowerShell

Untuk mengaitkan kode produk dengan AMI Anda

Gunakan Edit-EC2ImageAttributecmdlet.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
```

```
    -ProductCode "cdef1234abc567def8EXAMPLE"
```

Tagihan untuk dibayar dan didukung AMIs

Di setiap akhir bulan, Anda akan menerima email dengan jumlah yang ditagih ke kartu kredit untuk penggunaan AMI yang dibayar atau didukung selama bulan tersebut. Tagihan ini terpisah dari tagihan Amazon EC2 reguler Anda. Untuk informasi selengkapnya, lihat Membayar produk dalam Panduan Pembeli AWS Marketplace .

Kelola AWS Marketplace langganan Anda

Di AWS Marketplace situs web, Anda dapat memeriksa detail langganan, melihat petunjuk penggunaan vendor, mengelola langganan, dan banyak lagi.

Periksa detail berlangganan

Untuk memeriksa detail langganan Anda

1. Masuk ke AWS Marketplace.
2. Pilih Akun Marketplace Anda.
3. Pilih Kelola langganan perangkat lunak Anda.
4. Semua langganan Anda saat ini akan tercantum. Pilih Petunjuk Penggunaan untuk melihat petunjuk spesifik untuk menggunakan produk, misalnya, nama pengguna untuk menghubungkan ke instans yang sedang berjalan.

Batalkan langganan

> **Note**
>
> - Membatalkan langganan tidak menghentikan instans yang diluncurkan dengan AMI tersebut. Kami akan terus menagih Anda untuk instans yang sedang berjalan hingga instans tersebut dihentikan. Anda harus menghentikan semua instans yang diluncurkan dengan AMI untuk menghentikan penagihan langganan.
> - Setelah membatalkan langganan, Anda tidak lagi dapat meluncurkan instans apa pun dari AMI tersebut. Untuk menggunakan AMI itu lagi, Anda harus berlangganan kembali, baik di AWS Marketplace situs web, atau melalui panduan peluncuran di konsol Amazon EC2.

Untuk membatalkan AWS Marketplace langganan

1. Untuk menghentikan penagihan langganan, pastikan bahwa Anda telah menghentikan semua instans yang berjalan dari langganan.

   > **Warning**
   >
   > Mengakhiri sebuah instance bersifat permanen dan ireversibel.
   > Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance. Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

   a. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
   b. Di panel navigasi, pilih Instans.
   c. Pilih instance, lalu pilih Instance state, Terminate (delete) instance.
   d. Pilih Hentikan (hapus) saat diminta konfirmasi.
2. Masuk ke AWS Marketplace, dan pilih Akun Marketplace Anda, lalu Kelola langganan perangkat lunak Anda.
3. Pilih Batalkan langganan. Anda diminta untuk mengonfirmasi pembatalan.

Siklus hidup Amazon EC2 AMI

Amazon Machine Image (AMI) adalah gambar yang berisi konfigurasi perangkat lunak yang diperlukan untuk mengatur dan mem-boot instance. Anda harus menentukan AMI saat meluncurkan instans. Anda dapat menggunakan AMIs yang disediakan oleh Amazon, atau Anda dapat membuat sendiri AMIs. AMI harus terletak AWS Region di tempat Anda ingin meluncurkan instance Anda.

Siklus hidup AMI termasuk membuat, menyalin, menghentikan, menonaktifkan, dan menghapus (membatalkan pendaftaran) AMI.

Buat AMIs. Meskipun Amazon menyediakan AMIs yang dapat Anda gunakan untuk meluncurkan instans, Anda dapat membuat kustom yang AMIs disesuaikan dengan kebutuhan Anda. Untuk

membuat AMI kustom, luncurkan instance dari AMI yang ada, sesuaikan instance (misalnya, instal perangkat lunak dan konfigurasikan pengaturan sistem operasi), lalu buat AMI dari instance. Setiap penyesuaian instans disimpan ke AMI baru, sehingga instance yang diluncurkan dari AMI baru Anda menyertakan penyesuaian ini.

Dapat dibuktikan. AMIs Untuk membuat AMI yang mendukung pengesahan instans EC2, lihat. Dapat dibuktikan AMIs

Salin AMIs. Anda dapat menggunakan AMI untuk meluncurkan instance hanya AWS Region di tempat AMI berada. Jika Anda perlu meluncurkan instance dengan konfigurasi yang sama di beberapa Wilayah, salin AMI ke Wilayah lain.

Menghentikan AMIs. Untuk menandai AMI sebagai digantikan atau kedaluwarsa, Anda dapat menetapkan tanggal penghentian langsung atau masa depan. Usang AMIs disembunyikan dari daftar AMI, tetapi pengguna dan layanan dapat terus menggunakan usang jika AMIs mereka mengetahui ID AMI.

Nonaktifkan AMIs. Untuk mencegah sementara AMI digunakan, Anda dapat menonaktifkannya. Ketika AMI dinonaktifkan, AMI tidak dapat digunakan untuk meluncurkan instance baru. Namun, jika Anda mengaktifkan kembali AMI, AMI dapat digunakan untuk meluncurkan instance lagi. Perhatikan bahwa menonaktifkan AMI tidak memengaruhi instans yang ada yang telah diluncurkan darinya.

Deregister (hapus). AMIs Ketika Anda tidak lagi membutuhkan AMI, Anda dapat membatalkan pendaftarannya, mencegahnya digunakan untuk meluncurkan instance baru. Jika AMI cocok dengan aturan retensi, AMI pindah ke Recycle Bin, di mana AMI dapat dipulihkan sebelum periode retensi berakhir, setelah itu dihapus secara permanen. Jika tidak cocok dengan aturan retensi, itu akan segera dihapus secara permanen. Perhatikan bahwa membatalkan pendaftaran AMI tidak memengaruhi instans yang ada yang diluncurkan dari AMI.

Otomatiskan siklus hidup AMI. Anda dapat menggunakan Amazon Data Lifecycle Manager untuk melakukan otomatisasi pembuatan, penyimpanan, penyalinan, pengusangan, dan pembatalan pendaftaran AMI yang didukung Amazon EBS dan snapshot pendukungnya. Anda juga dapat menggunakan EC2 Image Builder untuk mengotomatiskan pembuatan, pengelolaan, penyebaran yang disesuaikan. AMIs Untuk informasi selengkapnya, lihat Mengotomatiskan pencadangan dengan Amazon Data Lifecycle Manager di Panduan Pengguna Amazon EBS dan Panduan Pengguna EC2 Image Builder.

Daftar Isi

- Buat AMI yang didukung Amazon EBS-Backed

- Buat AMI yang didukung Amazon S3
- Buat Amazon EC2 AMI menggunakan Windows Sysprep
- Salin Amazon EC2 AMI
- Simpan dan pulihkan AMI menggunakan S3
- Gunakan keturunan AMI untuk melacak asal usul AMI
- Kelola dan pantau penggunaan AMI
- Menghentikan Amazon AMI EC2
- Nonaktifkan Amazon EC2 AMI
- Membatalkan pendaftaran ke Amazon EC2 AMI

Buat AMI yang didukung Amazon EBS-Backed

Anda dapat membuat sendiri AMI yang didukung Amazon EBS-backed dari instans Amazon EC2 atau dari snapshot volume root instans Amazon EC2.

Untuk membuat AMI yang didukung Amazon EBS-backed dari sebuah instans, mulailah dengan meluncurkan instans menggunakan AMI yang didukung Amazon EBS-backed yang sudah ada. AMI ini dapat berupa AMI yang Anda peroleh dari AWS Marketplace, dibuat menggunakan VM Import/ Export, atau AMI lain yang dapat Anda akses. Setelah menyesuaikan instans untuk memenuhi persyaratan spesifik Anda, buat dan daftarkan AMI baru. Anda kemudian dapat menggunakan AMI baru untuk meluncurkan instance baru dengan penyesuaian Anda.

> **Note**
>
> Untuk membuat AMI yang mendukung pengesahan instans EC2, lihat. Dapat dibuktikan AMIs

Prosedur yang dijelaskan di bawah berfungsi untuk instans Amazon EC2 yang didukung oleh volume Amazon Elastic Block Store (Amazon EBS) terenkripsi (termasuk volume root) serta volume yang tidak dienkripsi.

Proses pembuatan AMI berbeda untuk Amazon S3 AMIs yang didukung. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon S3.

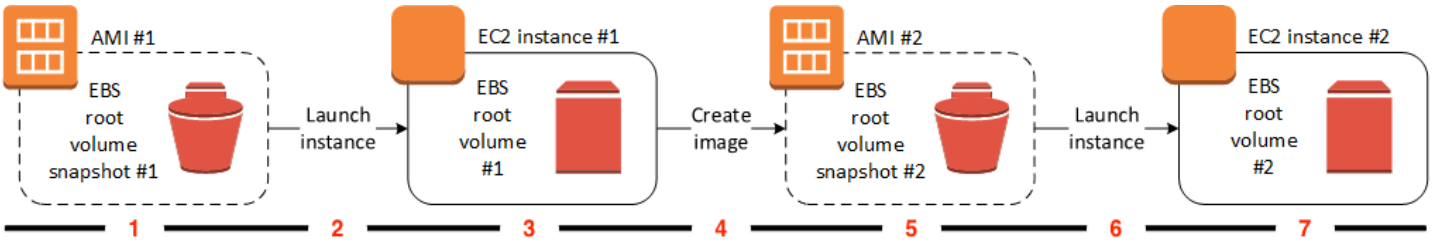
Daftar Isi

- Ikhtisar pembuatan AMI dari sebuah instance

- Buat AMI dari sebuah instance
- Buat AMI dari snapshot

Ikhtisar pembuatan AMI dari sebuah instance

Diagram berikut merangkum proses pembuatan AMI yang didukung Amazon EBS dari instans EC2 yang sedang berjalan: Mulai dengan AMI yang ada, luncurkan instans, kustomisasi, buat AMI baru darinya, dan terakhir luncurkan instans AMI baru Anda. Angka-angka dalam diagram cocok dengan angka-angka dalam deskripsi berikut.



1 – AMI #1: Mulailah dengan AMI yang ada

Cari AMI yang mirip dengan AMI yang ingin Anda buat. Ini bisa berupa AMI yang Anda peroleh dari AWS Marketplace, AMI yang telah Anda buat menggunakan VM Import/Export, atau AMI lain yang dapat Anda akses. Anda akan mengkustomisasi AMI ini untuk kebutuhan Anda.

Dalam diagram, Snapshot volume root EBS #1 menunjukkan bahwa AMI adalah AMI yang didukung Amazon EBS dan informasi tentang volume root disimpan dalam snapshot ini.

2 – Luncurkan instans dari AMI yang ada

Cara mengonfigurasi AMI adalah dengan meluncurkan instans dari AMI tempat Anda ingin mendasarkan AMI baru Anda, lalu mengustomisasi instans (ditunjukkan pada 3 dalam diagram). Kemudian, Anda akan membuat AMI baru yang menyertakan kustomisasi (ditunjukkan pada 4 dalam diagram).

3 – Instans EC2 #1: Kustomisasi instans

Sambungkan ke instans Anda dan kustomisasi sesuai kebutuhan. AMI Anda yang baru akan menyertakan kustomisasi ini.

Anda dapat melakukan tindakan berikut ini pada instans Anda untuk mengustomisasikannya:

- Menginstal perangkat lunak dan aplikasi
- Menyalin data

- Kurangi waktu mulai dengan menghapus file sementara dan mendefragmentasi hard drive Anda
- Melampirkan volume EBS tambahan

4 – Buat gambar

Saat Anda membuat AMI dari instans, Amazon EC2 menonaktifkan instans sebelum membuat AMI guna memastikan segala sesuatu yang ada pada instans dihentikan dan dalam kondisi yang konsisten selama proses pembuatan. Jika Anda yakin instans Anda berada dalam kondisi konsisten yang cocok untuk pembuatan AMI, Anda dapat memberi tahu Amazon EC2 untuk tidak mematikan dan melakukan boot ulang instans. Beberapa sistem file, seperti XFS, dapat membekukan dan membatalkan pembekuan aktivitas sehingga aman untuk membuat gambar tanpa boot ulang instans.

Selama proses pembuatan AMI, Amazon EC2 membuat snapshot volume root instans dan volume EBS lainnya yang dilampirkan ke instans Anda. Anda dikenai biaya untuk snapshot hingga Anda membatalkan pendaftaran AMI dan menghapus snapshot. Jika setiap volume yang dilampirkan pada instans dienkripsi, AMI yang baru hanya akan berhasil diluncurkan pada tipe instans yang mendukung enkripsi Amazon EBS.

Bergantung pada ukuran volume, pembuatan AMI dapat memakan waktu beberapa menit untuk selesai (terkadang hingga 24 jam). Anda mungkin merasa lebih efisien untuk membuat snapshot volume sebelum membuat AMI. Dengan begitu, hanya snapshot kecil dan bertahap yang perlu dibuat saat AMI dibuat, dan proses ini selesai lebih cepat (total waktu untuk pembuatan snapshot tetap sama).

5 – AMI #2: AMI Baru

Setelah proses selesai, Anda memiliki AMI baru dan snapshot (snapshot #2) dibuat dari volume root instans. Jika Anda menambahkan volume penyimpanan instans atau volume EBS ke instans, selain volume root, pemetaan perangkat blok untuk AMI baru berisi informasi untuk volume ini.

Amazon EC2 secara otomatis mendaftarkan AMI untuk Anda.

6 – Meluncurkan instans dari AMI baru

Anda dapat menggunakan AMI baru untuk meluncurkan instans.

7 – Instans EC2 #2: Instans baru

Saat Anda meluncurkan instans menggunakan AMI baru, Amazon EC2 membuat volume EBS baru untuk volume root instans menggunakan snapshot. Jika Anda menambahkan volume

penyimpanan instans atau volume EBS saat Anda menyesuaikan instans, pemetaan perangkat blok untuk AMI baru berisi informasi untuk volume ini, dan pemetaan perangkat blok untuk instance yang Anda luncurkan dari AMI baru secara otomatis berisi informasi untuk volume ini. Volume penyimpanan instans yang ditentukan dalam pemetaan perangkat blok untuk instans yang baru adalah volume baru dan tidak berisi data dari volume penyimpanan instans yang Anda gunakan untuk membuat AMI. Data di volume EBS tetap ada. Untuk informasi selengkapnya, lihat Blokir pemetaan perangkat untuk volume di instans Amazon EC2.

Saat membuat instans baru dari AMI yang didukung EBS, Anda harus menginisialisasi volume root dan penyimpanan EBS tambahan sebelum memasukkannya ke tahap produksi. Untuk informasi selengkapnya, lihat Menginisialisasi volume Amazon EBS di Panduan Pengguna Amazon EBS.

Buat AMI dari sebuah instance

Jika Anda memiliki instance yang sudah ada, Anda dapat membuat AMI dari instance ini.

Console

Untuk membuat AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans untuk membuat AMI, lalu pilih Tindakan, Gambar dan templat, Buat gambar.

   > **Tip**
   >
   > Jika opsi ini dinonaktifkan, instans Anda bukan instans yang didukung Amazon EBS.

4. Pada halaman Buat gambar, tentukan informasi berikut:

   a. Untuk Nama gambar, masukkan nama yang unik untuk gambar, hingga 127 karakter.

   b. Untuk Deskripsi gambar, masukkan deskripsi opsional gambar, hingga 255 karakter.

   c. Untuk contoh Reboot, simpan kotak centang yang dipilih (default), atau hapus.

      - Jika instans Reboot dipilih, saat Amazon EC2 membuat AMI baru, instans akan me-reboot instans sehingga dapat mengambil snapshot dari volume yang dilampirkan saat data dalam keadaan diam, untuk memastikan status yang konsisten.

- Jika instans Reboot dihapus, saat Amazon EC2 membuat AMI baru, instans tidak mematikan dan mem-boot ulang instance.

> **Warning**
>
> Jika Anda menghapus instance Reboot, kami tidak dapat menjamin integritas sistem file dari gambar yang dibuat.

d. Volume instans – Anda dapat memodifikasi volume root, dan menambahkan Amazon EBS tambahan serta volume penyimpanan instans, sebagai berikut:

   i. Volume root ditentukan dalam baris pertama.

      - Untuk mengubah ukuran volume root, untuk Ukuran, masukkan nilai yang diperlukan.
      - Jika Anda memilih Hapus saat pengakhiran, saat Anda mengakhiri instans yang dibuat dari AMI ini, volume EBS akan dihapus. Jika Anda mengosongkan Hapus saat pengakhiran, saat Anda mengakhiri instans, volume EBS tidak dihapus. Untuk informasi selengkapnya, lihat Pertahankan data saat instans diakhiri.

   ii. Untuk menambahkan volume EBS, pilih Tambahkan Volume (yang akan menambahkan baris baru). Untuk Tipe Penyimpanan, pilih EBS, dan isi bidang dalam baris. Saat Anda meluncurkan instans dari AMI baru, volume tambahan ini secara otomatis dilampirkan ke instans. Volume kosong harus diformat dan dipasang. Volume berdasarkan snapshot harus dipasang.

   iii. Untuk menambahkan volume penyimpanan instans, lihat Tambahkan volume penyimpanan instans ke Amazon EC2 AMI. Saat Anda meluncurkan instans dari AMI baru, volume tambahan ini secara otomatis diinisialisasi dan dipasang. Volume ini tidak berisi data dari volume penyimpanan instans pada instans berjalan yang Anda gunakan untuk membuat AMI.

e. Tujuan snapshot - Jika volume instans Anda berada di Zona Lokal yang mendukung snapshot lokal EBS, pilih tempat untuk membuat snapshot AMI:

   - AWS Region: Buat snapshot di Wilayah induk Zona Lokal volume Anda.
   - AWS Zona Lokal: Buat snapshot di Zona Lokal yang sama dengan volume Anda.

> **Note**
>
> Opsi ini hanya muncul di Local Zones yang mendukung snapshot lokal EBS, dan hanya jika instance Anda dibuat di Zona Lokal. Jika volume berada di Wilayah, opsi ini tidak muncul, dan snapshot secara otomatis dibuat di Wilayah yang sama dengan volume. Untuk informasi selengkapnya, lihat Snapshot lokal di Local Zones di Panduan Pengguna Amazon EBS.

> **Important**
>
> Semua snapshot dari volume instance harus berada di lokasi yang sama. Verifikasi lokasi snapshot yang ada. Jika ada snapshot yang ada di lokasi yang berbeda dari tujuan yang Anda pilih, pembuatan AMI akan gagal.

f. Tag – Anda dapat menandai AMI dan snapshot dengan tag yang sama, atau Anda dapat menandai keduanya dengan tag yang berbeda.

- Untuk menandai AMI dan snapshot dengan tag yang sama, pilih Tag gambar dan snapshot bersama-sama. Tag yang sama akan diterapkan pada AMI dan setiap snapshot yang dibuat.
- Untuk menandai AMI dan snapshot dengan tanda yang berbeda, pilih Tag gambar dan snapshot secara terpisah. Tag yang berbeda akan diterapkan pada AMI dan setiap snapshot yang dibuat. Namun, semua snapshot mendapatkan tag yang sama; Anda tidak dapat menandai setiap snapshot dengan tag yang berbeda.

Untuk menambahkan tag , pilih Tambahkan tag dan masukkan kunci dan nilai tag. Ulangi hal itu untuk setiap tanda.

g. Saat Anda siap membuat AMI, pilih Buat gambar.

5. Untuk melihat status AMI Anda saat sedang dibuat:

a. Di panel navigasi, pilih AMIs.

b. Atur filter ke Dimiliki oleh saya, dan cari AMI Anda dalam daftar.

Awalnya, statusnya adalah `pending` namun akan berubah menjadi `available` setelah beberapa menit.

6. (Opsional) Untuk melihat snapshot yang dibuat untuk AMI baru:

   a. Perhatikan ID AMI Anda di langkah sebelumnya.

   b. Di panel navigasi, pilih Snapshot.

   c. Atur filter ke Dimiliki oleh saya, lalu cari snapshot dengan ID AMI baru di kolom Deskripsi.

      Saat Anda meluncurkan instance dari AMI ini, Amazon EC2 menggunakan snapshot ini untuk membuat volume root instans.

AWS CLI

Untuk membuat AMI

Gunakan perintah create-image.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "my-web-server" \
    --description "My web server image" \
    --no-reboot
```

PowerShell

Untuk membuat AMI

Gunakan New-EC2Imagecmdlet.

```
New-EC2Image `
    -InstanceId i-1234567890abcdef0 `
    -Name "my-web-server" `
    -Description "My web server image" `
    -NoReboot $true
```

Buat AMI dari snapshot

Jika Anda memiliki snapshot volume root dari sebuah instance, Anda dapat membuat AMI dari snapshot ini.

> **Note**
>
> Dalam kebanyakan kasus, AMIs untuk Windows, Red Hat, SUSE, dan SQL Server memerlukan informasi lisensi yang benar untuk hadir di AMI. Untuk informasi selengkapnya, lihat Memahami informasi penagihan AMI. Saat membuat AMI dari snapshot, `RegisterImage` operasi memperoleh informasi penagihan yang benar dari metadata snapshot, tetapi ini memerlukan metadata yang sesuai untuk hadir. Untuk memverifikasi apakah informasi penagihan yang benar diterapkan, periksa bidang Detail Platform pada AMI baru. Jika bidang kosong atau tidak cocok dengan kode sistem operasi yang diharapkan (misalnya, Windows, Red Hat, SUSE, atau SQL), pembuatan AMI tidak berhasil, dan Anda harus membuang AMI dan mengikuti instruksi di. Buat AMI dari sebuah instance

Console

Untuk membuat AMI dari snapshot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Snapshot.
3. Pilih snapshot untuk membuat AMI, lalu pilih Tindakan, Buat gambar dari snapshot.
4. Pada halaman Buat gambar dari snapshot, tentukan informasi berikut:
   a. Untuk Nama gambar, masukkan nama deskriptif untuk gambar tersebut.
   b. Untuk Deskripsi, masukkan deskripsi singkat untuk gambar tersebut.
   c. Untuk Arsitektur, pilih arsitektur gambar. Pilih i386 untuk 32-bit, x86_64 untuk 64-bit, arm64 untuk ARM 64-bit, atau x86_64 untuk macOS 64-bit.
   d. Untuk nama perangkat Root, masukkan nama perangkat yang akan digunakan untuk volume root. Untuk informasi selengkapnya, lihat Nama perangkat untuk volume di EC2 instans Amazon.
   e. Untuk Tipe virtualisasi, pilih tipe virtualisasi yang akan digunakan oleh instans yang diluncurkan dari AMI ini. Untuk informasi selengkapnya, lihat Tipe virtualisasi.

f. (Hanya untuk virtualisasi paravirtual) Untuk ID Kernel, pilih kernel sistem operasi untuk gambar tersebut. Jika Anda menggunakan snapshot dari volume root sebuah instance, pilih ID kernel yang sama dengan instance aslinya. Jika Anda tidak yakin, gunakan kernel default.

g. (Hanya untuk virtualisasi paravirtual) Untuk ID disk RAM, pilih disk RAM untuk gambar tersebut. Jika Anda memilih kernel tertentu, Anda mungkin perlu memilih RAM disk tertentu dengan driver yang mendukungnya.

h. Untuk mode Boot, pilih mode boot untuk gambar, atau pilih Use default sehingga ketika instance diluncurkan dengan AMI ini, boot dengan mode boot yang didukung oleh jenis instance. Untuk informasi selengkapnya, lihat Mengatur mode boot Amazon EC2 AMI.

i. (Opsional) Di bawah Blokir pemetaan perangkat, sesuaikan volume root dan tambahkan volume data tambahan.

   Untuk setiap volume, Anda dapat menentukan ukuran, tipe, karakteristik performa, perilaku penghapusan saat pengakhiran, dan status enkripsi. Untuk volume root, ukurannya tidak bisa lebih kecil dari ukuran snapshot. Untuk tipe volume, General Purpose SSD `gp3` adalah pilihan default.

j. (Opsional) Di bawah Tag, Anda dapat menambahkan satu atau beberapa tag ke AMI baru. Untuk menambahkan tag , pilih Tambahkan tag dan masukkan kunci dan nilai tag. Ulangi hal itu untuk setiap tanda.

k. Saat Anda siap membuat AMI, pilih Buat gambar.

5. (Hanya Windows, Red Hat, SUSE, dan SQL Server) Untuk memverifikasi apakah informasi penagihan yang benar diterapkan, periksa bidang Detail Platform pada AMI baru. Jika bidang kosong atau tidak cocok dengan kode sistem operasi yang diharapkan (misalnya, Windows atau Red Hat), pembuatan AMI tidak berhasil, dan Anda harus membuang AMI dan mengikuti instruksi di. Buat AMI dari sebuah instance

AWS CLI

Untuk membuat AMI dari snapshot menggunakan AWS CLI

Gunakan perintah register-image.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
```

```
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0db2cf683925d191f}
```

PowerShell

Untuk membuat AMI dari snapshot menggunakan PowerShell

Gunakan Register-EC2Imagecmdlet.

```
$block = @{SnapshotId=snap-0db2cf683925d191f}
Register-EC2Image `
    -Name my-image `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block}
```

Buat AMI yang didukung Amazon S3

AMI yang Anda tentukan saat meluncurkan instans menentukan jenis volume root.

Untuk membuat AMI Linux yang didukung Amazon S3, mulailah dari instance yang telah Anda luncurkan dari AMI Linux yang didukung Amazon S3 yang sudah ada. Setelah Anda mengustomisasi instans sesuai kebutuhan, paketkan dan daftarkan AMI baru tersebut, yang dapat Anda gunakan untuk meluncurkan instans baru dengan kustomisasi ini.

Anda tidak dapat membuat AMI Windows yang didukung Amazon S3 karena Windows AMIs tidak mendukung penyimpanan instance untuk volume root.

> **Important**
>
> Hanya jenis instance berikut yang mendukung volume penyimpanan instans sebagai volume root dan memerlukan AMI yang didukung Amazon S3: C1, C3, D2, I2, M1, M2, M3, R3, dan X1.

Proses pembuatan AMI berbeda untuk Amazon EBS yang didukung AMIs. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.

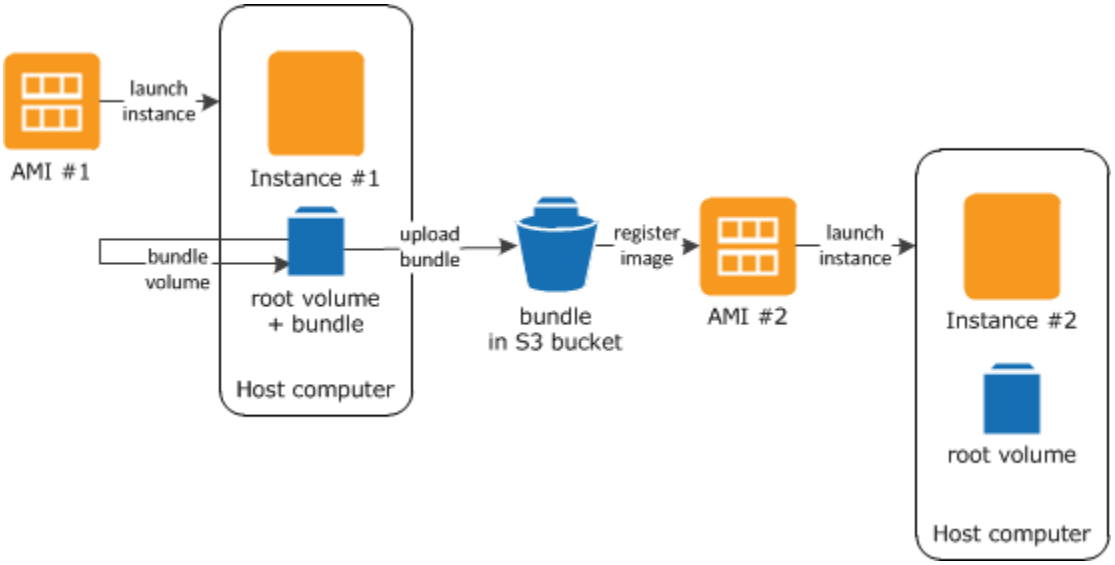
Daftar Isi

- Ikhtisar penciptaan AMI

- Prasyarat
- Buat AMI dari instans Amazon Linux
- Siapkan alat Amazon EC2 AMI
- Referensi alat Amazon EC2 AMI
- Konversikan AMI yang didukung Amazon S3 Anda ke AMI yang didukung EBS

Ikhtisar penciptaan AMI

Diagram berikut merangkum proses pembuatan AMI dari sebuah instance dengan volume root penyimpanan instance.



Pertama, luncurkan instans dari AMI yang serupa dengan AMI yang ingin Anda buat. Anda dapat menyambungkan ke instans dan mengustomisasikannya. Saat instans diatur sesuai keinginan, Anda dapat membuat paketan. Perlu beberapa menit untuk menyelesaikan proses pembuatan paket. Setelah proses selesai, Anda akan memiliki paketan, yang terdiri atas manifes gambar (`image.manifest.xml`) dan file (`image.part.xx`) yang berisi templat untuk volume root. Berikutnya, Anda mengunggah paketan tersebut ke bucket Amazon S3 kemudian mendaftarkan AMI Anda.

> **Note**
>
> Untuk mengunggah objek ke bucket S3 untuk AMI Linux yang didukung Amazon S3, ACL harus diaktifkan untuk bucket. Jika tidak, Amazon EC2 tidak akan dapat mengatur ACLs objek yang akan diunggah. Jika bucket tujuan Anda menggunakan setelan yang diberlakukan pemilik bucket untuk Kepemilikan Objek S3, ini tidak akan berfungsi karena

ACLs dinonaktifkan. Untuk informasi selengkapnya, lihat Mengontrol kepemilikan objek dan menonaktifkan bucket ACLs Anda.

Saat Anda meluncurkan instans menggunakan AMI yang baru, kami membuat volume root untuk instans tersebut menggunakan paketan yang Anda unggah ke Amazon S3. Ruang penyimpanan yang digunakan oleh paketan di Amazon S3 akan menimbulkan biaya sampai Anda menghapusnya. Untuk informasi selengkapnya, lihat Membatalkan pendaftaran ke Amazon EC2 AMI.

Jika Anda menambahkan volume penyimpanan instans ke instans Anda selain volume root, pemetaan perangkat blok untuk AMI baru berisi informasi untuk volume ini, dan pemetaan perangkat blok untuk instance yang Anda luncurkan dari AMI baru secara otomatis berisi informasi untuk volume ini. Untuk informasi selengkapnya, lihat Blokir pemetaan perangkat untuk volume di instans Amazon EC2.

Prasyarat

Sebelum dapat membuat AMI, Anda harus menyelesaikan tugas berikut:

- Menginstal alat AMI. Untuk informasi selengkapnya, lihat Siapkan alat Amazon EC2 AMI.
- Instal AWS CLI. Untuk informasi selengkapnya, lihat Memulai dengan AWS CLI.
- Pastikan Anda memiliki bucket S3 untuk bundel, dan bucket Anda telah ACLs diaktifkan. Untuk informasi selengkapnya tentang mengonfigurasi ACLs, lihat Mengkonfigurasi ACLs.
  - Untuk membuat bucket S3 menggunakan Konsol Manajemen AWS, buka konsol Amazon S3 https://console.aws.amazon.com/s3/di dan pilih Create Bucket.
  - Untuk membuat bucket S3 dengan AWS CLI, Anda dapat menggunakan perintah mb. Jika versi alat AMI yang terinstal adalah 1.5.18 atau yang lebih baru, Anda juga dapat menggunakan perintah `ec2-upload-bundle` untuk membuat bucket S3. Untuk informasi selengkapnya, lihat ec2-upload-bundle.
- Pastikan file dalam bundel Anda tidak dienkripsi di bucket S3. Jika Anda memerlukan enkripsi untuk AMI Anda, Anda dapat menggunakan AMI yang didukung EBS sebagai gantinya. Untuk informasi selengkapnya, lihat Gunakan enkripsi dengan dukungan EBS AMIs.
- Pastikan Anda memiliki ID AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Akun AWS pengenal di Panduan Referensi Manajemen AWS Akun.
- Pastikan Anda memiliki kredensial untuk menggunakan AWS CLI. Untuk informasi selengkapnya, lihat Authentication and access credentials for the AWS CLI in the User Guide.AWS Command Line Interface

- Pastikan Anda memiliki sertifikat X.509 dan kunci privat yang sesuai.
  - Jika Anda perlu membuat sertifikat X.509, lihat Mengelola sertifikat penandatanganan. Sertifikat X.509 dan kunci privat digunakan untuk mengenkripsi dan mendekripsi AMI Anda.
  - [Tiongkok (Beijing)] Gunakan sertifikat `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.
  - [AWS GovCloud (AS-Barat)] Gunakan `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` sertifikat.
- Sambungkan ke instans Anda dan kustomisasikan. Misalnya, Anda dapat menginstal perangkat lunak dan aplikasi, menyalin data, menghapus file sementara, dan mengubah konfigurasi Linux.

Buat AMI dari instans Amazon Linux

Prosedur berikut menjelaskan cara membuat AMI dari instance dengan volume root penyimpanan instance yang menjalankan Amazon Linux 1. Mereka mungkin tidak berfungsi untuk instance yang menjalankan distribusi Linux lainnya.

Untuk mempersiapkan penggunaan alat AMI (khusus instans HVM)

1. Alat AMI memerlukan GRUB Legacy untuk melakukan boot dengan benar. Gunakan perintah berikut untuk menginstal GRUB:

   ```
   [ec2-user ~]$ sudo yum install -y grub
   ```

2. Instal paket manajemen partisi dengan perintah berikut:

   ```
   [ec2-user ~]$ sudo yum install -y gdisk kpartx parted
   ```

Untuk membuat AMI dari instans Amazon Linux dengan volume root penyimpanan instance

Prosedur ini mengasumsikan bahwa Anda telah memenuhi prasyarat dalam Prasyarat.

Dalam perintah berikut, ganti masing-masing *`user input placeholder`* dengan informasi Anda sendiri.

1. Unggah kredensial Anda ke instans. Kami menggunakan kredensial ini untuk memastikan hanya Anda dan Amazon EC2 yang dapat mengakses AMI.

   a. Buat direktori sementara pada instans untuk kredensial Anda sebagai berikut:

```
[ec2-user ~]$ mkdir /tmp/cert
```

Ini memungkinkan Anda mengecualikan kredensial Anda dari gambar yang dibuat.

b. Salin sertifikat X.509 dan kunci privat terkait dari komputer Anda ke direktori `/tmp/cert` pada instans dengan alat penyalin aman, seperti scp. Opsi `-i` *`my-private-key`*`.pem` dalam perintah scp berikut adalah kunci privat yang Anda gunakan untuk terhubung ke instan Anda dengan SSH, bukan kunci privat X.509. Sebagai contoh:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
```

Atau, karena ini adalah file teks biasa, Anda dapat membuka sertifikat dan mengetikannya dalam editor teks dan menyalin kontennya ke dalam file baru di `/tmp/cert`.

2. Siapkan paketan untuk diunggah ke Amazon S3 dengan menjalankan perintah ec2-bundle-vol dari dalam instans Anda. Pastikan untuk menentukan opsi `-e` untuk mengecualikan direktori tempat kredensial Anda disimpan. Secara default, proses paketan mengecualikan file yang mungkin berisi informasi sensitif. File ini termasuk `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys`, dan `*/.bash_history`. Untuk menyertakan semua file ini, gunakan opsi `--no-filter`. Untuk menyertakan beberapa file ini, gunakan opsi `--include`.

> **Important**
>
> Secara default, proses pembuatan paketan AMI membuat koleksi file yang dikompresi dan dienkripsi di direktori `/tmp` yang mewakili volume root Anda. Jika tidak memiliki cukup ruang disk di `/tmp` untuk menyimpan paketan, Anda perlu menentukan lokasi berbeda untuk paketan yang akan disimpan dengan opsi `-d` *`/path/to/bundle/storage`*. Beberapa instance memiliki penyimpanan sementara yang terpasang pada `/mnt` atau `/media/ephemeral0` yang dapat Anda gunakan, atau Anda juga dapat membuat, melampirkan, dan memasang volume Amazon EBS baru) untuk menyimpan

bundel. Untuk informasi selengkapnya, lihat Membuat volume Amazon EBS di Panduan Pengguna Amazon EBS.

a. Anda harus menjalankan perintah ec2-bundle-vol sebagai root. Untuk sebagian besar perintah, Anda dapat menggunakan sudo untuk mendapatkan izin yang lebih tinggi, tetapi dalam kasus ini, Anda harus menjalankan sudo -E su untuk menjaga variabel lingkungan Anda.

```
[ec2-user ~]$ sudo -E su
```

Perhatikan bahwa perintah bash kini mengidentifikasi Anda sebagai pengguna root, dan bahwa tanda dolar telah diganti dengan tanda pagar, menandakan bahwa Anda berada dalam shell root:

```
[root ec2-user]#
```

b. Untuk membuat paketan AMI, jalankan perintah ec2-bundle-vol sebagai berikut:

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

> **Note**
>
> Untuk Wilayah Tiongkok (Beijing) AWS GovCloud dan (AS-Barat), gunakan `--ec2cert` parameter dan tentukan sertifikat sesuai prasyarat.

Perlu waktu beberapa menit untuk membuat gambar. Ketika perintah ini selesai, direktori Anda `/tmp` (atau non-default) berisi bundel (`image.manifest.xml`, ditambah beberapa `image.part.` *xx* file).

c. Keluar dari shell root.

```
[root ec2-user]# exit
```

3. (Opsional) Untuk menambahkan volume penyimpanan instans, edit pemetaan perangkat blok dalam file `image.manifest.xml` untuk AMI Anda. Untuk informasi selengkapnya, lihat Blokir pemetaan perangkat untuk volume di instans Amazon EC2.

   a. Membuat cadangan file `image.manifest.xml` Anda.

   ```
   [ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
   ```

   b. Format ulang file `image.manifest.xml` agar lebih mudah dibaca dan diubah.

   ```
   [ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
   image.manifest.xml
   ```

   c. Edit pemetaan perangkat blok di `image.manifest.xml` editor teks. Contoh di bawah ini menunjukkan entri baru untuk volume penyimpanan instans `ephemeral1`.

   > **Note**
   >
   > Untuk daftar file yang dikecualikan, lihat ec2-bundle-vol.

   ```
   <block_device_mapping>
     <mapping>
       <virtual>ami</virtual>
       <device>sda</device>
     </mapping>
     <mapping>
       <virtual>ephemeral0</virtual>
       <device>sdb</device>
     </mapping>
     <mapping>
       <virtual>ephemeral1</virtual>
       <device>sdc</device>
     </mapping>
     <mapping>
       <virtual>root</virtual>
       <device>/dev/sda1</device>
     </mapping>
   </block_device_mapping>
   ```

   d. Simpan file `image.manifest.xml`, dan tutup editor teks Anda.

4. Untuk mengunggah paketan Anda ke Amazon S3, jalankan perintah ec2-upload-bundle sebagai berikut.

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name -
m /tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Untuk mendaftarkan AMI Anda di Wilayah selain AS Timur (Virginia Utara), Anda harus menentukan Wilayah target dengan opsi `--region` dan jalur bucket yang sudah ada di Wilayah target atau jalur bucket unik yang dapat dibuat di Wilayah target.

5. (Opsional) Setelah bundel diunggah ke Amazon S3, Anda dapat menghapus bundel dari direktori `/tmp` pada instans menggunakan perintah rm berikut:

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Jika Anda menentukan jalur dengan opsi `-d /path/to/bundle/storage` di Step 2, gunakan jalur tersebut, alih-alih `/tmp`.

6. Untuk mendaftarkan AMI Anda, jalankan perintah register-image sebagai berikut.

```
[ec2-user ~]$ aws ec2 register-image --image-location amzn-s3-demo-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Jika sebelumnya Anda menentukan Wilayah untuk perintah ec2-upload-bundle, tentukan Wilayah itu untuk perintah ini.

Siapkan alat Amazon EC2 AMI

Anda dapat menggunakan alat AMI untuk membuat dan mengelola Linux yang didukung Amazon S3. AMIs Untuk menggunakan alat ini, Anda harus menginstalnya di instans Linux Anda. Alat AMI tersedia baik sebagai RPM dan sebagai file .zip untuk distribusi Linux yang tidak mendukung RPM.

Untuk menyiapkan alat AMI menggunakan RPM

1. Instal Ruby menggunakan manajer paket untuk distribusi Linux Anda, seperti yum. Sebagai contoh:

   ```
   [ec2-user ~]$ sudo yum install -y ruby
   ```

2. Unduh file RPM menggunakan alat seperti wget atau curl. Sebagai contoh:

   ```
   [ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
   ```

3. Verifikasikan tanda tangan file RPM menggunakan perintah berikut:

   ```
   [ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
   ```

   Perintah di atas harus menunjukkan bahwa file SHA1 dan MD5 hash adalah OK. Jika perintah menunjukkan bahwa hash tersebutNOT OK, gunakan perintah berikut untuk melihat Header SHA1 dan MD5 hash file:

   ```
   [ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
   ```

   Kemudian, bandingkan Header SHA1 dan MD5 hash file Anda dengan hash alat AMI terverifikasi berikut untuk mengonfirmasi keaslian file:

   - Tajuk SHA1: a1f662d6f25f69871104e6a62187fa4df508f880
   - MD5: 9faff05258064e2f7909b66142de6782

   Jika Header SHA1 dan MD5 hash file Anda cocok dengan hash alat AMI yang diverifikasi, lanjutkan ke langkah berikutnya.

4. Instal RPM menggunakan perintah berikut:

   ```
   [ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
   ```

5. Verifikasi instalasi alat AMI Anda menggunakan perintah ec2- ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

> **Note**
>
> Jika Anda menerima kesalahan pemuatan seperti “tidak dapat memuat file tersebut -- ec2/amitools/version (LoadError)”, selesaikan langkah berikutnya untuk menambahkan lokasi instalasi alat AMI Anda ke jalur Anda. RUBYLIB

6. (Opsional) Jika Anda menerima kesalahan pada langkah sebelumnya, tambahkan lokasi instalasi alat AMI Anda ke jalur RUBYLIB.

   a. Jalankan perintah berikut untuk menentukan jalur yang akan ditambahkan.

```
[ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
/usr/lib/ruby/site_ruby/ec2/amitools/version.rb
/usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
```

   Dalam contoh di atas, file yang hilang dari kesalahan pemuatan sebelumnya berada di /usr/lib/ruby/site_ruby dan /usr/lib64/ruby/site_ruby.

   b. Tambahkan lokasi dari langkah sebelumnya ke jalur RUBYLIB Anda.

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/
site_ruby
```

   c. Verifikasi instalasi alat AMI Anda menggunakan perintah ec2- ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Untuk menyiapkan alat AMI menggunakan file .zip

1. Instal Ruby dan bongkar file .zip menggunakan pengelola paket untuk distribusi Linux Anda, seperti apt-get. Sebagai contoh:

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. Unduh file .zip menggunakan alat seperti wget atau curl. Sebagai contoh:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Bongkar file .zip ke dalam direktori instalasi yang sesuai, seperti `/usr/local/ec2`.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

Perhatikan bahwa file.zip berisi folder ec2-ami-tools-. *x x*. *x*, dimana*x*. *x*. *x*adalah nomor versi alat (misalnya,`ec2-ami-tools-1.5.7`).

4. Atur variabel lingkungan `EC2_AMITOOL_HOME` untuk direktori instalasi alat. Sebagai contoh:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Tambahkan alat ke variabel lingkungan `PATH` Anda. Sebagai contoh:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. Anda dapat memverifikasi instalasi alat AMI Anda menggunakan perintah ec2- ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Mengelola sertifikat penandatanganan

Perintah tertentu di alat AMI memerlukan penandatanganan sertifikat (juga dikenal sebagai sertifikat X.509). Anda harus membuat sertifikat dan kemudian mengunggahnya ke AWS. Misalnya, Anda dapat menggunakan alat pihak ketiga, seperti OpenSSL untuk membuat sertifikat.

Untuk membuat sertifikat tanda tangan

1. Instal dan konfigurasi OpenSSL.
2. Buat kunci privat menggunakan perintah `openssl genrsa` dan simpan output-nya ke file `.pem`. Kami sarankan Anda membuat kunci RSA 2048- atau 4096-bit.

```
openssl genrsa 2048 > private-key.pem
```

3. Munculkan sertifikat menggunakan perintah `openssl req`.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
out certificate.pem
```

Untuk mengunggah sertifikat ke AWS, gunakan upload-signing-certificateperintah.

```
aws iam upload-signing-certificate --user-name user-name --certificate-body
 file://path/to/certificate.pem
```

Untuk membuat daftar sertifikat untuk pengguna, gunakan list-signing-certificatesperintah:

```
aws iam list-signing-certificates --user-name user-name
```

Untuk menonaktifkan atau mengaktifkan kembali sertifikat penandatanganan untuk pengguna, gunakan update-signing-certificateperintah. Perintah berikut ini menonaktifkan sertifikat:

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --
status Inactive --user-name user-name
```

Untuk menghapus sertifikat, gunakan delete-signing-certificateperintah:

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

Referensi alat Amazon EC2 AMI

Anda dapat menggunakan perintah alat AMI untuk membuat dan mengelola Linux yang didukung Amazon S3. AMIs Untuk menyiapkan alat, lihat Siapkan alat Amazon EC2 AMI.

Untuk informasi tentang kunci akses Anda, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Commands

- ec2- ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle

- ec2-download-bundle
- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Opsi umum untuk alat AMI

ec2- ami-tools-version

Deskripsi

Menjelaskan versi alat AMI.

Sintaksis

ec2-ami-tools-version

Output

Informasi versi.

Contoh

Perintah contoh ini menampilkan informasi versi untuk alat AMI yang Anda gunakan.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

Deskripsi

Membuat AMI Linux yang didukung Amazon S3 dari image sistem operasi yang dibuat dalam file loopback.

Sintaksis

ec2-bundle-image -c *path* -k *path* -u *account* -i *path* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [-p *prefix*]

Opsi

jalur `-c, --cert`

File sertifikat kunci publik RSA yang dienkode PEM.

Wajib: Ya

jalur `-k, --privatekey`

Jalur menuju file kunci RSA yang dienkode PEM. Anda akan perlu menentukan kunci ini untuk membuka paketan ini, jadi simpanlah di tempat yang aman. Perhatikan bahwa kunci tidak harus didaftarkan ke AWS akun Anda.

Wajib: Ya

akun `-u, --user`

ID AWS akun pengguna, tanpa tanda hubung.

Wajib: Ya

jalur `-i, --image`

Jalur ke gambar yang akan dipaketkan.

Wajib: Ya

jalur `-d, --destination`

Direktori untuk membuat paketan.

Default: `/tmp`

Wajib: Tidak

jalur `--ec2cert`

Jalur ke sertifikat kunci publik Amazon EC2 X.509 digunakan untuk mengenkripsi manifes gambar.

Wilayah `us-gov-west-1` dan `cn-north-1` menggunakan sertifikat kunci publik non-default dan jalur ke sertifikat tersebut harus ditetapkan dengan opsi ini. Jalur ke sertifikat berbeda-beda tergantung metode instalasi alat AMI. Untuk Amazon Linux, sertifikat terletak di `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Jika Anda menginstal alat AMI dari file RPM atau

ZIP di Siapkan alat Amazon EC2 AMI, sertifikat berada di `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Wajib: Hanya untuk Wilayah `us-gov-west-1` dan `cn-north-1`.

arsitektur `-r, --arch`

Arsitektur gambar. Jika Anda tidak memberikan arsitektur pada baris perintah, Anda akan diminta memberikannya saat pembuatan paketan dimulai.

Nilai yang valid: `i386` | `x86_64`

Wajib: Tidak

kode1,kode2,... `--productcodes`

Kode produk yang dilampirkan ke gambar pada waktu pendaftaran, dipisahkan dengan koma.

Wajib: Tidak

pemetaan `-B, --block-device-mapping`

Menentukan bagaimana perangkat blok terpapar ke instans AMI ini jika tipe instans mendukung perangkat yang ditentukan.

Tentukan daftar pasangan kunci-nilai yang dipisahkan koma, di mana setiap kunci adalah nama virtual dan setiap nilai adalah nama perangkat yang terkait. Nama virtual mencakup hal berikut:

- `ami`—Perangkat sistem file root, seperti yang terlihat oleh instans
- `root`—Perangkat sistem file root, seperti yang terlihat oleh kernel
- `swap`—Perangkat pertukaran, seperti yang terlihat oleh instans
- `ephemeralN`—Volume penyimpanan instans ke-N

Wajib: Tidak

awalan `-p, --prefix`

Awalan nama file untuk file AMI yang dipaketkan.

Default: Nama file gambar. Misalnya, jika jalur gambar adalah `/var/spool/my-image/version-2/debian.img`, awalan default-nya adalah `debian.img`.

Wajib: Tidak

kernel_id `--kernel`

Tidak lagi digunakan. Gunakan register-image untuk mengatur kernel.

Wajib: Tidak

ramdisk_id `--ramdisk`

Tidak lagi digunakan. Gunakan register-image untuk mengatur disk RAM jika diperlukan.

Wajib: Tidak

Output

Pesan status yang menjelaskan tahap dan status proses pembuatan paketan.

Contoh

Contoh ini membuat paketan AMI dari gambar sistem operasi yang dibuat dalam file loopback.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
```

```
ec2-bundle-image complete.
```

ec2-bundle-vol

Deskripsi

Membuat AMI Linux yang didukung Amazon S3 dengan mengompresi, mengenkripsi, dan menandatangani salinan volume root untuk instance.

Amazon EC2 mencoba mewarisi kode produk, pengaturan kernel, pengaturan disk RAM, dan memblokir pemetaan perangkat dari instance.

Secara default, proses paketan mengecualikan file yang mungkin berisi informasi sensitif. File ini termasuk `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys`, dan `*/.bash_history`. Untuk menyertakan semua file ini, gunakan opsi `--no-filter`. Untuk menyertakan beberapa file ini, gunakan opsi `--include`.

Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon S3.

Sintaksis

ec2-bundle-vol -c *path* -k *path* -u *account* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [--all] [-e *directory1*,*directory2*,...] [-i *file1*,*file2*,...] [--no-filter] [-p *prefix*] [-s *size*] [--[no-]inherit] [-v *volume*] [-P *type*] [-S *script*] [--fstab *path*] [--generate-fstab] [--grub-config *path*]

Opsi

jalur `-c, --cert`

File sertifikat kunci publik RSA yang dienkode PEM.

Wajib: Ya

jalur `-k, --privatekey`

Jalur menuju file kunci RSA yang dienkode PEM milik pengguna.

Wajib: Ya

akun `-u, --user`

ID AWS akun pengguna, tanpa tanda hubung.

Wajib: Ya

tujuan `-d, --destination`

Direktori untuk membuat paketan.

Default: `/tmp`

Wajib: Tidak

jalur `--ec2cert`

Jalur ke sertifikat kunci publik Amazon EC2 X.509 digunakan untuk mengenkripsi manifes gambar.

Wilayah `us-gov-west-1` dan `cn-north-1` menggunakan sertifikat kunci publik non-default dan jalur ke sertifikat tersebut harus ditetapkan dengan opsi ini. Jalur ke sertifikat berbeda-beda tergantung metode instalasi alat AMI. Untuk Amazon Linux, sertifikat terletak di `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Jika Anda menginstal alat AMI dari file RPM atau ZIP di Siapkan alat Amazon EC2 AMI, sertifikat berada di `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Wajib: Hanya untuk Wilayah `us-gov-west-1` dan `cn-north-1`.

arsitektur `-r, --arch`

Arsitektur gambar. Jika Anda tidak memberikannya pada baris perintah, Anda akan diminta untuk memberikannya saat pembuatan paketan dimulai.

Nilai yang valid: `i386` | `x86_64`

Wajib: Tidak

kode1,kode2,... `--productcodes`

Kode produk yang dilampirkan ke gambar pada waktu pendaftaran, dipisahkan dengan koma.

Wajib: Tidak

pemetaan `-B, --block-device-mapping`

Menentukan bagaimana perangkat blok terpapar ke instans AMI ini jika tipe instans mendukung perangkat yang ditentukan.

Tentukan daftar pasangan kunci-nilai yang dipisahkan koma, di mana setiap kunci adalah nama virtual dan setiap nilai adalah nama perangkat yang terkait. Nama virtual mencakup hal berikut:

- `ami`—Perangkat sistem file root, seperti yang terlihat oleh instans
- `root`—Perangkat sistem file root, seperti yang terlihat oleh kernel
- `swap`—Perangkat pertukaran, seperti yang terlihat oleh instans
- `ephemeralN`—Volume penyimpanan instans ke-N

Wajib: Tidak

`-a, --all`

Membuat paketan semua direktori, termasuk yang ada di sistem file yang dipasang dari jauh.

Wajib: Tidak

direktori1,direktori2,... `-e, --exclude`

Daftar jalur dan file direktori mutlak yang akan dikecualikan dari operasi paketan. Parameter ini menimpa opsi `--all`. Jika ada pengecualian, direktori dan subdirektori yang tercantum dengan parameter tidak akan dipaketkan dengan volume.

Wajib: Tidak

file1,file2,... `-i, --include`

Daftar file yang akan disertakan dalam operasi paketan. File yang ditentukan akan dikecualikan dari AMI karena mungkin mengandung informasi sensitif.

Wajib: Tidak

`--no-filter`

Jika ditentukan, kami tidak akan mengecualikan file dari AMI karena file tersebut mungkin berisi informasi sensitif.

Wajib: Tidak

awalan `-p, --prefix`

Awalan nama file untuk file AMI yang dipaketkan.

Default: `image`

Wajib: Tidak

ukuran `-s, --size`

Ukuran, dalam MB (1024 * 1024 byte), dari file gambar yang akan dibuat. Ukuran maksimalnya adalah 10240 MB.

Default: 10240

Wajib: Tidak

`--[no-]inherit`

Mengindikasikan apakah gambar harus mewarisi metadata instans (default-nya adalah mewarisi). Pembuatan paketan gagal jika Anda mengaktifkan `--inherit`, tetapi metadata instans tidak dapat diakses.

Wajib: Tidak

volume `-v, --volume`

Jalur mutlak ke volume yang dipasang dari tempat untuk membuat paketan.

Default: Direktori root (/)

Wajib: Tidak

tipe `-P, --partition`

Menunjukkan apakah gambar disk harus menggunakan tabel partisi. Jika Anda tidak menentukan tipe tabel partisi, default-nya adalah tipe yang digunakan pada perangkat blok induk volume, jika berlaku. Jika tidak, default-nya adalah `gpt`.

Nilai yang valid: `mbr` | `gpt` | `none`

Wajib: Tidak

skrip `-S, --script`

Skrip kustomisasi akan dijalankan tepat sebelum pembuatan paketan. Skrip harus menantikan satu argumen, titik pemasangan volume.

Wajib: Tidak

jalur `--fstab`

Jalur ke fstab yang akan dipaketkan ke dalam gambar. Jika ini tidak ditentukan, Amazon EC2 bundles /etc/fstab.

Wajib: Tidak

`--generate-fstab`

Bundel volume menggunakan fstab EC2 yang disediakan Amazon.

Wajib: Tidak

`--grub-config`

Jalur menuju file konfigurasi grub alternatif untuk dipaketkan ke dalam gambar. Secara default, `ec2-bundle-vol` menunggu `/boot/grub/menu.lst` atau `/boot/grub/grub.conf` ada pada gambar hasil klona. Opsi ini memungkinkan Anda menentukan jalur ke file konfigurasi grub alternatif, yang kemudian akan disalin menggantikan default (jika ada).

Wajib: Tidak

kernel_id `--kernel`

Tidak lagi digunakan. Gunakan register-image untuk mengatur kernel.

Wajib: Tidak

ramdisk_id`--ramdisk`

Tidak lagi digunakan. Gunakan register-image untuk mengatur disk RAM jika diperlukan.

Wajib: Tidak

Output

Pesan status yang menjelaskan tahap dan status proses pemaketan.

Contoh

Contoh ini membuat AMI paketan dengan mengompresi, mengenkripsi, dan menandatangani snapshot sistem file root mesin lokal.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c
 cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
```

```
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
  1+0 records in
  1+0 records out
  mke2fs 1.38 (30-Jun-2005)
  warning: 256 blocks unused.

  Splitting /mnt/image.gz.crypt...
  Created image.part.00
  Created image.part.01
  Created image.part.02
  Created image.part.03
  ...
  Created image.part.22
  Created image.part.23
  Generating digests for each part...
  Digests generated.
  Creating bundle manifest...
  Bundle Volume complete.
```

ec2-delete-bundle

Deskripsi

Menghapus paketan tertentu dari penyimpanan Amazon S3. Setelah menghapus paketan, Anda tidak dapat meluncurkan instans dari AMI terkait.

Sintaksis

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

Opsi

bucket `-b, --bucket`

Nama bucket Amazon S3 yang berisi paketan AMI, diikuti dengan awalan jalur opsional yang dibatasi '/'

Wajib: Ya

access_key_id `-a, --access-key`

ID kunci AWS akses.

Wajib: Ya

secret_access_key `-s, --secret-key`

Kunci akses AWS rahasia.

Wajib: Ya

token `-t, --delegation-token`

Token delegasi untuk diteruskan ke AWS permintaan. Untuk informasi selengkapnya, lihat Kredensyal keamanan sementara di Panduan Pengguna IAM.

Wajib: Hanya saat Anda menggunakan kredensial keamanan sementara.

Default: Nilai dari variabel lingkungan `AWS_DELEGATION_TOKEN` (jika diatur).

wilayah`--region`

Wilayah yang akan digunakan dalam tanda tangan permintaan.

Default: `us-east-1`

Wajib: Wajib jika menggunakan tanda tangan versi 4

version `--sigv`

Versi tanda tangan yang digunakan ketika menandatangani permintaan.

Nilai yang valid: 2 | 4

Default: 4

Wajib: Tidak

path`-m, --manifest`

Jalur ke file manifes.

Wajib: Anda harus menentukan `--prefix` atau `--manifest`.

awalan `-p, --prefix`

Awalan nama file AMI yang dipaketkan. Berikan seluruh awalan. Misalnya, jika awalannya adalah image.img, gunakan `-p image.img` dan bukan `-p image`.

Wajib: Anda harus menentukan `--prefix` atau `--manifest`.

`--clear`

Menghapus bucket Amazon S3 jika kosong setelah menghapus paketan tertentu.

Wajib: Tidak

`--retry`

Otomatis mencoba ulang semua kesalahan Amazon S3, hingga lima kali per operasi.

Wajib: Tidak

`-y, --yes`

Secara otomatis mengasumsikan jawaban semua permintaan adalah ya.

Wajib: Tidak

Output

Amazon EC2 menampilkan pesan status yang menunjukkan tahapan dan status proses penghapusan.

Contoh

Contoh ini menghapus paketan dari Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b amzn-s3-demo-bucket -a your_access_key_id -
s your_secret_access_key
Deleting files:
```

```
amzn-s3-demo-bucket/image.manifest.xml
amzn-s3-demo-bucket/image.part.00
amzn-s3-demo-bucket/image.part.01
amzn-s3-demo-bucket/image.part.02
amzn-s3-demo-bucket/image.part.03
amzn-s3-demo-bucket/image.part.04
amzn-s3-demo-bucket/image.part.05
amzn-s3-demo-bucket/image.part.06
Continue? [y/n]
y
Deleted amzn-s3-demo-bucket/image.manifest.xml
Deleted amzn-s3-demo-bucket/image.part.00
Deleted amzn-s3-demo-bucket/image.part.01
Deleted amzn-s3-demo-bucket/image.part.02
Deleted amzn-s3-demo-bucket/image.part.03
Deleted amzn-s3-demo-bucket/image.part.04
Deleted amzn-s3-demo-bucket/image.part.05
Deleted amzn-s3-demo-bucket/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Deskripsi

Mengunduh Linux yang didukung Amazon S3 yang ditentukan AMIs dari penyimpanan Amazon S3.

Sintaksis

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

Opsi

bucket `-b, --bucket`

Nama bucket Amazon S3 tempat paketan berada, diikuti dengan awalan jalur opsional yang dibatasi '/'.

Wajib: Ya

access_key_id `-a, --access-key`

ID kunci AWS akses.

Wajib: Ya

secret_access_key `-s, --secret-key`

Kunci akses AWS rahasia.

Wajib: Ya

jalur `-k, --privatekey`

Kunci privat yang digunakan untuk mendekripsi manifes.

Wajib: Ya

url `--url`

URL layanan Amazon S3.

Default: `https://s3.amazonaws.com/`

Wajib: Tidak

wilayah `--region`

Wilayah yang akan digunakan dalam tanda tangan permintaan.

Default: `us-east-1`

Wajib: Wajib jika menggunakan tanda tangan versi 4

versi `--sigv`

Versi tanda tangan yang digunakan ketika menandatangani permintaan.

Nilai yang valid: `2` | `4`

Default: `4`

Wajib: Tidak

file `-m, --manifest`

Nama file manifes (tanpa jalur). Kami sarankan Anda untuk menentukan manifes (`-m`) atau awalan(`-p`).

Wajib: Tidak

awalan `-p, --prefix`

Awalan nama file untuk file AMI yang dipaketkan.

Default: `image`

Wajib: Tidak

direktori `-d, --directory`

Direktori tempat paketan yang diunduh disimpan. Direktori harus ada.

Default: Direktori kerja saat ini.

Wajib: Tidak

`--retry`

Otomatis mencoba ulang semua kesalahan Amazon S3, hingga lima kali per operasi.

Wajib: Tidak

Output

Pesan status yang menunjukkan berbagai tahap proses pengunduhan ditampilkan.

Contoh

Contoh ini membuat direktori `bundled` (menggunakan perintah Linux mkdir) dan mengunduh paketan dari bucket Amazon S3 `amzn-s3-demo-bucket`.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from amzn-s3-demo-bucket to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.00 ...
Downloaded image.part.00 from amzn-s3-demo-bucket
Downloading part image.part.01 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.01 ...
```

```
Downloaded image.part.01 from amzn-s3-demo-bucket
Downloading part image.part.02 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.02 ...
Downloaded image.part.02 from amzn-s3-demo-bucket
Downloading part image.part.03 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.03 ...
Downloaded image.part.03 from amzn-s3-demo-bucket
Downloading part image.part.04 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.04 ...
Downloaded image.part.04 from amzn-s3-demo-bucket
Downloading part image.part.05 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.05 ...
Downloaded image.part.05 from amzn-s3-demo-bucket
Downloading part image.part.06 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.06 ...
Downloaded image.part.06 from amzn-s3-demo-bucket
```

ec2-migrate-manifest

Deskripsi

Memodifikasi AMI Linux yang didukung Amazon S3 (misalnya, sertifikat, kernel, dan disk RAM) sehingga mendukung Wilayah yang berbeda.

Sintaksis

ec2-migrate-manifest -c *path* -k *path* -m *path* {(-a *access_key_id* -s *secret_access_key* --region *region*) | (--no-mapping)} [--ec2cert *ec2_cert_path*] [--kernel *kernel-id*] [--ramdisk *ramdisk_id*]

Opsi

jalur `-c, --cert`

File sertifikat kunci publik RSA yang dienkode PEM.

Wajib: Ya

jalur `-k, --privatekey`

Jalur menuju file kunci RSA yang dienkode PEM milik pengguna.

Wajib: Ya

jalur `--manifest`

Jalur ke file manifes.

Wajib: Ya

access_key_id `-a, --access-key`

ID kunci AWS akses.

Wajib: Wajib jika menggunakan pemetaan otomatis.

secret_access_key `-s, --secret-key`

Kunci akses AWS rahasia.

Wajib: Wajib jika menggunakan pemetaan otomatis.

wilayah `--region`

Wilayah untuk dicari di file pemetaan.

Wajib: Wajib jika menggunakan pemetaan otomatis.

`--no-mapping`

Menonaktifkan pemetaan otomatis kernel dan disk RAM.

Selama migrasi, Amazon EC2 mengganti disk kernel dan RAM dalam file manifes dengan kernel dan disk RAM yang dirancang untuk wilayah tujuan. Kecuali parameter `--no-mapping` diberikan, `ec2-migrate-bundle` dapat menggunakan operasi `DescribeRegions` dan `DescribeImages` untuk melakukan pemetaan otomatis.

Wajib: Wajib jika Anda tidak menyediakan opsi `-a`, `-s`, dan `--region` yang digunakan untuk pemetaan otomatis.

jalur `--ec2cert`

Jalur ke sertifikat kunci publik Amazon EC2 X.509 digunakan untuk mengenkripsi manifes gambar.

Wilayah `us-gov-west-1` dan `cn-north-1` menggunakan sertifikat kunci publik non-default dan jalur ke sertifikat tersebut harus ditetapkan dengan opsi ini. Jalur ke sertifikat berbeda-beda tergantung metode instalasi alat AMI. Untuk Amazon Linux, sertifikat terletak di `/opt/aws/`

`amitools/ec2/etc/ec2/amitools/`. Jika Anda menginstal alat AMI dari file ZIP di Siapkan alat Amazon EC2 AMI, sertifikat berada di `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Wajib: Hanya untuk Wilayah `us-gov-west-1` dan `cn-north-1`.

kernel_id `--kernel`

ID kernel yang akan dipilih.

> **Important**
>
> Kami menyarankan Anda menggunakan PV-GRUB dibandingkan kernel dan disk RAM. Untuk informasi selengkapnya, lihat Kernel yang disediakan pengguna di Panduan Pengguna Amazon Linux 2.

Wajib: Tidak

ramdisk_id `--ramdisk`

ID disk RAM yang akan dipilih.

> **Important**
>
> Kami menyarankan Anda menggunakan PV-GRUB dibandingkan kernel dan disk RAM. Untuk informasi selengkapnya, lihat Kernel yang disediakan pengguna di Panduan Pengguna Amazon Linux 2.

Wajib: Tidak

Output

Pesan status yang menjelaskan tahap dan status proses pembuatan paketan.

Contoh

Contoh ini menyalin AMI yang ditentukan dalam manifes `my-ami.manifest.xml` dari AS ke UE.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
 --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1
```

```
Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Deskripsi

Membuat ulang bundel dari AMI Linux yang didukung Amazon S3.

Sintaksis

ec2-unbundle -k *path* -m *path* [-s *source_directory*] [-d *destination_directory*]

Opsi

jalur `-k, --privatekey`

Jalur menuju file kunci RSA yang dienkode PEM.

Wajib: Ya

jalur `-m, --manifest`

Jalur ke file manifes.

Wajib: Ya

source_directory `-s, --source`

Direktori yang berisi paketan.

Default: Direktori saat ini.

Wajib: Tidak

destination_directory `-d, --destination`

Direktori tempat membongkar paketan AMI. Direktori tujuan harus ada.

Default: Direktori saat ini.

Wajib: Tidak

Contoh

Contoh Linux dan UNIX ini membongkar paketan AMI yang ditentukan dalam file `image.manifest.xml`.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Output

Pesan status yang menunjukkan berbagai tahap proses pembongkaran paketan ditampilkan.

ec2-upload-bundle

Deskripsi

Mengunggah bundel untuk AMI Linux yang didukung Amazon S3 ke Amazon S3 dan menetapkan daftar kontrol akses (ACLs) yang sesuai pada objek yang diunggah. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon S3.

> **Note**
>
> Untuk mengunggah objek ke bucket S3 untuk AMI Linux yang didukung Amazon S3, ACLs harus diaktifkan untuk bucket. Jika tidak, Amazon tidak EC2 akan dapat mengatur ACLs objek yang akan diunggah. Jika bucket tujuan Anda menggunakan setelan yang diberlakukan pemilik bucket untuk Kepemilikan Objek S3, ini tidak akan berfungsi karena ACLs dinonaktifkan. Untuk informasi selengkapnya, lihat Mengontrol kepemilikan objek dan menonaktifkan bucket ACLs Anda.

Sintaksis

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t
token] -m path [--url url] [--region region] [--sigv version] [--acl acl]
[-d directory] [--part part] [--retry] [--skipmanifest]
```

Opsi

bucket `-b, --bucket`

Nama bucket Amazon S3 untuk menyimpan paketan, diikuti dengan awalan jalur opsional yang dibatasi '/'. Jika bucket tidak tersedia, bucket akan dibuat jika namanya tersedia. Selain itu, jika bucket tidak ada dan versi alat AMI adalah 1.5.18 atau yang lebih baru, perintah ini akan ACLs menetapkan bucket.

Wajib: Ya

access_key_id `-a, --access-key`

ID kunci AWS akses Anda.

Wajib: Ya

secret_access_key `-s, --secret-key`

Kunci akses AWS rahasia Anda.

Wajib: Ya

token `-t, --delegation-token`

Token delegasi untuk diteruskan ke AWS permintaan. Untuk informasi selengkapnya, lihat Kredensyal keamanan sementara di Panduan Pengguna IAM.

Wajib: Hanya saat Anda menggunakan kredensial keamanan sementara.

Default: Nilai dari variabel lingkungan `AWS_DELEGATION_TOKEN` (jika diatur).

jalur `-m, --manifest`

Jalur ke file manifes. File manifes dibuat selama proses pembuatan paketan dan dapat ditemukan di direktori yang berisi paketan tersebut.

Wajib: Ya

url `--url`

Tidak lagi digunakan. Gunakan opsi `--region` sebagai gantinya kecuali jika bucket Anda dibatasi ke lokasi `EU` (dan bukan `eu-west-1`). Bendera `--location` adalah satu-satunya cara untuk menarget batasan lokasi tertentu.

URL layanan titik akhir Amazon S3.

Default: `https://s3.amazonaws.com/`

Wajib: Tidak

wilayah `--region`

Wilayah yang akan digunakan dalam tanda tangan permintaan untuk bucket S3 tujuan.

- Jika bucket tidak ada dan Anda tidak menentukan Wilayah, alat akan membuat bucket tanpa batasan lokasi (di `us-east-1`).
- Jika bucket tidak ada dan Anda menentukan Wilayah, alat akan membuat bucket di Wilayah yang ditentukan.
- Jika bucket tersedia dan Anda tidak menentukan Wilayah, alat ini akan menggunakan lokasi bucket.
- Jika bucket tersedia dan Anda menentukan `us-east-1` sebagai Wilayah, alat ini akan menggunakan lokasi aktual bucket tanpa pesan kesalahan apa pun, setiap file yang cocok akan ditimpa.
- Jika bucket tersedia dan Anda menetapkan Wilayah (selain `us-east-1`) yang tidak sesuai dengan lokasi aktual bucket, alat akan keluar dengan kesalahan.

Jika bucket Anda dibatasi ke lokasi `EU` (dan bukan `eu-west-1`), gunakan bendera `--location` sebagai gantinya. Bendera `--location` adalah satu-satunya cara untuk menarget batasan lokasi tertentu.

Default: `us-east-1`

Wajib: Wajib jika menggunakan tanda tangan versi `4`

versi `--sigv`

Versi tanda tangan yang digunakan ketika menandatangani permintaan.

Nilai yang valid: `2` | `4`

Default: `4`

Wajib: Tidak

acl `--acl`

Kebijakan daftar kontrol akses dari gambar yang dipaketkan.

Nilai yang valid: `public-read` | `aws-exec-read`

Default: `aws-exec-read`

Wajib: Tidak

direktori `-d, --directory`

Direktori yang berisi bagian AMI yang dipaketkan.

Default: Direktori yang berisi file manifes (lihat opsi `-m`).

Wajib: Tidak

bagian `--part`

Mulai mengunggah bagian tertentu dan semua bagian berikutnya. Sebagai contoh, `--part 04`.

Wajib: Tidak

`--retry`

Otomatis mencoba ulang semua kesalahan Amazon S3, hingga lima kali per operasi.

Wajib: Tidak

`--skipmanifest`

Tidak mengunggah manifes.

Wajib: Tidak

lokasi `--location`

Tidak lagi digunakan. Gunakan opsi `--region` sebagai gantinya, kecuali jika bucket Anda dibatasi ke lokasi `EU` (dan bukan `eu-west-1`). Bendera `--location` adalah satu-satunya cara untuk menarget batasan lokasi tersebut.

Batasan lokasi tujuan bucket Amazon S3. Jika bucket tersedia dan Anda menetapkan lokasi yang tidak sesuai dengan lokasi aktual bucket, alat akan keluar dengan kesalahan. Jika bucket tersedia dan Anda tidak menentukan lokasi, alat ini akan menggunakan lokasi bucket. Jika bucket tidak tersedia dan Anda menentukan lokasi, alat akan membuat bucket di lokasi yang ditentukan. Jika bucket tidak ada dan Anda tidak menentukan lokasi, alat akan membuat bucket tanpa batasan lokasi (di `us-east-1`).

Default: Jika `--region` ditentukan, lokasi diatur ke Wilayah yang ditentukan. Jika `--region` tidak ditentukan, lokasi secara default menjadi `us-east-1`.

Wajib: Tidak

Output

Amazon EC2 menampilkan pesan status yang menunjukkan tahapan dan status proses unggahan.

Contoh

Contoh ini mengunggah paketan yang ditentukan oleh manifes `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket amzn-s3-demo-bucket ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Opsi umum untuk alat AMI

Sebagian besar alat AMI menerima parameter opsional berikut.

`--help, -h`

Menampilkan pesan bantuan.

`--version`

Menampilkan versi dan pemberitahuan hak cipta.

`--manual`

Menampilkan entri manual.

`--batch`

Berjalan dalam mode batch, menahan perintah interaktif.

`--debug`

Menampilkan informasi yang dapat berguna saat pemecahan masalah.

Konversikan AMI yang didukung Amazon S3 Anda ke AMI yang didukung EBS

Anda dapat mengonversi AMI Linux yang didukung Amazon S3 yang Anda miliki ke AMI Linux yang didukung Amazon EBS.

> **Important**
>
> Anda tidak dapat mengonversi AMI yang tidak Anda miliki.

Untuk mengonversi AMI yang didukung Amazon S3 ke AMI yang didukung Amazon EBS

1. Luncurkan instans Amazon Linux dari AMI yang didukung Amazon EBS. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol. Instans Amazon Linux memiliki alat AWS CLI dan AMI yang sudah diinstal sebelumnya.
2. Unggah kunci pribadi X.509 yang Anda gunakan untuk menggabungkan AMI yang didukung Amazon S3 ke instans Anda. Kami menggunakan kunci ini untuk memastikan hanya Anda dan Amazon EC2 yang dapat mengakses AMI.
   a. Buat direktori sementara pada instans Anda untuk kunci privat X.509 sebagai berikut:

      ```
      [ec2-user ~]$ mkdir /tmp/cert
      ```

   b. Salin kunci privat X.509 dari komputer Anda ke direktori `/tmp/cert` pada instans, menggunakan alat penyalin aman seperti scp. *`my-private-key`*Parameter dalam perintah

berikut adalah kunci pribadi yang Anda gunakan untuk terhubung ke instance Anda dengan SSH. Contoh:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
```

3. Konfigurasikan variabel lingkungan Anda untuk menggunakan AWS CLI. Untuk informasi selengkapnya, lihat Variabel lingkungan.

   a. (Disarankan) Tetapkan variabel lingkungan untuk kunci AWS akses, kunci rahasia, dan token sesi Anda.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   [ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
   ```

   b. Tetapkan variabel lingkungan untuk kunci AWS akses Anda, dan kunci rahasia.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   ```

4. Siapkan volume Amazon Elastic Block Store (Amazon EBS) untuk AMI baru Anda.

   a. Buat volume EBS kosong di Zona Ketersediaan yang sama dengan instans Anda menggunakan perintah create-volume. Perhatikan ID volume di output perintah.

   > **Important**
   >
   > Volume EBS ini harus berukuran sama atau lebih besar dari volume root penyimpanan instans awal.

   ```
   aws ec2 create-volume \
       --size 10 \
       --region us-west-2 \
       --availability-zone us-west-2b
   ```

   b. Lampirkan volume ke instans yang didukung Amazon EBS menggunakan perintah attach-volume.

```
aws ec2 attach-volume \
    --volume-id vol-01234567890abcdef \
    --instance-id i-1234567890abcdef0 \
    --region us-west-2
```

5. Buat folder untuk paketan Anda.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Unduh paketan untuk AMI berbasis penyimpanan instans Anda ke `/tmp/bundle` menggunakan perintah ec2-download-bundle.

```
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name
 -m image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --
privatekey /path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Susun kembali file gambar dari paketan menggunakan perintah ec2-unbundle.

   a. Ubah direktori ke folder paketan.

```
[ec2-user ~]$ cd /tmp/bundle/
```

   b. Jalankan perintah ec2-unbundle.

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Salin file dari gambar yang tidak dipaketkan ke volume EBS baru.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Periksa volume apakah ada partisi baru yang tidak dipaketkan.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Buat daftar perangkat blok untuk mencari nama perangkat yang akan dipasang.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
```

```
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

Dalam contoh ini, partisi yang akan dipasang adalah `/dev/sdb1`, tetapi nama perangkat Anda mungkin akan berbeda. Jika volume Anda tidak dipartisi, perangkat yang akan dipasang akan serupa dengan `/dev/sdb` (tanpa digit di bagian akhir partisi perangkat).

11. Buat titik pemasangan untuk volume EBS yang baru dan pasang volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Buka file `/etc/fstab` pada volume EBS dengan editor teks favorit Anda (seperti vim atau nano) dan hapus entri apa pun untuk volume penyimpanan instans (ephemeral). Karena volume EBS dipasang di `/mnt/ebs`, file `fstab` berada di `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

Dalam contoh ini, baris terakhir harus dihapus.

13. Lepas volume dan pisahkan dari instans.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id vol-01234567890abcdef --
region us-west-2
```

14. Buat AMI dari volume EBS baru sebagai berikut.

    a. Buat snapshot volume EBS yang baru.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
 "your_snapshot_description" --volume-id vol-01234567890abcdef
```

    b. Periksa untuk memastikan kelengkapan snapshot Anda.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snap-0abcdef1234567890
```

c. Identifikasi arsitektur prosesor, tipe virtualisasi, dan gambar kernel (`aki`) yang digunakan pada AMI asli dengan perintah describe-images. Anda memerlukan ID AMI dari AMI asli yang didukung Amazon S3 untuk langkah ini.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-
id ami-0abcdef1234567890 --output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
 available public machine aki-fc8f11cc instance-store paravirtual xen
```

Dalam contoh ini, arsitekturnya adalah `x86_64` dan ID gambar kernel-nya adalah `aki-fc8f11cc`. Gunakan nilai-nilai ini di langkah berikut. Jika output perintah di atas juga mencantumkan ID `ari`, perhatikan juga hal tersebut.

d. Daftarkan AMI baru Anda dengan ID snapshot volume EBS baru Anda dan nilai-nilai dari langkah sebelumnya. Jika output perintah sebelumnya mencantumkan ID `ari`, sertakan ID tersebut dalam perintah berikut ini dengan `--ramdisk-id` *`ari_id`*.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings DeviceName=device-
name,Ebs={SnapshotId=snap-0abcdef1234567890} --virtualization-type paravirtual
 --architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Opsional) Setelah Anda menguji bahwa Anda dapat meluncurkan instans dari AMI baru, Anda dapat menghapus volume EBS yang Anda buat untuk prosedur ini.

```
aws ec2 delete-volume --volume-id vol-01234567890abcdef
```

Buat Amazon EC2 AMI menggunakan Windows Sysprep

Alat Microsoft System Preparation (Windows Sysprep) membuat versi umum dari sistem operasi, dengan konfigurasi sistem khusus instance dihapus sebelum menangkap gambar baru.

Kami menyarankan Anda menggunakan EC2 Image Builder untuk mengotomatiskan pembuatan, pengelolaan, dan penyebaran gambar server yang disesuaikan, aman, up-to-date dan “emas” yang telah diinstal sebelumnya dan dikonfigurasi sebelumnya dengan perangkat lunak dan pengaturan.

Anda juga dapat menggunakan Windows Sysprep untuk membuat AMI standar menggunakan agen peluncuran Windows: Launch v2, Launch, dan EC2 Config. EC2 EC2

> **Important**
>
> Jangan gunakan Windows Sysprep untuk membuat cadangan instance. Windows Sysprep menghapus informasi spesifik sistem; menghapus informasi ini mungkin memiliki konsekuensi yang tidak diinginkan untuk cadangan instance.

Untuk memecahkan masalah Windows Sysprep, lihat. Memecahkan masalah Sysprep dengan instans Windows Amazon EC2

Daftar Isi

- Fase Windows Sysprep
- Sebelum Anda mulai
- Buat AMI menggunakan Windows Sysprep dengan Launch v2 EC2
- Buat AMI menggunakan Windows Sysprep dengan Launch EC2
- Buat AMI menggunakan Windows Sysprep dengan Config EC2

Fase Windows Sysprep

Windows Sysprep berjalan melalui fase-fase berikut:

- Generalisasi: Alat Sysprep menghapus informasi dan konfigurasi khusus gambar. Misalnya, Windows Sysprep menghapus pengenal keamanan (SID), nama komputer, log peristiwa, dan driver tertentu, untuk beberapa nama. Setelah fase ini selesai, sistem operasi (OS) siap untuk membuat AMI.

  > **Note**
  >
  > Ketika Anda menjalankan Windows Sysprep dengan agen peluncuran Windows, sistem mencegah driver dihapus karena diatur ke true `PersistAllDeviceInstalls` secara default.

- Spesialisasi: Plug and Play memindai komputer dan menginstal driver untuk perangkat yang terdeteksi. Alat Sysprep menghasilkan persyaratan OS, seperti nama komputer dan SID. Anda juga dapat menjalankan perintah dalam fase ini.
- Out-of-Box Experience (OOBE): Sistem menjalankan versi singkat dari Windows Setup dan meminta Anda untuk memasukkan informasi seperti bahasa sistem, zona waktu, dan organisasi terdaftar. Ketika Anda menjalankan Windows Sysprep dengan agen peluncuran Windows, file jawaban mengotomatiskan fase ini.

Sebelum Anda mulai

- Sebelum melakukan Windows Sysprep, kami sarankan Anda menghapus semua akun pengguna lokal dan semua profil akun selain satu akun administrator di mana Windows Sysprep akan dijalankan. Jika Anda menjalankan Windows Sysprep dengan akun dan profil tambahan, perilaku tak terduga dapat terjadi, termasuk hilangnya data profil atau kegagalan untuk menyelesaikan Windows Sysprep.
- Pelajari selengkapnya tentang Ikhtisar Sysprep.
- Pelajari Dukungan Sysprep untuk Peran Server.

Buat AMI menggunakan Windows Sysprep dengan Launch v2 EC2

Saat Anda membuat gambar dari instance dengan agen EC2 Launch v2 diinstal, EC2 Launch v2 melakukan tugas tertentu saat gambar disiapkan. Ini termasuk bekerja dengan Windows Sysprep. Untuk informasi selengkapnya, lihat the section called “Fase Windows Sysprep”.

Daftar Isi

- Tindakan Windows Sysprep
- Pasca Sysprep
- Jalankan Windows Sysprep dengan Launch v2 EC2

Tindakan Windows Sysprep

Windows Sysprep dan EC2 Launch v2 melakukan tindakan berikut saat menyiapkan gambar.

1. Ketika Anda memilih Shutdown dengan Sysprep di kotak dialog EC2Launch settings, sistem menjalankan perintah. `ec2launch sysprep`

2. EC2Luncurkan v2 mengedit konten `unattend.xml` file dengan membaca nilai registri di`HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName`. File ini terletak di direktori berikut: `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. Sistem menjalankan `BeforeSysprep.cmd`. Perintah ini membuat kunci registri sebagai berikut:

   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

   Kunci registri akan menonaktifkan koneksi RDP hingga diaktifkan kembali. Menonaktifkan koneksi RDP adalah langkah keamanan yang diperlukan karena, selama sesi boot pertama setelah Windows Sysprep berjalan, ada periode waktu singkat di mana RDP memungkinkan koneksi dan kata sandi Administrator kosong.
4. Layanan EC2 Launch v2 memanggil Windows Sysprep dengan menjalankan perintah berikut:

   sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch \sysprep\unattend.xml"

Fase Generalisasi

- EC2Launch v2 menghapus informasi dan konfigurasi khusus gambar, seperti nama komputer dan SID. Jika instans adalah anggota sebuah domain, instans akan dihapus dari domain tersebut. File jawaban `unattend.xml` mencakup pengaturan berikut yang memengaruhi fase ini:
  - PersistAllDeviceInstalls: Pengaturan ini mencegah Pengaturan Windows menghapus dan mengonfigurasi ulang perangkat, yang mempercepat proses persiapan gambar karena Amazon AMIs memerlukan driver tertentu untuk dijalankan dan deteksi ulang driver tersebut akan memakan waktu.
  - DoNotCleanUpNonPresentDevices: Pengaturan ini menyimpan informasi Plug and Play untuk perangkat yang saat ini tidak ada.
- Windows Sysprep mematikan OS saat bersiap untuk membuat AMI. Sistem meluncurkan instans baru atau memulai instans asal.

Tahap Spesialisasi

Sistem menghasilkan persyaratan spesifik OS, seperti nama komputer dan SID. Sistem juga melakukan tindakan berikut berdasarkan konfigurasi yang Anda tentukan dalam file jawaban `unattend.xml`.

- CopyProfile: Windows Sysprep dapat dikonfigurasi untuk menghapus semua profil pengguna, termasuk profil Administrator bawaan. Pengaturan ini mempertahankan akun Administrator bawaan sehingga kustomisasi apa pun yang Anda buat pada akun tersebut dipindahkan ke gambar baru. Nilai bawaannya adalah `True`.

  CopyProfile mengganti profil default dengan profil administrator lokal yang ada. Semua akun yang Anda masuk setelah menjalankan Windows Sysprep menerima salinan profil itu dan isinya saat login pertama.

  Jika Anda tidak memiliki kustomisasi profil pengguna tertentu yang ingin Anda tampilkan ke gambar baru tersebut, ubah pengaturan ini menjadi `False`. Windows Sysprep akan menghapus semua profil pengguna (ini menghemat waktu dan ruang disk).
- TimeZone: Zona waktu diatur ke Coordinate Universal Time (UTC) secara default.
- Perintah sinkron dengan order 1: Sistem menjalankan perintah berikut, yang mengaktifkan akun administrator dan menentukan persyaratan kata sandi:

  ```
  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /
  PASSWORDREQ:YES
  ```
- Perintah sinkron dengan order 2: Sistem mengacak kata sandi administrator. Langkah keamanan ini dirancang untuk mencegah instance agar tidak dapat diakses setelah Windows Sysprep selesai jika Anda tidak mengonfigurasi tugas. `setAdminAccount`

  Sistem menjalankan perintah berikut dari direktori agen peluncuran lokal Anda (`C:\Program Files\Amazon\EC2Launch\`).

  ```
  EC2Launch.exe internal randomize-password --username Administrator
  ```
- Untuk mengaktifkan koneksi desktop jarak jauh, sistem menetapkan kunci `fDenyTSConnections` registri Terminal Server ke false.

Fase OOBE

1. Sistem menentukan konfigurasi berikut menggunakan file jawaban EC2 Launch v2:
   - `<InputLocale>en-US</InputLocale>`
   - `<SystemLocale>en-US</SystemLocale>`
   - `<UILanguage>en-US</UILanguage>`

- `<UserLocale>en-US</UserLocale>`
- `<HideEULAPage>true</HideEULAPage>`
- `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`
- `<ProtectYourPC>3</ProtectYourPC>`
- `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
- `<TimeZone>UTC</TimeZone>`
- `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
- `<RegisteredOwner>EC2</RegisteredOwner>`

> **Note**
>
> Selama fase generalisasi dan spesialisasi, EC2 Launch v2 memantau status OS. Jika EC2 Launch v2 mendeteksi bahwa OS berada dalam fase Sysprep, maka ia menerbitkan pesan berikut ke log sistem:
> Windows sedang dikonfigurasi. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Sistem menjalankan EC2 Launch v2.

Pasca Sysprep

Setelah Windows Sysprep selesai, EC2 Launch v2 mengirimkan pesan berikut ke output konsol:

```
Windows sysprep configuration complete.
```

EC2Luncurkan v2 kemudian melakukan tindakan berikut:

1. Membaca konten file `agent-config.yml` dan menjalankan tugas-tugas yang dikonfigurasi.
2. Menjalankan semua tugas dalam tahap `preReady`.
3. Setelah selesai, mengirim pesan `Windows is ready` ke log sistem instans.
4. Menjalankan semua tugas dalam tahap `PostReady`.

Untuk informasi selengkapnya tentang EC2 Launch v2, lihatGunakan agen EC2launch v2 untuk melakukan tugas selama peluncuran instans Windows EC2.

Jalankan Windows Sysprep dengan Launch v2 EC2

Gunakan prosedur berikut untuk membuat AMI standar menggunakan Windows Sysprep dengan Launch v2. EC2

1. Di konsol Amazon EC2, cari AMI yang ingin Anda duplikat.
2. Jalankan dan hubungkan ke instans Windows Anda.
3. Sesuaikan pengaturan
    a. Dari menu Start Windows, cari dan pilih pengaturan Amazon EC2 Launch. Untuk informasi selengkapnya tentang opsi dan pengaturan di kotak dialog Pengaturan EC2 Peluncuran Amazon, lihatKonfigurasikan pengaturan EC2 Launch v2 untuk instance Windows.
    b. Jika Anda telah membuat perubahan, pilih Simpan sebelum Anda mematikan.
4. Pilih Shutdown dengan Sysprep atau Shutdown tanpa Sysprep.

Ketika Anda diminta untuk mengonfirmasi bahwa Anda ingin menjalankan Windows Sysprep dan mematikan instance, klik Ya. EC2Luncurkan v2 menjalankan Windows Sysprep. Selanjutnya, Anda keluar dari instans, dan instans tersebut padam. Jika Anda memeriksa halaman Instans di konsol Amazon EC2, status instan berubah dari `Running` ke `Stopping`, lalu ke `Stopped`. Ketika itu, aman untuk membuat AMI dari instans ini.

Anda dapat secara manual memanggil alat Windows Sysprep dari baris perintah menggunakan perintah berikut:

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Buat AMI menggunakan Windows Sysprep dengan Launch EC2

Saat Anda membuat gambar dari instance dengan agen EC2 Peluncuran diinstal, EC2 Launch melakukan tugas tertentu saat gambar disiapkan. Ini termasuk bekerja dengan Windows Sysprep. Untuk informasi selengkapnya, lihat the section called “Fase Windows Sysprep”.

EC2Launch menawarkan file jawaban default dan file batch untuk Windows Sysprep yang mengotomatiskan dan mengamankan proses persiapan gambar pada AMI Anda. Memodifikasi file ini bersifat opsional. File ini terletak di direktori berikut secara default: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

> **Important**
>
> Jangan gunakan Windows Sysprep untuk membuat cadangan instance. Windows Sysprep menghapus informasi spesifik sistem. Jika Anda menghapus informasi ini, mungkin ada konsekuensi yang tidak diinginkan untuk pencadangan instans.

Daftar Isi

- EC2Luncurkan jawaban dan file batch untuk Windows Sysprep
- Jalankan Windows Sysprep dengan Launch EC2
- Perbarui metadata/KMS rute untuk Server 2016 dan yang lebih baru saat meluncurkan AMI khusus

EC2Luncurkan jawaban dan file batch untuk Windows Sysprep

File jawaban EC2 Launch dan file batch untuk Windows Sysprep meliputi yang berikut:

`Unattend.xml`

Ini adalah file jawaban default. Jika Anda menjalankan `SysprepInstance.ps1` atau memilih ShutdownWithSysprep dalam antarmuka pengguna, sistem membaca pengaturan dari file ini.

`BeforeSysprep.cmd`

Sesuaikan file batch ini untuk menjalankan perintah sebelum EC2 Launch menjalankan Windows Sysprep.

`SysprepSpecialize.cmd`

Sesuaikan file batch ini untuk menjalankan perintah selama fase spesialisasi Windows Sysprep.

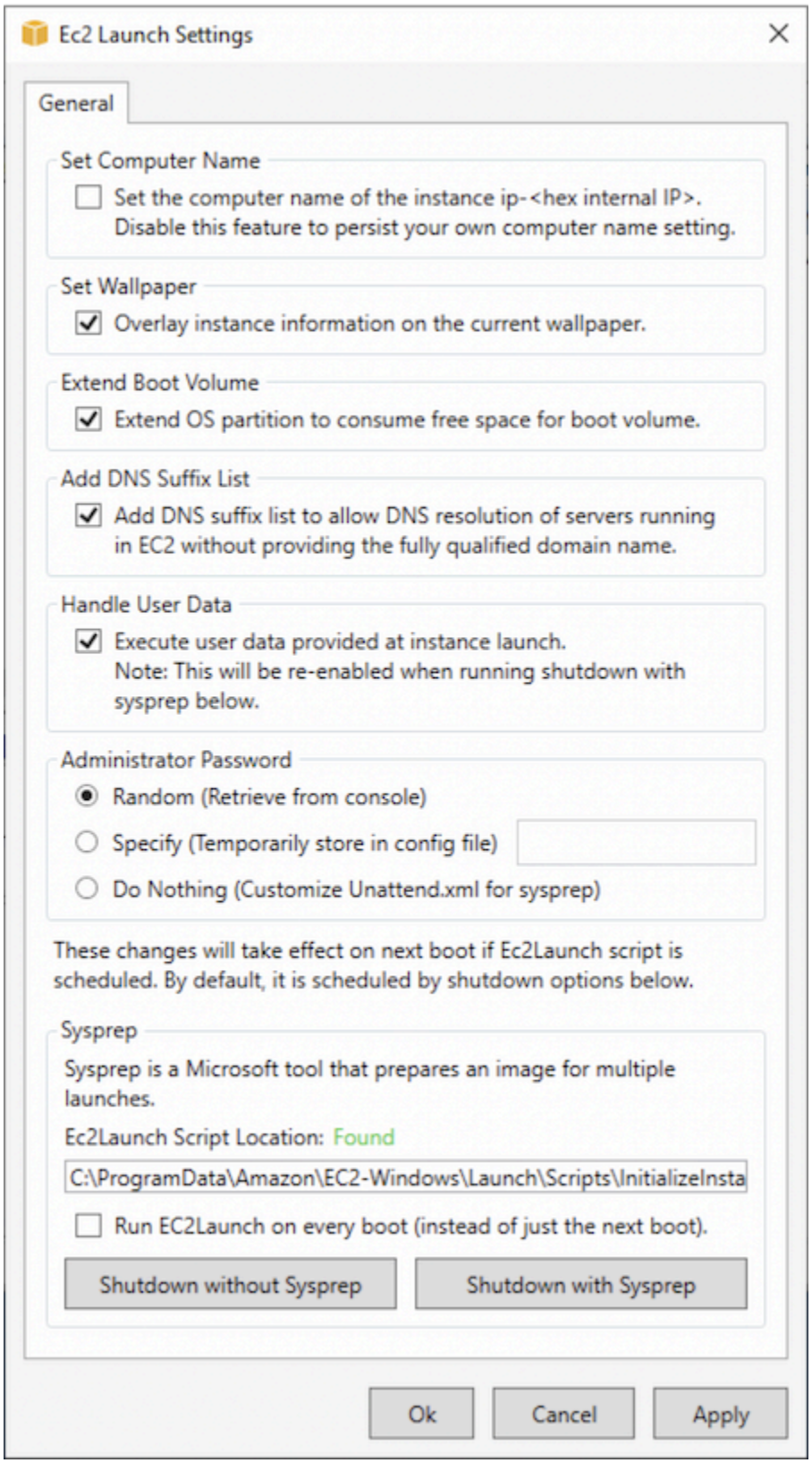
Jalankan Windows Sysprep dengan Launch EC2

Pada instalasi penuh Windows Server 2016 dan yang lebih baru (dengan pengalaman desktop), Anda dapat menjalankan Windows Sysprep dengan EC2 Launch secara manual atau dengan menggunakan aplikasi EC2 Launch Settings.

Untuk menjalankan Windows Sysprep menggunakan aplikasi Launch Settings EC2

1. Di konsol Amazon EC2, cari atau buat AMI Windows Server 2016 atau yang lebih baru.

2. Luncurkan instans Windows dari AMI.
3. Sambungkan ke instans Windows Anda dan kustomisasikan.
4. Cari dan jalankan aplikasi EC2LaunchSettings. Aplikasi ini terletak di direktori berikut secara default: `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.



5. Pilih atau hapus opsi sesuai kebutuhan. Pengaturan ini disimpan dalam file `LaunchConfig.json` Anda.

6. Untuk Kata Sandi Administrator, lakukan salah satu hal berikut:

   - Pilih Acak. EC2Peluncuran menghasilkan kata sandi dan mengenkripsi menggunakan kunci pengguna. Sistem akan menonaktifkan pengaturan ini setelah instans dijalankan sehingga kata sandi akan tetap ada meskipun instans di-boot ulang atau dihentikan dan dimulai.
   - Pilih Tentukan dan ketik kata sandi yang memenuhi persyaratan sistem. Kata sandi disimpan dalam teks `LaunchConfig.json` yang jelas dan dihapus setelah Windows Sysprep menetapkan kata sandi administrator. Jika Anda mematikan sekarang, kata sandi segera diatur. EC2Luncurkan mengenkripsi kata sandi menggunakan kunci pengguna.
   - Pilih DoNothing dan tentukan kata sandi dalam file `unattend.xml`. Jika Anda tidak menentukan kata sandi di `unattend.xml`, akun administrator akan dinonaktifkan.

7. Pilih Matikan dengan Sysprep.

Untuk menjalankan Windows Sysprep secara manual menggunakan Launch EC2

1. Di konsol Amazon EC2, cari atau buat AMI edisi Datacenter Windows Server 2016 atau lebih baru yang ingin Anda duplikasi.
2. Luncurkan dan sambungkan ke instans Windows Anda.
3. Kustomisasikan instans.
4. Tentukan pengaturan di file `LaunchConfig.json`. File ini terletak di direktori `C:\ProgramData\Amazon\EC2-Windows\Launch\Config` secara default.

   Untuk `adminPasswordType`, tentukan satu dari nilai-nilai berikut:

   `Random`

   EC2Peluncuran menghasilkan kata sandi dan mengenkripsi menggunakan kunci pengguna. Sistem akan menonaktifkan pengaturan ini setelah instans dijalankan sehingga kata sandi ini akan tetap ada jika instans tersebut di-boot ulang atau dihentikan dan dimulai.

   `Specify`

   EC2Peluncuran menggunakan kata sandi yang Anda tentukan`adminPassword`. Jika kata sandi tidak memenuhi persyaratan sistem, EC2 Lauch menghasilkan kata sandi acak sebagai gantinya. Kata sandi disimpan dalam teks `LaunchConfig.json` yang jelas dan dihapus setelah Windows Sysprep menetapkan kata sandi administrator. EC2Luncurkan mengenkripsi kata sandi menggunakan kunci pengguna.

`DoNothing`

EC2Peluncuran menggunakan kata sandi yang Anda tentukan dalam `unattend.xml` file. Jika Anda tidak menentukan kata sandi di `unattend.xml`, akun administrator akan dinonaktifkan.

5. (Opsional) Tentukan pengaturan di `unattend.xml` dan file konfigurasi lainnya. Jika berencana mengatur instalasi, Anda tidak perlu mengubah file-file ini. File ini terletak di direktori berikut secara default: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. Di Windows PowerShell, jalankan `./InitializeInstance.ps1 -Schedule`. Skrip ini terletak di direktori berikut secara default: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Skrip ini menjadwalkan instans untuk diinisialisasi saat boot berikutnya. Anda harus menjalankan skrip ini sebelum menjalankan skrip `SysprepInstance.ps1` dalam langkah berikutnya.
7. Di Windows PowerShell, jalankan `./SysprepInstance.ps1`. Skrip ini terletak di direktori berikut secara default: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Anda keluar dari instans dan instans akan dimatikan. Jika Anda memeriksa halaman Instans di konsol Amazon EC2, status instan berubah dari `Running` ke `Stopping`, lalu ke `Stopped`. Saat itu, aman untuk membuat AMI dari instans ini.

Perbarui metadata/KMS rute untuk Server 2016 dan yang lebih baru saat meluncurkan AMI khusus

Untuk memperbarui metadata/KMS rute untuk Server 2016 dan yang lebih baru saat meluncurkan AMI kustom, lakukan salah satu hal berikut:

- Jalankan EC2 LaunchSettings GUI (C:\\ ProgramData Amazon\ EC2-Windows\ Launch\ Settings\ Ec2 LaunchSettings .exe) dan pilih opsi untuk mematikan dengan Windows Sysprep.
- Jalankan EC2 LaunchSettings dan matikan tanpa Windows Sysprep sebelum membuat AMI. Ini akan mengatur tugas inisialisasi EC2 Launch untuk berjalan pada boot berikutnya, yang akan mengatur rute berdasarkan subnet untuk instans.
- Menjadwalkan ulang secara manual tugas inisialisasi EC2 Launch sebelum membuat AMI dari PowerShell.

> **Important**
>
> Perhatikan perilaku reset kata sandi default sebelum menjadwalkan ulang tugas.

- Untuk memperbarui rute pada instans yang mengalami aktivasi atau komunikasi Windows dengan kegagalan metadata instans, lihat “Tidak dapat mengaktivasi Windows”.

Buat AMI menggunakan Windows Sysprep dengan Config EC2

Saat Anda membuat gambar dari instance dengan layanan EC2 Config diinstal, EC2 Config melakukan tugas tertentu saat gambar disiapkan. Ini termasuk bekerja dengan Windows Sysprep. Untuk informasi selengkapnya, lihat the section called “Fase Windows Sysprep”.

Daftar Isi

- Tindakan Windows Sysprep
- Pasca Sysprep
- Jalankan Windows Sysprep dengan layanan Config EC2

Tindakan Windows Sysprep

Windows Sysprep dan layanan EC2 Config melakukan tindakan berikut saat menyiapkan gambar.

1. Saat Anda memilih Matikan dengan Sysprep di kotak dialog Properti Layanan EC2, sistem menjalankan perintah ec2config.exe –sysprep.
2. Layanan EC2 Config membaca konten file. `BundleConfig.xml` Secara default, file terletak dalam direktori berikut: `C:\Program Files\Amazon\Ec2ConfigService\Settings`.

   File `BundleConfig.xml` mencakup pengaturan berikut. Anda dapat mengubah pengaturan ini:

   - AutoSysprep: Menunjukkan apakah akan menggunakan Windows Sysprep secara otomatis. Anda tidak perlu mengubah nilai ini jika Anda menjalankan Windows Sysprep dari kotak dialog Properti Layanan EC2. Nilai default-nya adalah `No`.
   - Set RDPCertificate: Menetapkan sertifikat yang ditandatangani sendiri untuk server Remote Desktop. Ini memungkinkan Anda menggunakan Remote Desktop Protocol (RDP) secara aman untuk tersambung ke instans. Ubah nilai ke `Yes` jika instans baru harus menggunakan sertifikat. Pengaturan ini tidak digunakan dengan instance Windows Server 2012 karena sistem operasi ini dapat menghasilkan sertifikat mereka sendiri. Nilai default-nya adalah `No`.
   - SetPasswordAfterSysprep: Menetapkan kata sandi acak pada instance yang baru diluncurkan, mengenkripsi dengan kunci peluncuran pengguna, dan mengeluarkan kata sandi terenkripsi ke konsol. Ubah nilai ke `No` jika instans baru tidak boleh diatur ke kata sandi terenkripsi acak. Nilai default-nya adalah `Yes`.

- PreSysprepRunCmd: Lokasi perintah untuk dijalankan. Skrip ini terletak di direktori berikut secara default: `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. Sistem menjalankan `BeforeSysprep.cmd`. Perintah ini membuat kunci registri sebagai berikut:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
 fDenyTSConnections /t REG_DWORD /d 1 /f
```

   Kunci registri akan menonaktifkan koneksi RDP hingga diaktifkan kembali. Menonaktifkan koneksi RDP adalah langkah keamanan yang diperlukan karena, selama sesi boot pertama setelah Windows Sysprep berjalan, ada periode waktu singkat di mana RDP memungkinkan koneksi dan kata sandi Administrator kosong.

4. Layanan EC2 Config memanggil Windows Sysprep dengan menjalankan perintah berikut:

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /
oobe /generalize /shutdown
```

Fase Generalisasi

- Alat ini menghapus informasi dan konfigurasi spesifik gambar, seperti nama komputer dan SID. Jika instans adalah anggota sebuah domain, instans akan dihapus dari domain tersebut. File jawaban `sysprep2008.xml` mencakup pengaturan berikut yang memengaruhi fase ini:
  - PersistAllDeviceInstalls: Pengaturan ini mencegah Pengaturan Windows menghapus dan mengonfigurasi ulang perangkat, yang mempercepat proses persiapan gambar karena Amazon AMIs memerlukan driver tertentu untuk dijalankan dan deteksi ulang driver tersebut akan memakan waktu.
  - DoNotCleanUpNonPresentDevices: Pengaturan ini menyimpan informasi Plug and Play untuk perangkat yang saat ini tidak ada.
- Windows Sysprep mematikan OS saat bersiap untuk membuat AMI. Sistem meluncurkan instans baru atau memulai instans asal.

Tahap Spesialisasi

Sistem menghasilkan persyaratan spesifik OS, seperti nama komputer dan SID. Sistem juga melakukan tindakan berikut ini berdasarkan konfigurasi yang Anda tentukan dalam file jawaban sysprep2008.xml.

- CopyProfile: Windows Sysprep dapat dikonfigurasi untuk menghapus semua profil pengguna, termasuk profil Administrator bawaan. Pengaturan ini mempertahankan akun Administrator bawaan sehingga kustomisasi apa pun yang Anda buat pada akun tersebut dipindahkan ke gambar baru. Nilai default-nya adalah True.

  CopyProfile mengganti profil default dengan profil administrator lokal yang ada. Semua akun yang masuk setelah menjalankan Windows Sysprep akan menerima salinan profil itu dan isinya pada login pertama.

  Apabila Anda tidak memiliki kustomisasi profil pengguna tertentu yang ingin Anda tampilkan ke gambar baru tersebut, ubah pengaturan ini menjadi False. Windows Sysprep akan menghapus semua profil pengguna; ini menghemat waktu dan ruang disk.
- TimeZone: Zona waktu diatur ke Coordinate Universal Time (UTC) secara default.
- Perintah sinkron dengan order 1: Sistem menjalankan perintah berikut, yang mengaktifkan akun administrator dan menentukan persyaratan kata sandi.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER / PASSWORDREQ:YES
- Perintah sinkron dengan order 2: Sistem mengacak kata sandi administrator. Langkah keamanan ini dirancang untuk mencegah instance agar tidak dapat diakses setelah Windows Sysprep selesai jika Anda tidak mengaktifkan pengaturan ec2setpassword.

  C:\Program Files\ Amazon\ Ec2ConfigService\ ScramblePassword .exe” -u Administrator
- Perintah sinkron dengan order 3: Sistem menjalankan perintah berikut:

  C:\Program File\ Amazon\ Ec2\ SkripConfigService\ .cmd SysprepSpecializePhase

  Perintah ini menambahkan kunci registri berikut ini, yang mengaktifkan ulang RDP:

  reg tambahkan “HKEY_LOCAL_MACHINE\ SYSTEM\\ ControlCurrentControlSet\ Terminal Server” /v fDeny/t REG_DWORD /d 0 /f TSConnections

Fase OOBE

1. Menggunakan file jawaban layanan EC2 Config, sistem menentukan konfigurasi berikut:
   - < InputLocale InputLocale >en-kami</ >
   - < SystemLocale SystemLocale >en-kami</ >
   - < UILanguage UILanguage >en-kami</ >
   - < UserLocale UserLocale >en-kami</ >
   - <Sembunyikan EULAPage >Benar</Sembunyikan > EULAPage
   - < HideWirelessSetupIn OOBE>BENAR</ HideWirelessSetupIn OOBE>
   - < NetworkLocation NetworkLocation >Lainnya</ >
   - < ProtectYour PC> 3 </ PC> ProtectYour
   - < BluetoothTaskbarIconEnabled BluetoothTaskbarIconEnabled >salah</ >
   - < TimeZone TimeZone >UTC</ >
   - < RegisteredOrganization RegisteredOrganization >Amazon.com</ >
   - < RegisteredOwner RegisteredOwner >Amazon</ >

   > **Note**
   >
   > Selama fase generalisasi dan spesialisasi, layanan EC2 Config memantau status OS. Jika EC2 Config mendeteksi bahwa OS berada dalam fase Sysprep, maka ia menerbitkan pesan berikut ke log sistem:
   > EC2ConfigMonitorState: 0 Windows sedang dikonfigurasi.
   > SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Setelah fase OOBE selesai, sistem menjalankan `SetupComplete.cmd` dari lokasi berikut: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. Di Amazon publik AMIs sebelum April 2015 file ini kosong dan tidak menjalankan apa pun pada gambar. Di depan umum AMIs tertanggal setelah April 2015, file tersebut mencakup nilai berikut:call "C:\Program Files\Amazon \Ec2ConfigService\Scripts\PostSysprep.cmd".
3. Sistem menjalankan `PostSysprep.cmd`, yang melakukan operasi berikut:
   - Mengatur kata sandi Administrator lokal agar tidak kedaluwarsa. Jika kata sandi kedaluwarsa, Administrator mungkin tidak bisa masuk.
   - Menetapkan nama MSSQLServer mesin (jika diinstal) sehingga nama akan sinkron dengan AMI.

Pasca Sysprep

Setelah Windows Sysprep selesai, layanan EC2 Config mengirimkan pesan berikut ke output konsol:

```
Windows sysprep configuration complete.
   Message: Sysprep Start
   Message: Sysprep End
```

EC2Config kemudian melakukan tindakan berikut:

1. Membaca konten file config.xml dan mencantumkan semua plug-in yang diaktifkan.
2. Menjalankan semua plug-in “Sebelum Windows siap” secara bersamaan.
   - Ec2 SetPassword
   - Ec2 SetComputerName
   - Ec2 InitializeDrives
   - Ec2 EventLog
   - Ec2ConfigureRDP
   - Keluaran Ec2 RDPCert
   - Ec2 SetDriveLetter
   - Ec2 WindowsActivate
   - Ec2 DynamicBootVolumeSize
3. Setelah selesai, mengirimkan pesan “Windows siap” ke log sistem instans.
4. Menjalankan semua plug-in “Setelah Windows siap” secara bersamaan.
   - CloudWatch Log Amazon
   - UserData
   - AWS Systems Manager (Systems Manager)

Untuk informasi selengkapnya tentang plug-in Windows, lihat Gunakan layanan EC2config untuk melakukan tugas selama peluncuran instans sistem operasi Windows lama EC2.

Jalankan Windows Sysprep dengan layanan Config EC2

Gunakan prosedur berikut untuk membuat AMI standar menggunakan Windows Sysprep dan layanan Config. EC2

1. Di konsol Amazon EC2, cari atau buat AMI yang ingin Anda duplikasi.

2. Luncurkan dan sambungkan ke instans Windows Anda.
3. Kustomisasikan.
4. Tentukan pengaturan konfigurasi dalam file jawaban layanan EC2 Config:

   ```
   C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
   ```

5. Dari menu Mulai Windows, pilih Semua Program, lalu pilih Pengaturan EC2ConfigService.
6. Pilih tab Gambar di kotak dialog Properti Layanan Ec2. Untuk informasi selengkapnya tentang opsi dan pengaturan di kotak dialog Properti Layanan Ec2, lihat Properti Layanan Ec2.
7. Pilih opsi untuk kata sandi Administrator, lalu pilih Shutdown dengan Sysprep atau Shutdown tanpa Sysprep. EC2Config mengedit file pengaturan berdasarkan opsi kata sandi yang Anda pilih.
   - Acak: EC2 Config menghasilkan kata sandi, mengenkripsi dengan kunci pengguna, dan menampilkan kata sandi terenkripsi ke konsol. Kami menonaktifkan pengaturan ini setelah peluncuran pertama sehingga kata sandi ini akan tetap ada jika instans tersebut di-boot ulang atau dihentikan dan dimulai.
   - Tentukan: Kata sandi disimpan dalam file jawaban Windows Sysprep dalam bentuk yang tidak terenkripsi (teks yang jelas). Ketika Windows Sysprep berjalan berikutnya, ia menetapkan kata sandi Administrator. Jika Anda mematikan sekarang, kata sandi akan segera ditetapkan. Saat layanan dimulai lagi, kata sandi Administrator dihapus. Penting untuk mengingat kata sandi ini karena Anda tidak dapat mengambilnya nanti.
   - Tetap Ada: Kata sandi yang ada untuk akun Administrator tidak berubah saat Windows Sysprep dijalankan atau Config EC2 dimulai ulang. Penting untuk mengingat kata sandi ini karena Anda tidak dapat mengambilnya nanti.
8. Pilih OK.

Ketika Anda diminta untuk mengonfirmasi bahwa Anda ingin menjalankan Windows Sysprep dan mematikan instance, klik Ya. Anda akan melihat bahwa EC2 Config menjalankan Windows Sysprep. Selanjutnya, Anda keluar dari instans, dan instansnya dimatikan. Jika Anda memeriksa halaman Instans di konsol Amazon EC2, status instan berubah dari `Running` ke `Stopping`, lalu ke `Stopped`. Ketika itu, aman untuk membuat AMI dari instans ini.

Anda dapat secara manual memanggil alat Windows Sysprep dari baris perintah menggunakan perintah berikut:

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep""
```

> **Note**
>
> Tanda kutip ganda dalam perintah tidak diperlukan jika shell CMD Anda sudah ada di direktori C:\Program Files\ Amazon\ EC2ConfigService\.

Namun, Anda harus sangat berhati-hati agar opsi file XML yang ditentukan dalam folder `Ec2ConfigService\Settings` sudah benar; jika tidak, Anda mungkin tidak dapat terhubung ke instans. Untuk informasi selengkapnya tentang file pengaturan, lihat EC2File pengaturan Config. Untuk contoh mengkonfigurasi dan kemudian menjalankan Windows Sysprep dari baris perintah, lihat. `Ec2ConfigService\Scripts\InstallUpdates.ps1`

Salin Amazon EC2 AMI

Jika Anda memerlukan konfigurasi instans Amazon EC2 yang konsisten di beberapa Wilayah, Anda dapat menggunakan satu Amazon Machine Image (AMI) sebagai template untuk meluncurkan semua instans. Namun, AMIs adalah sumber daya khusus Wilayah—untuk meluncurkan instance secara spesifik, AMI harus berada di Wilayah AWS Region tersebut. Oleh karena itu, untuk menggunakan AMI yang sama di beberapa Wilayah, Anda harus menyalinnya dari Wilayah sumber ke setiap Wilayah target.

Metode yang Anda gunakan untuk menyalin AMI bergantung pada apakah Anda menyalin di seluruh Wilayah dalam partisi yang sama atau di partisi yang berbeda:

- Penyalinan Lintas Wilayah — Salin AMIs di seluruh Wilayah dalam partisi yang sama, misalnya, di seluruh Wilayah dalam partisi komersial. Metode penyalinan ini dijelaskan dalam topik ini.
- Penyalinan partisi silang — Salin AMIs dari satu partisi ke partisi lain, misalnya, dari partisi komersial ke partisi. AWS GovCloud (US) Untuk informasi tentang metode penyalinan ini, lihatMenyimpan dan memulihkan AMI.
- Penyalinan lintas akun — Buat salinan AMI yang Akun AWS telah dibagikan orang lain dengan Anda. Akun AWS Metode penyalinan ini dijelaskan dalam topik ini.

Waktu yang dibutuhkan untuk menyelesaikan operasi penyalinan AMI lintas wilayah dan lintas akun adalah upaya terbaik. Jika Anda memerlukan kontrol atas waktu penyelesaian, Anda dapat menentukan jendela penyelesaian mulai dari 15 menit hingga 48 jam, memastikan AMI Anda disalin dalam jangka waktu yang diperlukan. Biaya tambahan berlaku untuk operasi penyalinan AMI

berbasis waktu. Untuk informasi selengkapnya, lihat Salinan berbasis waktu di Panduan Pengguna Amazon EBS.

Daftar Isi

- Pertimbangan-pertimbangan
- Biaya
- Berikan izin untuk menyalin Amazon EC2 AMIs
- Menyalin AMI
- Menghentikan operasi penyalinan AMI yang tertunda
- Cara kerja salinan Amazon EC2 AMI

Pertimbangan-pertimbangan

- Izin untuk menyalin AMIs — Anda dapat menggunakan kebijakan IAM untuk memberikan atau menolak izin pengguna untuk menyalin AMIs. Mulai 28 Oktober 2024, Anda dapat menentukan izin tingkat sumber daya untuk tindakan `CopyImage` di sumber AMI. Izin tingkat sumber daya untuk AMI baru tersedia seperti sebelumnya.
- Izin peluncuran dan izin bucket Amazon S3 AWS — tidak menyalin izin peluncuran atau izin bucket Amazon S3 dari sumber AMI ke AMI baru. Setelah operasi penyalinan selesai, Anda dapat menerapkan izin peluncuran dan izin bucket Amazon S3 ke AMI yang baru.
- Tag — Anda hanya dapat menyalin tag AMI yang ditentukan pengguna yang Anda lampirkan ke sumber AMI. Tag sistem (diawali dengan `aws:`) dan tag yang ditentukan pengguna yang dilampirkan oleh Akun AWS lain tidak akan disalin. Saat menyalin AMI, Anda dapat melampirkan tag baru ke AMI baru dan snapshot dukungannya.
- Kuota untuk salinan AMI berbasis waktu — Setelah Anda mencapai kuota throughput salinan snapshot kumulatif, permintaan salinan AMI berbasis waktu berikutnya gagal. Untuk informasi selengkapnya, lihat Kuota untuk salinan berbasis waktu di Panduan Pengguna Amazon EBS.
- Salinan tujuan sumber yang didukung — Lokasi AMI sumber menentukan apakah Anda dapat menyalinnya dan tujuan yang diizinkan untuk AMI baru:
  - Jika sumber AMI berada di Wilayah, Anda dapat menyalinnya di dalam Wilayah tersebut, ke Wilayah lain, ke Pos Terdepan yang terkait dengan Wilayah tersebut, atau ke Zona Lokal di Wilayah tersebut.

  - Jika AMI sumber berada di Zona Lokal, Anda dapat menyalinnya di dalam Zona Lokal tersebut, ke Wilayah induk Zona Lokal tersebut, atau ke Local Zone tertentu lainnya dengan Wilayah induk yang sama.
  - Jika sumber AMI ada di Outpost, Anda tidak dapat menyalinnya.
- Parameter CLI untuk sumber dan tujuan — Saat menggunakan CLI, parameter berikut didukung untuk menentukan lokasi sumber AMI yang akan disalin dan tujuan AMI baru. Perhatikan bahwa operasi penyalinan harus dimulai di Wilayah tujuan; jika Anda menghilangkan `--region` parameter, tujuan mengasumsikan Wilayah default yang dikonfigurasi dalam pengaturan Anda. AWS CLI

Sumber ke tujuan	Parameter sumber	Parameter tujuan
Wilayah ke Wilayah	`--source-region`	`--region`
Wilayah ke Pos Terdepan	`--source-region`	`--destination-outpost-arn` (ARN dari Pos Terdepan)
Wilayah ke Zona Lokal	`--source-region` Harus menjadi Wilayah induk dari Zona Lokal.	`--destination-availability-zone` (nama Zona Lokal) atau `--destination-availability-zone-id` (ID Zona Lokal)
Zona Lokal ke Wilayah	`--source-region` Harus menjadi Wilayah induk dari Zona Lokal. Sumber Local Zone diasumsikan dari lokasi ID AMI sumber yang ditentukan.	`--region` Harus menjadi Wilayah induk dari Zona Lokal.
Zona Lokal ke Zona Lokal	`--source-region` Harus menjadi Wilayah induk dari Zona Lokal.	`--destination-availability-zone` (nama Zona Lokal) atau `--destina`

Sumber ke tujuan	Parameter sumber	Parameter tujuan
	Sumber Local Zone diasumsikan dari lokasi ID AMI sumber yang ditentukan.	`tion-availability-zone-id` (ID Zona Lokal)

Biaya

Tidak ada biaya untuk menyalin AMI ketika tidak ada waktu penyelesaian yang ditentukan. Namun, biaya tambahan berlaku untuk operasi penyalinan AMI berbasis waktu. Untuk informasi selengkapnya, lihat Salinan berbasis waktu di Panduan Pengguna Amazon EBS.

Tarif penyimpanan dan transfer data standar berlaku. Jika Anda menyalin AMI yang didukung oleh EBS, Anda akan dikenai biaya untuk penyimpanan snapshot EBS tambahan.

Berikan izin untuk menyalin Amazon EC2 AMIs

Untuk menyalin AMI yang didukung EBS atau yang didukung Amazon S3, Anda memerlukan izin IAM berikut:

- `ec2:CopyImage`— Untuk menyalin AMI. Untuk yang didukung EBS AMIs, itu juga memberikan izin untuk menyalin snapshot dukungan AMI.
- `ec2:CreateTags`— Untuk menandai target AMI. Untuk yang didukung EBSAMIs, itu juga memberikan izin untuk menandai snapshot dukungan AMI target.

Jika Anda menyalin AMI yang didukung penyimpanan instans, Anda memerlukan izin IAM tambahan berikut:

- `s3:CreateBucket`— Untuk membuat bucket S3 di Wilayah target untuk AMI baru
- `s3:PutBucketOwnershipControls`— ACLs Untuk mengaktifkan bucket S3 yang baru dibuat sehingga objek dapat ditulis dengan ACL `aws-exec-read` kalengan
- `s3:GetBucketAcl`— Untuk membaca ember sumber ACLs
- `s3:ListAllMyBuckets`— Untuk menemukan bucket S3 yang ada AMIs di Wilayah target
- `s3:GetObject`— Untuk membaca objek di ember sumber
- `s3:PutObject`— Untuk menulis objek di ember target

- `s3:PutObjectAcl`— Untuk menulis izin untuk objek baru di bucket target

> **Note**
>
> Mulai 28 Oktober 2024, Anda dapat menentukan izin tingkat sumber daya untuk tindakan `CopyImage` di sumber AMI. Izin tingkat sumber daya untuk AMI target tersedia seperti sebelumnya. Untuk informasi selengkapnya, lihat tabel CopyImagedi bawah Tindakan yang ditentukan oleh Amazon EC2 di Referensi Otorisasi Layanan.

Contoh kebijakan IAM untuk menyalin AMI yang didukung EBS dan menandai AMI target dan snapshot

Contoh kebijakan berikut memberi Anda izin untuk menyalin AMI yang didukung EBS dan menandai AMI target dan snapshot dukungannya.

> **Note**
>
> Mulai 28 Oktober 2024, Anda dapat menentukan snapshot di elemen. `Resource` Untuk informasi selengkapnya, lihat tabel CopyImagedi bawah Tindakan yang ditentukan oleh Amazon EC2 di Referensi Otorisasi Layanan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:*::image/*",
            "arn:aws:ec2:*::snapshot/*"
        ]
    }]
```

```
}
```

Contoh kebijakan IAM untuk menyalin AMI yang didukung EBS tetapi menolak menandai snapshot baru

`ec2:CopySnapshot`Izin secara otomatis diberikan ketika Anda mendapatkan `ec2:CopyImage` izin. Izin untuk menandai snapshot dukungan baru dapat ditolak secara eksplisit, mengesampingkan efek untuk tindakan tersebut`Allow`. `ec2:CreateTags`

Contoh kebijakan berikut memberi Anda izin untuk menyalin AMI yang didukung EBS, tetapi menolak Anda untuk menandai snapshot dukungan baru dari AMI target.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*::image/*",
                "arn:aws:ec2:*::snapshot/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Contoh kebijakan IAM untuk menyalin AMI yang didukung Amazon S3 dan menandai AMI target

Contoh kebijakan berikut memberi Anda izin untuk menyalin AMI yang didukung Amazon S3 di bucket sumber yang ditentukan ke Wilayah yang ditentukan, dan menandai AMI target.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-111122223333-in-us-east-2-hash"
            ]
        }
    ]
}
```

Untuk menemukan Nama Sumber Daya Amazon (ARN) bucket sumber AMI, buka konsol Amazon EC2 https://console.aws.amazon.com/ec2/di, di panel navigasi AMIspilih, dan cari nama bucket di kolom Sumber.

> **Note**
>
> `s3:CreateBucket`Izin hanya diperlukan saat pertama kali Anda menyalin AMI yang didukung Amazon S3 ke Wilayah individual. Setelah itu, bucket Amazon S3 yang sudah dibuat di Wilayah digunakan untuk menyimpan semua future AMIs yang Anda salin ke Wilayah tersebut.

Menyalin AMI

Anda dapat menyalin AMI yang Anda miliki atau AMI yang dibagikan dengan Anda dari akun lain. Untuk kombinasi sumber dan tujuan yang didukung, lihatPertimbangan-pertimbangan.

Console

Untuk menyalin AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari bilah navigasi konsol, pilih Wilayah yang berisi AMI.
3. Di panel navigasi, pilih AMIsuntuk menampilkan daftar yang AMIs tersedia untuk Anda di Wilayah.
4. Jika Anda tidak melihat AMI yang ingin Anda salin, pilih filter yang berbeda. Anda dapat memfilter berdasarkan AMIs Dimiliki oleh saya, Gambar pribadi, Gambar publik, dan gambar Dinonaktifkan.
5. Pilih AMI yang akan disalin, lalu pilih Tindakan, Salin AMI.
6. Pada halaman Salin Gambar Mesin Amazon (AMI), tentukan informasi berikut:

    a. Nama salinan AMI: Nama untuk AMI baru. Anda dapat menyertakan informasi sistem operasi dalam nama karena Amazon EC2 tidak memberikan informasi ini saat menampilkan detail tentang AMI.

    b. Deskripsi salinan AMI: Secara default, deskripsi mencakup informasi tentang AMI sumber sehingga Anda dapat membedakan salinan dari aslinya. Anda dapat mengubah deskripsi ini sesuai kebutuhan.

c. Wilayah Tujuan: Wilayah untuk menyalin AMI. Untuk informasi selengkapnya, lihat Penyalinan Lintas Wilayah dan Penyalinan lintas akun.

d. Salin tag: Pilih kotak centang ini untuk menyertakan tag AMI yang ditentukan pengguna saat menyalin AMI. Tag sistem (diawali dengan `aws:`) dan tag yang ditentukan pengguna yang dilampirkan oleh Akun AWS lain tidak akan disalin.

e. Salinan berbasis waktu: Anda dapat menentukan apakah operasi penyalinan selesai dalam jangka waktu tertentu atau berdasarkan upaya terbaik, sebagai berikut:

- Untuk melengkapi salinan dalam jangka waktu tertentu:
  - Pilih Aktifkan salinan berbasis waktu.
  - Untuk durasi Penyelesaian, masukkan jumlah menit (dalam kenaikan 15 menit) yang diizinkan untuk operasi penyalinan. Durasi penyelesaian berlaku untuk semua snapshot yang terkait dengan AMI.

    Untuk informasi selengkapnya, lihat Salinan berbasis waktu di Panduan Pengguna Amazon EBS.
- Untuk melengkapi salinan dengan upaya terbaik:
  - Biarkan Aktifkan salinan berbasis waktu tidak dipilih.

f. (AMIs Hanya didukung EBS) Enkripsi snapshot EBS dari salinan AMI: Pilih kotak centang ini untuk mengenkripsi snapshot target, atau untuk mengenkripsi ulang mereka menggunakan kunci yang berbeda. Jika enkripsi secara default diaktifkan, kotak centang Enkripsi snapshot EBS dari salinan AMI dipilih dan tidak dapat dihapus. Untuk informasi selengkapnya, lihat Enkripsi dan penyalinan.

g. (AMIs Hanya didukung EBS) Kunci KMS: Kunci KMS yang digunakan untuk mengenkripsi snapshot target.

h. Tag: Anda dapat menandai AMI baru dan snapshot baru dengan tag yang sama, atau Anda dapat menandai mereka dengan tag yang berbeda.

- Untuk menandai AMI baru dan snapshot baru dengan tag yang sama, pilih Tag image dan snapshot bersama-sama. Tag yang sama diterapkan ke AMI baru dan setiap snapshot yang dibuat.
- Untuk menandai AMI baru dan snapshot baru dengan tag yang berbeda, pilih Tag image dan snapshot secara terpisah. Tag yang berbeda diterapkan ke AMI baru dan snapshot yang dibuat. Namun, perhatikan bahwa semua snapshot baru yang

dibuat mendapatkan tag yang sama; Anda tidak dapat menandai setiap snapshot baru dengan tag yang berbeda.

Untuk menambahkan tag , pilih Tambahkan tag dan masukkan kunci dan nilai tag. Ulangi hal itu untuk setiap tanda.

i. Saat Anda siap untuk menyalin AMI, pilih Salin AMI.

Status awal AMI baru adalah `Pending`. Operasi penyalinan AMI selesai saat statusnya `Available`.

AWS CLI

Untuk menyalin AMI dari satu Wilayah ke Wilayah lain

Gunakan perintah copy-image. Anda harus menentukan Wilayah sumber dan tujuan. Anda menentukan Wilayah sumber menggunakan parameter `--source-region`. Anda dapat menentukan Wilayah tujuan menggunakan `--region` parameter (atau menghilangkan parameter ini untuk mengasumsikan Wilayah default yang dikonfigurasi dalam AWS CLI pengaturan Anda).

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region us-west-2 \
    --name my-ami \
    --region us-east-1
```

Saat Anda mengenkripsi snapshot target selama penyalinan AMI, Anda harus menentukan parameter tambahan ini: `--encrypted` dan. `--kms-key-id`

Untuk menyalin AMI dari Wilayah ke Zona Lokal

Gunakan perintah copy-image. Anda harus menentukan sumber dan tujuan. Anda menentukan Wilayah sumber menggunakan parameter `--source-region`. Anda menentukan tujuan Local Zone menggunakan `--destination-availability-zone` parameter (Anda dapat menggunakan `--destination-availability-zone-id` sebagai gantinya). Perhatikan bahwa Anda hanya dapat menyalin AMI dari Wilayah ke Zona Lokal dalam Wilayah yang sama.

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
```

```
    --destination-availability-zone cn-north-1-pkx-1a \
    --name my-ami \
    --region cn-north-1
```

Untuk menyalin AMI dari Zona Lokal ke Wilayah

Gunakan perintah copy-image. Anda harus menentukan sumber dan tujuan. Anda menentukan Wilayah sumber menggunakan parameter `--source-region`. Anda menentukan Wilayah tujuan menggunakan `--region` parameter (atau menghilangkan parameter ini untuk mengasumsikan Wilayah default yang dikonfigurasi dalam AWS CLI pengaturan Anda). Sumber Local Zone diasumsikan dari lokasi ID AMI sumber yang ditentukan. Perhatikan bahwa Anda hanya dapat menyalin AMI dari Zona Lokal ke Wilayah induknya.

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --name my-ami \
    --region cn-north-1
```

Untuk menyalin AMI dari satu Zona Lokal ke Zona Lokal lainnya

Gunakan perintah copy-image. Anda harus menentukan sumber dan tujuan. Anda menentukan wilayah sumber dari zona lokal menggunakan `--source-region` parameter. Anda menentukan tujuan Local Zone menggunakan `--destination-availability-zone` parameter (Anda dapat menggunakan `--destination-availability-zone-id` sebagai gantinya). Sumber Local Zone diasumsikan dari lokasi ID AMI sumber yang ditentukan. Anda menentukan Wilayah induk dari Zona Lokal tujuan menggunakan `--region` parameter (atau menghilangkan parameter ini untuk mengasumsikan Wilayah default yang dikonfigurasi dalam AWS CLI pengaturan Anda).

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --destination-availability-zone cn-north-1-pkx-1a \
    --name my-ami \
    --region cn-north-1
```

PowerShell

Untuk menyalin AMI dari satu Wilayah ke Wilayah lain

Gunakan Copy-EC2Imagecmdlet. Anda harus menentukan Wilayah sumber dan tujuan. Anda menentukan Wilayah sumber menggunakan parameter `-SourceRegion`. Anda dapat menentukan Wilayah tujuan menggunakan `-Region` parameter atau cmdlet Set- AWSDefault Region.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion us-west-2 `
    -Name my-ami `
    -Region us-east-1
```

Saat Anda mengenkripsi snapshot target selama penyalinan AMI, Anda harus menentukan parameter tambahan ini: `-Encrypted` dan. `-KmsKeyId`

Untuk menyalin AMI dari Wilayah ke Zona Lokal

Gunakan Copy-EC2Imagecmdlet. Anda harus menentukan sumber dan tujuan. Anda menentukan Wilayah sumber menggunakan parameter `-SourceRegion`. Anda menentukan tujuan Local Zone menggunakan `-DestinationAvailabilityZone` parameter (Anda dapat menggunakan `-DestinationAvailabilityZoneId` sebagai gantinya). Perhatikan bahwa Anda hanya dapat menyalin AMI dari Wilayah ke Zona Lokal dalam Wilayah yang sama.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -DestinationAvailabilityZone cn-north-1-pkx-1a `
    -Name my-ami `
    -Region cn-north-1
```

Untuk menyalin AMI dari Zona Lokal ke Wilayah

Gunakan Copy-EC2Imagecmdlet. Anda harus menentukan sumber dan tujuan. Anda menentukan Wilayah sumber menggunakan parameter `-SourceRegion`. Anda menentukan Wilayah tujuan menggunakan `-Region` parameter atau cmdlet Set- AWSDefault Region. Sumber Local Zone diasumsikan dari lokasi ID AMI sumber yang ditentukan. Perhatikan bahwa Anda hanya dapat menyalin AMI dari Zona Lokal ke Wilayah induknya.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
```

```
    -Name my-ami `
    -Region cn-north-1
```

Untuk menyalin AMI dari satu Zona Lokal ke Zona Lokal lainnya

Gunakan Copy-EC2Imagecmdlet. Anda harus menentukan sumber dan tujuan. Anda menentukan wilayah sumber dari zona lokal menggunakan `-SourceRegion` parameter. Anda menentukan tujuan Local Zone menggunakan `-DestinationAvailabilityZone` parameter (Anda dapat menggunakan `-DestinationAvailabilityZoneId` sebagai gantinya). Sumber Local Zone diasumsikan dari lokasi ID AMI sumber yang ditentukan. Anda menentukan Wilayah induk dari Zona Lokal tujuan menggunakan `-Region` parameter atau cmdlet Set- AWSDefault Region.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -DestinationAvailabilityZone cn-north-1-pkx-1a `
    -Name my-ami `
    -Region cn-north-1
```

Menghentikan operasi penyalinan AMI yang tertunda

Anda dapat menghentikan salinan AMI yang tertunda menggunakan prosedur berikut.

Console

Untuk menghentikan operasi penyalinan AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari bilah navigasi, pilih Wilayah tujuan dari pemilih Wilayah.
3. Di panel navigasi, pilih AMIs.
4. Pilih AMI untuk berhenti menyalin, lalu pilih Actions, Deregister AMI.
5. Saat diminta konfirmasi, pilih Batalkan pendaftaran AMI.

AWS CLI

Untuk menghentikan operasi penyalinan AMI

Gunakan perintah deregister-image.

```
aws ec2 deregister-image --image-id ami-0abcdef1234567890
```

PowerShell

Untuk menghentikan operasi penyalinan AMI menggunakan

Gunakan Unregister-EC2Imagecmdlet.

```
Unregister-EC2Image -ImageId ami-0abcdef1234567890
```

Cara kerja salinan Amazon EC2 AMI

Menyalin AMI sumber menghasilkan AMI baru yang identik namun berbeda yang juga kami sebut sebagai AMI target. Target AMI memiliki ID AMI uniknya sendiri. Anda dapat mengubah atau membatalkan pendaftaran AMI sumber tanpa memengaruhi AMI target. Begitu juga sebaliknya.

Dengan AMI yang didukung EBS, setiap snapshot pendukungnya disalin ke snapshot target yang identik namun berbeda. Jika Anda menyalin AMI ke Wilayah baru, snapshot tersebut merupakan salinan lengkap (non-inkremental). Jika Anda mengenkripsi snapshot dukungan yang tidak dienkripsi atau mengenkripsinya ke kunci KMS baru, snapshot tersebut merupakan salinan lengkap (non-inkremental). Operasi penyalinan AMI berikutnya akan menghasilkan salinan inkremental dari snapshot cadangan.

Daftar Isi

- Penyalinan Lintas Wilayah
- Penyalinan lintas akun
- Operasi penyalinan AMI berbasis waktu
- Enkripsi dan penyalinan

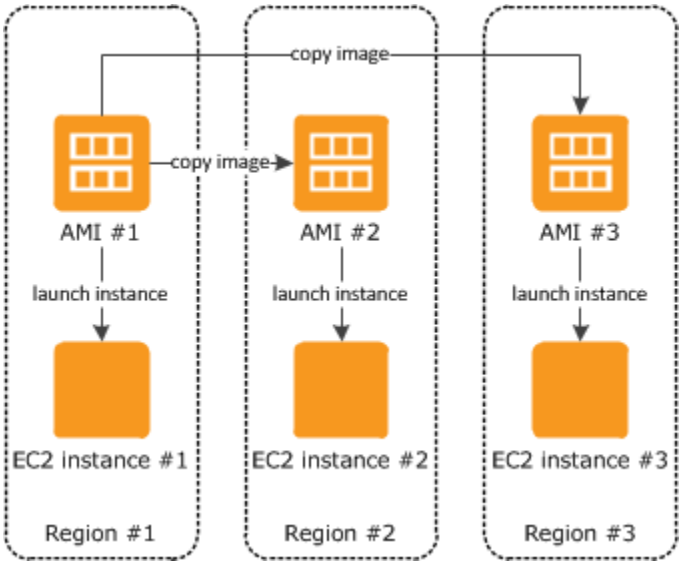
Penyalinan Lintas Wilayah

Menyalin AMI di Wilayah yang berbeda secara geografis memiliki keuntungan berikut:

- Deployment global yang konsisten: Menyalin AMI dari satu Wilayah ke Wilayah lain memungkinkan Anda meluncurkan instans yang konsisten di Wilayah yang berbeda berdasarkan AMI yang sama.
- Skalabilitas: Anda dapat dengan lebih mudah merancang dan membangun aplikasi global yang memenuhi kebutuhan pengguna Anda, terlepas dari lokasi mereka.

- Performa: Anda dapat meningkatkan performa dengan mendistribusikan aplikasi Anda, serta menemukan komponen penting pada aplikasi Anda dalam jarak yang lebih dekat dengan pengguna Anda. Anda juga dapat memanfaatkan fitur spesifik Wilayah, seperti tipe instans atau layanan AWS lainnya.
- Ketersediaan tinggi: Anda dapat merancang dan melakukan deploy aplikasi di berbagai Wilayah AWS , untuk meningkatkan ketersediaan.

Diagram berikut menunjukkan hubungan antara AMI sumber dan dua AMI yang disalin di Wilayah yang berbeda, serta instans EC2 yang diluncurkan dari masing-masing. Saat Anda meluncurkan instans dari sebuah AMI, instans tersebut berada di Wilayah yang sama dengan AMI berada. Jika Anda membuat perubahan pada AMI sumber dan ingin perubahan tersebut tercermin AMIs di Wilayah target, Anda harus menyalin ulang AMI sumber ke Wilayah target.



Saat pertama kali menyalin AMI yang didukung Amazon S3 ke Wilayah, kami membuat bucket Amazon S3 untuk disalin ke Wilayah AMIs tersebut. Semua yang didukung Amazon S3 AMIs yang Anda salin ke Wilayah tersebut disimpan dalam bucket ini. Nama bucket memiliki format berikut: amis-for- *account* -in- -*region*. *hash* Sebagai contoh: `amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Prasyarat

Sebelum menyalin AMI, Anda harus memastikan konten AMI sumber telah diperbarui agar dapat berjalan di Wilayah yang berbeda. Misalnya, Anda harus memperbarui setiap string koneksi basis data atau data konfigurasi aplikasi serupa untuk mengarah ke sumber daya yang sesuai. Jika tidak,

instans yang diluncurkan dari AMI baru di Wilayah tujuan mungkin masih menggunakan sumber daya dari Wilayah sumber, yang dapat memengaruhi kinerja dan biaya.

Batasan

- Wilayah Tujuan dibatasi hingga 300 operasi penyalinan AMI bersamaan. Ini juga berlaku untuk operasi penyalinan AMI berbasis waktu.
- Anda tidak dapat menyalin AMI paravirtual (PV) ke Wilayah yang tidak mendukung PV. AMIs Untuk informasi selengkapnya, lihat Tipe virtualisasi.

Penyalinan lintas akun

Jika AMI dari yang lain Akun AWS dibagikan dengan Anda Akun AWS, Anda dapat menyalin AMI bersama. Ini dikenal sebagai penyalinan lintas akun. AMI yang dibagikan dengan Anda adalah sumber AMI. Saat Anda menyalin sumber AMI, Anda membuat AMI baru. AMI baru sering disebut sebagai target AMI.

Biaya AMI

- Untuk AMI bersama, akun AMI bersama dikenakan biaya untuk penyimpanan di Wilayah.
- Jika Anda menyalin AMI yang dibagikan dengan akun Anda, Anda adalah pemilik AMI target di akun Anda.
  - Pemilik sumber AMI dikenakan biaya transfer Amazon EBS atau Amazon S3 standar.
  - Anda dikenakan biaya untuk penyimpanan AMI target di Wilayah tujuan.

Izin Sumber Daya

Untuk menyalin AMI yang dibagikan dengan Anda dari akun lain, pemilik sumber AMI harus memberi Anda izin baca untuk penyimpanan yang mendukung AMI, bukan hanya untuk AMI itu sendiri. Penyimpanan adalah snapshot EBS terkait (untuk AMI yang didukung Amazon EBS-backed) atau bucket S3 terkait (untuk AMI yang didukung Amazon S3). Jika AMI bersama memiliki snapshot terenkripsi, pemilik harus membagikan kunci atau kunci dengan Anda. Untuk informasi selengkapnya tentang pemberian izin sumber daya, untuk snapshot EBS, lihat Membagikan snapshot Amazon EBS dengan yang lain di Akun AWS Panduan Pengguna Amazon EBS, dan untuk bucket S3, lihat Manajemen identitas dan akses untuk Amazon S3 di Panduan Pengguna Amazon S3.

> **Note**
>
> Tag yang dilampirkan ke sumber AMI tidak disalin di seluruh akun ke AMI target.

Operasi penyalinan AMI berbasis waktu

Saat Anda memulai operasi penyalinan AMI berbasis waktu untuk AMI yang didukung EBS dengan satu snapshot terkait, ia berperilaku dengan cara yang sama seperti operasi penyalinan snapshot berbasis waktu individual, dan batasan throughput yang sama berlaku.

Saat Anda memulai operasi penyalinan AMI berbasis waktu untuk AMI yang didukung EBS dengan beberapa snapshot terkait, ia berperilaku dengan cara yang sama seperti operasi penyalinan snapshot berbasis waktu bersamaan, dan batasan throughput yang sama berlaku. Setiap snapshot terkait menghasilkan permintaan salinan snapshot terpisah, yang masing-masing berkontribusi pada kuota throughput salinan snapshot kumulatif Anda. Durasi penyelesaian yang Anda tentukan berlaku untuk setiap snapshot terkait.

Untuk informasi selengkapnya, lihat Salinan berbasis waktu di Panduan Pengguna Amazon EBS.

Enkripsi dan penyalinan

Tabel berikut ini menunjukkan dukungan enkripsi untuk berbagai skenario penyalinan AMI. Meskipun Anda dapat menyalin snapshot yang tidak terenkripsi untuk menghasilkan snapshot yang terenkripsi, Anda tidak dapat menyalin snapshot yang terenkripsi untuk menghasilkan snapshot yang tidak terenkripsi.

Skenario	Deskripsi	Didukung
1	Tidak terenkripsi ke tidak terenkripsi	Ya
2	Dienkripsi untuk dienkripsi	Ya
3	Tidak terenkripsi untuk dienkripsi	Ya
4	Terenkripsi ke tidak terenkripsi	Tidak

> **Note**
>
> Enkripsi selama `CopyImage` tindakan hanya berlaku untuk Amazon EBS yang didukung. AMIs Karena AMI yang didukung Amazon S3 tidak menggunakan snapshot, Anda tidak dapat menggunakan penyalinan untuk mengubah status enkripsi.

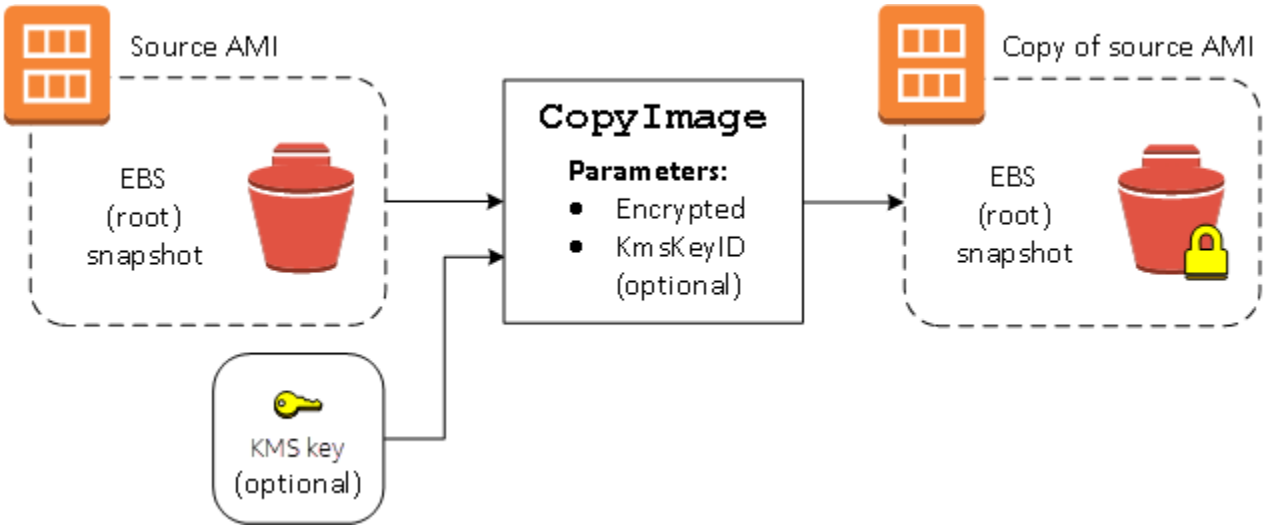
Saat Anda menyalin AMI tanpa menentukan parameter enkripsi, snapshot dukungan disalin dengan status enkripsi aslinya secara default. Oleh karena itu, jika sumber AMI didukung oleh snapshot yang tidak terenkripsi, snapshot target yang dihasilkan juga akan tidak dienkripsi. Demikian pula, jika snapshot sumber AMI dienkripsi, snapshot target yang dihasilkan juga akan dienkripsi dengan kunci yang sama. AWS KMS Untuk AMIs didukung oleh beberapa snapshot, setiap snapshot target mempertahankan status enkripsi snapshot sumber yang sesuai.

Untuk mengubah status enkripsi snapshot dukungan target selama salinan AMI, Anda dapat menentukan parameter enkripsi. Contoh berikut menunjukkan kasus non-default, di mana parameter enkripsi ditentukan dengan `CopyImage` tindakan untuk mengubah status enkripsi AMI target.

Menyalin AMI sumber yang tidak terenkripsi ke AMI target yang dienkripsi

Dalam skenario ini, AMI yang didukung oleh snapshot root yang tidak dienkripsi disalin ke AMI dengan snapshot root yang dienkripsi. Tindakan `CopyImage` diinvokasi dengan dua parameter enkripsi, termasuk kunci yang dikelola konsumen. Hasilnya, status enkripsi root snapshot berubah sehingga AMI target didukung oleh snapshot root yang berisi data yang sama dengan snapshot sumber, tetapi dienkripsi menggunakan kunci yang ditentukan. Anda dikenakan biaya penyimpanan untuk snapshot di keduanyaAMIs, serta biaya untuk setiap instance yang Anda luncurkan dari AMI.

> **Note**
>
> Mengaktifkan enkripsi secara default memiliki efek yang sama seperti mengatur `Encrypted` parameter `true` untuk semua snapshot di AMI.



Mengatur parameter `Encrypted` akan mengenkripsi snapshot tunggal untuk instans ini. Jika Anda tidak menentukan parameter `KmsKeyId`, kunci default yang dikelola konsumen akan digunakan untuk mengenkripsi salinan snapshot.

Untuk informasi selengkapnya tentang menyalin AMIs dengan snapshot terenkripsi, lihat. Gunakan enkripsi dengan dukungan EBS AMIs

Simpan dan pulihkan AMI menggunakan S3

Anda dapat menyimpan Amazon Machine Image (AMI) dalam bucket Amazon S3, menyalin AMI ke bucket S3 lain, lalu memulihkannya dari bucket S3. Dengan menyimpan dan memulihkan AMI menggunakan bucket S3, Anda dapat menyalin AMIs dari satu AWS partisi ke partisi lainnya, misalnya, dari partisi komersial utama ke partisi. AWS GovCloud (US) Anda juga dapat membuat salinan arsip AMIs dengan menyimpannya di ember S3.

Yang didukung APIs untuk menyimpan dan memulihkan AMI menggunakan S3 adalah`CreateStoreImageTask`,`DescribeStoreImageTasks`, dan. `CreateRestoreImageTask`

`CopyImage`adalah API yang direkomendasikan untuk digunakan untuk menyalin AMIs dalam AWS partisi. Namun, `CopyImage` tidak dapat menyalin AMI ke partisi lain.

Untuk informasi tentang AWS partisi, lihat *`partition`* di halaman Amazon Resource Names (ARNs) di Panduan Pengguna IAM.

> **Warning**
>
> Pastikan Anda mematuhi semua hukum dan persyaratan bisnis yang berlaku saat memindahkan data antar AWS partisi atau AWS Wilayah, termasuk, namun tidak terbatas pada, peraturan pemerintah dan persyaratan residensi data yang berlaku.

Daftar Isi

- Kasus penggunaan
- Batasan
- Biaya
- Cara kerja penyimpanan dan pemulihan AMI
- Buat tugas gambar toko

Kasus penggunaan

Gunakan toko dan pulihkan APIs untuk melakukan hal berikut:

- Salin AMI antar AWS partisi
- Buat salinan arsip AMIs

Salin AMI antar AWS partisi

Dengan menyimpan dan memulihkan AMI menggunakan bucket S3, Anda dapat menyalin AMI dari satu AWS partisi ke partisi lainnya, atau dari satu AWS Wilayah ke wilayah lainnya. Dalam contoh berikut, Anda menyalin AMI dari partisi komersial utama ke AWS GovCloud (US) partisi, khususnya dari `us-east-2` Wilayah ke `us-gov-east-1` Wilayah.

Untuk menyalin AMI dari satu partisi ke partisi lain, ikuti langkah berikut:

- Menyimpan AMI dalam bucket S3 di Wilayah saat ini dengan menggunakan `CreateStoreImageTask`. Dalam contoh ini, bucket S3 terletak di `us-east-2`.
- Pantau kemajuan tugas penyimpanan dengan menggunakan `DescribeStoreImageTasks`. Objek akan terlihat dalam bucket S3 ketika tugas selesai.
- Salin objek AMI yang tersimpan ke bucket S3 di partisi target menggunakan prosedur pilihan Anda. Dalam contoh ini, bucket S3 terletak di `us-gov-east-1`.

> **Note**
>
> Karena Anda memerlukan AWS kredensi yang berbeda untuk setiap partisi, Anda tidak dapat menyalin objek S3 langsung dari satu partisi ke partisi lainnya. Proses untuk menyalin objek S3 di seluruh partisi berada di luar lingkup dokumentasi ini. Kami menyediakan proses penyalinan berikut sebagai contoh, namun Anda harus menggunakan proses penyalinan yang memenuhi persyaratan keamanan Anda.
>
> - Untuk menyalin satu AMI antar partisi, proses penyalinan dapat sesederhana berikut ini: Unduh objek dari bucket sumber ke host perantara (misalnya, instans EC2 atau laptop), lalu unggah objek tersebut dari host perantara ke bucket target. Untuk setiap tahap proses, gunakan AWS kredensil untuk partisi.
> - Untuk penggunaan yang lebih berkelanjutan, pertimbangkan untuk mengembangkan aplikasi yang mengelola salinan, yang berpotensi menggunakan unduhan dan unggahan multipart S3.

- Pulihkan AMI dari S3 bucket di partisi target dengan menggunakan `CreateRestoreImageTask`. Dalam contoh ini, bucket S3 terletak di `us-gov-east-1`.
- Pantau kemajuan tugas pemulihan dengan menggambarkan AMI untuk memeriksa kapan status menjadi tersedia. Anda juga dapat memantau persentase kemajuan dari snapshot yang membentuk AMI yang dipulihkan dengan menggambarkan snapshot.

Buat salinan arsip AMIs

Anda dapat membuat salinan arsip AMIs dengan menyimpannya dalam ember S3. AMI dikemas ke dalam satu objek di S3, dan semua metadata AMI (tidak termasuk berbagi informasi) dipertahankan sebagai bagian dari AMI yang disimpan. Data AMI dikompresi sebagai bagian dari proses penyimpanan. AMIs yang berisi data yang dapat dengan mudah dikompresi akan menghasilkan objek yang lebih kecil di S3. Untuk mengurangi biaya, Anda dapat menggunakan kelas penyimpanan S3 yang lebih murah. Untuk informasi selengkapnya, lihat Kelas Penyimpanan Amazon S3 dan Harga Amazon S3

Batasan

- Untuk menyimpan AMI, Anda Akun AWS harus memiliki AMI dan fotonya, atau AMI dan fotonya harus dibagikan langsung dengan akun Anda. Anda tidak dapat menyimpan AMI jika AMI tersebut hanya dibagikan secara publik.

- Hanya EBS yang didukung AMIs dapat disimpan menggunakan ini. APIs
- Paravirtual (PV) AMIs tidak didukung.
- Ukuran AMI (sebelum kompresi) yang dapat disimpan dibatasi hingga 5.000 GB.
- Kuota permintaan gambar toko: 1.200 GB pekerjaan penyimpanan (data snapshot) sedang berlangsung.
- Kuota untuk mengembalikan permintaan gambar: 600 GB pekerjaan pemulihan (data snapshot) sedang berlangsung.
- Untuk durasi tugas penyimpanan, snapshot tidak boleh dihapus dan pengguna utama IAM yang melakukan penyimpanan harus memiliki akses ke snapshot, jika tidak maka proses penyimpanan akan gagal.
- Anda tidak dapat membuat beberapa salinan AMI dalam bucket S3 yang sama.
- AMI yang disimpan dalam bucket S3 tidak dapat dipulihkan dengan ID AMI asalnya. Anda dapat memitigasi hal ini dengan menggunakan alias AMI.
- Saat ini penyimpanan dan pemulihan hanya APIs didukung dengan menggunakan AWS Command Line Interface, AWS SDK, dan Amazon EC2 API. Anda tidak dapat menyimpan dan memulihkan AMI menggunakan konsol Amazon EC2.

Biaya

Ketika Anda menyimpan dan memulihkan AMIs menggunakan S3, Anda dikenakan biaya untuk layanan yang digunakan oleh toko dan memulihkan APIs, dan untuk transfer data. APIs Penggunaan S3 dan EBS Direct API (digunakan secara internal oleh ini APIs untuk mengakses data snapshot). Untuk informasi selengkapnya, lihat harga Amazon S3 dan harga Amazon EBS.

Cara kerja penyimpanan dan pemulihan AMI

Untuk menyimpan dan memulihkan AMI menggunakan S3, Anda menggunakan yang berikut ini: APIs

- `CreateStoreImageTask` – Menyimpan AMI dalam bucket S3
- `DescribeStoreImageTasks` – Menyediakan kemajuan tugas penyimpanan AMI
- `CreateRestoreImageTask` – Memulihkan AMI dari bucket S3

Bagaimana cara APIs kerjanya

- CreateStoreImageTask
- DescribeStoreImageTasks

- CreateRestoreImageTask
- Jalur file

CreateStoreImageTask

`CreateStoreImageTask`API menyimpan AMI sebagai objek tunggal dalam bucket S3.

API menciptakan tugas yang membaca semua data dari AMI dan snapshot-nya, lalu menggunakan Unggahan multipart S3 untuk menyimpan data dalam objek S3. API mengambil semua komponen AMI, termasuk sebagian besar metadata non-Region-specific AMI, dan semua snapshot EBS yang terdapat dalam AMI, dan mengemasnya menjadi satu objek di S3. Data dikompresi sebagai bagian dari proses unggahan untuk mengurangi jumlah ruang yang digunakan di S3, sehingga objek di S3 mungkin lebih kecil dari jumlah ukuran snapshot di AMI.

Jika terlihat ada tag AMI dan snapshot ke akun yang memanggil API ini, tag tersebut dipertahankan.

Objek di S3 memiliki ID yang sama dengan AMI, tetapi dengan ekstensi `.bin`. Data berikut ini juga disimpan sebagai tag metadata S3 pada objek S3: nama AMI, deskripsi AMI, tanggal pendaftaran AMI, akun pemilik AMI, dan stempel waktu untuk operasi penyimpanan.

Waktu yang diperlukan untuk menyelesaikan tugas tergantung pada ukuran AMI. Hal ini juga bergantung pada berapa banyak tugas lain yang berlangsung karena tugas diantrekan. Anda dapat melacak kemajuan tugas dengan memanggil `DescribeStoreImageTasks` API.

Jumlah ukuran semua yang sedang berlangsung dibatasi hingga 1.200 GB data snapshot EBS per akun. AMIs Penciptaan tugas lebih lanjut akan ditolak sampai tugas yang sedang berlangsung kurang dari batasan tersebut. Misalnya, jika AMI dengan data snapshot 200 GB dan AMI lain dengan data snapshot 400 GB saat ini sedang disimpan, permintaan lain akan diterima, karena total yang sedang berlangsung adalah 600 GB, yang kurang dari batas. Tetapi jika satu AMI dengan 1.200 GB data snapshot saat ini sedang disimpan, tugas lebih lanjut ditolak hingga tugas selesai.

DescribeStoreImageTasks

`DescribeStoreImageTasks`API menjelaskan kemajuan tugas penyimpanan AMI. Anda dapat menjelaskan tugas untuk ditentukan AMIs. Jika Anda tidak menentukan AMIs, Anda mendapatkan daftar paginasi dari semua tugas gambar toko yang telah diproses dalam 31 hari terakhir.

Untuk setiap tugas AMI, respons menunjukkan jika tugas tersebut adalah `InProgress`, `Completed`, atau `Failed`. Untuk tugas `InProgress`, respons menunjukkan perkiraan kemajuan sebagai persentase.

Tugas tercantum dalam urutan kronologis terbalik.

Saat ini, hanya tugas dari bulan sebelumnya yang dapat dilihat.

CreateRestoreImageTask

`CreateRestoreImageTask`API memulai tugas yang mengembalikan AMI dari objek S3 yang sebelumnya dibuat dengan menggunakan permintaan. `CreateStoreImageTask`

Tugas pemulihan dapat dilakukan di Wilayah yang sama atau berbeda dari tempat tugas penyimpanan dilakukan.

Bucket S3 tempat objek AMI akan dipulihkan harus berada di Wilayah yang sama dengan tempat tugas pemulihan diminta. AMI akan dipulihkan di Wilayah ini.

AMI dipulihkan dengan metadata-nya, seperti nama, deskripsi, dan pemetaan perangkat blok yang sesuai dengan nilai-nilai AMI yang tersimpan. Nama harus unik untuk AMIs di Wilayah untuk akun ini. Jika Anda tidak memberikan nama, AMI yang baru akan mendapat nama yang sama dengan AMI asal. AMI akan mendapat ID AMI baru yang dihasilkan pada saat proses pemulihan.

Waktu yang diperlukan untuk menyelesaikan tugas pemulihan AMI bergantung pada ukuran AMI. Hal ini juga bergantung pada berapa banyak tugas lain yang berlangsung karena tugas diantrekan. Anda dapat melihat kemajuan tugas dengan menggambarkan AMI (describe-images) atau snapshot EBS-nya (describe-snapshot). Jika tugas gagal, AMI dan snapshot akan dipindahkan ke status gagal.

Jumlah ukuran semua yang sedang berlangsung dibatasi hingga 600 GB (berdasarkan ukuran setelah pemulihan) data snapshot EBS per akun. AMIs Penciptaan tugas lebih lanjut akan ditolak sampai tugas yang sedang berlangsung kurang dari batasan tersebut.

Jalur file

Anda dapat menggunakan jalur file saat menyimpan dan memulihkan AMIs, dengan cara berikut:

- Saat menyimpan AMI di S3, jalur file dapat ditambahkan ke nama bucket. Secara internal, sistem memisahkan jalur dari nama bucket, lalu menambahkan jalur ke kunci objek yang dibuat untuk menyimpan AMI. Jalur objek lengkap ditampilkan dalam respons dari panggilan API.
- Saat memulihkan AMI, karena parameter kunci objek tersedia, jalur dapat ditambahkan ke awal nilai kunci objek.

Contoh: Nama bucket dengan path file yang ditambahkan

Saat Anda menyimpan AMI, tentukan path file setelah nama bucket.

```
amzn-s3-demo-bucket/path1/path2
```

Berikut ini adalah kunci objek yang dihasilkan.

```
path1/path2/ami-0abcdef1234567890.bin
```

Saat memulihkan AMI, Anda menentukan nama bucket dan kunci objek. Sebagai contoh, lihat the section called “Buat tugas gambar toko”.

Buat tugas gambar toko

Saat Anda menyimpan AMI di bucket S3, tugas gambar toko akan dibuat. Anda dapat menggunakan tugas gambar toko untuk memantau kemajuan dan hasil proses.

Daftar Isi

- Mengamankan AMIs
- Izin untuk menyimpan dan memulihkan menggunakan S3 AMIs
- Buat tugas gambar toko
- Buat tugas mengembalikan gambar

Mengamankan AMIs

Penting untuk memastikan bahwa bucket S3 dikonfigurasi dengan keamanan yang cukup untuk mengamankan konten AMI dan bahwa keamanan dipertahankan selama objek AMI berada di dalam bucket. Jika ini tidak dapat dilakukan, penggunaan ini tidak APIs dianjurkan. Pastikan bahwa akses publik ke bucket S3 tidak diperbolehkan. Sebaiknya aktifkan enkripsi sisi Server untuk bucket S3 tempat Anda menyimpan AMIs, meskipun tidak diperlukan.

Untuk informasi tentang cara mengatur pengaturan keamanan yang sesuai untuk bucket S3 Anda, tinjau topik keamanan berikut:

- Memblokir akses publik ke penyimpanan Amazon S3 Anda
- Mengatur perilaku enkripsi sisi server default untuk bucket Amazon S3
- Kebijakan bucket S3 apa yang dapat saya gunakan untuk mematuhi AWS Config aturan s3-?bucket-ssl-requests-only
- Mengaktifkan logging akses server Amazon S3

Ketika snapshot AMI disalin ke objek S3, data kemudian disalin melalui koneksi TLS. Anda dapat menyimpan AMIs dengan snapshot terenkripsi, tetapi snapshot didekripsi sebagai bagian dari proses penyimpanan.

Izin untuk menyimpan dan memulihkan menggunakan S3 AMIs

Jika kepala sekolah IAM Anda akan menyimpan atau memulihkan menggunakan Amazon AMIs S3, Anda harus memberi mereka izin yang diperlukan.

Contoh kebijakan berikut ini mencakup semua tindakan yang diperlukan untuk memungkinkan pengguna utama IAM melaksanakan tugas penyimpanan dan pemulihan.

Anda juga dapat membuat kebijakan IAM yang memberikan akses kepada pengguna utama hanya ke sumber daya tertentu. Untuk kebijakan contoh lainnya, lihat Manajemen akses untuk AWS sumber daya di Panduan Pengguna IAM.

> **Note**
>
> Jika snapshot yang membentuk AMI dienkripsi, atau jika akun Anda diaktifkan untuk enkripsi secara default, pengguna utama IAM Anda harus memiliki izin untuk menggunakan kunci KMS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
```

```
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Buat tugas gambar toko

Untuk menyimpan AMI di bucket S3, mulailah dengan membuat tugas gambar toko. Waktu yang diperlukan untuk menyelesaikan tugas tergantung pada ukuran AMI. Anda dapat melacak kemajuan tugas sampai berhasil atau gagal.

AWS CLI

Untuk membuat tugas gambar toko

Gunakan perintah create-store-image-task.

```
aws ec2 create-store-image-task \
    --image-id ami-0abcdef1234567890 \
    --bucket amzn-s3-demo-bucket
```

Berikut ini adalah output contoh.

```
{
  "ObjectKey": "ami-0abcdef1234567890.bin"
}
```

Untuk menggambarkan kemajuan tugas gambar toko

Gunakan perintah describe-store-image-tasks.

```
aws ec2 describe-store-image-tasks \
```

```
    --image-ids ami-0abcdef1234567890 \
    --query StoreImageTaskResults[].StoreTaskState \
    --output text
```

Berikut ini adalah output contoh.

```
InProgress
```

PowerShell

Untuk membuat tugas gambar toko

Gunakan New-EC2StoreImageTaskcmdlet.

```
New-EC2StoreImageTask `
    -ImageId ami-0abcdef1234567890 `
    -Bucket amzn-s3-demo-bucket
```

Berikut ini adalah output contoh.

```
ObjectKey         : ami-0abcdef1234567890.bin
```

Untuk menggambarkan kemajuan tugas gambar toko

Gunakan Get-EC2StoreImageTaskcmdlet.

```
(Get-EC2StoreImageTask -ImageId ami-0abcdef1234567890).StoreTaskState
```

Berikut ini adalah output contoh.

```
InProgress
```

Buat tugas mengembalikan gambar

Anda harus menentukan nama untuk AMI yang dipulihkan. Nama harus unik untuk AMIs di Wilayah untuk akun ini. AMI yang dipulihkan akan mendapat ID AMI baru.

AWS CLI

Untuk membuat tugas mengembalikan gambar

Gunakan perintah create-restore-image-task.

```
aws ec2 create-restore-image-task \
    --object-key ami-0abcdef1234567890.bin \
    --bucket amzn-s3-demo-bucket \
    --name "my-restored-ami"
```

Berikut ini adalah output contoh.

```
{
   "ImageId": "ami-1234567890abcdef0"
}
```

PowerShell

Untuk membuat tugas mengembalikan gambar

Gunakan New-EC2RestoreImageTaskcmdlet.

```
New-EC2RestoreImageTask `
    -ObjectKey ami-0abcdef1234567890.bin `
    -Bucket amzn-s3-demo-bucket `
    -Name "my-restored-ami"
```

Berikut ini adalah output contoh.

```
ImageId         : ami-1234567890abcdef0
```

Gunakan keturunan AMI untuk melacak asal usul AMI

Leluhur AMI membantu Anda melacak asal usul AMI dengan mengembalikan IDs dan Wilayah dari semua leluhurnya. AMIs Saat Anda membuat atau menyalin AMI, AMI baru akan mempertahankan ID dan Wilayah AMI sumbernya (induk). Ini memungkinkan Anda untuk melacak rantai AMIs kembali ke root AMI.

Manfaat utama

Menggunakan keturunan AMI membantu Anda:

- Lacak turunan AMI untuk memastikan kepatuhan terhadap kebijakan internal.
- Identifikasi berpotensi rentan AMIs ketika masalah keamanan ditemukan pada AMI leluhur.
- Pertahankan visibilitas asal AMI di beberapa Wilayah.

Topik

- Cara kerja leluhur AMI
- Pertimbangan-pertimbangan
- Lihat keturunan AMI
- Identifikasi sumber AMI

Cara kerja leluhur AMI

Leluhur AMI mengidentifikasi AMI induk yang digunakan untuk membuat AMI yang ditentukan, induk induk, dan sebagainya, hingga AMI root. Begini cara kerjanya:

- Setiap AMI menampilkan ID dan Wilayah AMI sumbernya (induk).
- Dimulai dengan AMI yang Anda pilih, daftar entri leluhur menampilkan setiap AMI induk secara berurutan.
- Daftar entri leluhur ditelusuri kembali hingga mencapai root AMI. Akar AMI adalah salah satu dari yang berikut:
  - AMI publik dari penyedia terverifikasi (diidentifikasi oleh alias pemiliknya, yaitu salah satu `amazon` atau`aws-marketplace`).
  - AMI tanpa leluhur yang tercatat. Misalnya, saat menggunakan RegisterImageuntuk membuat AMI langsung dari sekumpulan snapshot, tidak ada sumber AMI untuk dilacak, tidak seperti saat membuat AMI dari sebuah instance.
  - AMI yang sumbernya AMI berasal dari partisi yang berbeda.
  - AMI ke-50 dalam daftar. Jumlah maksimum AMIs dalam daftar leluhur adalah 50.

Pertimbangan-pertimbangan

- ID dan Wilayah AMI sumber hanya tersedia untuk AMIs dibuat menggunakan CreateImage, CopyImage, atau CreateRestoreImageTask.
- Untuk AMIs dibuat menggunakan CreateImage(membuat AMI dari sebuah instance), ID AMI sumber adalah ID AMI yang digunakan untuk meluncurkan instance.

- Sumber informasi AMI tidak tersedia untuk:
  - AMIs dibuat menggunakan RegisterImagekarena dibuat dari snapshot.
  - Untuk beberapa yang lebih tua AMIs.
- Sumber informasi AMI disimpan ketika:
  - AMIs disalin di seluruh Wilayah.
  - Sumber AMIs dideregistrasi (dihapus).
  - Anda tidak memiliki akses ke sumbernya AMIs.
- Setiap daftar leluhur dibatasi hingga 50. AMIs

Lihat keturunan AMI

Anda dapat melihat leluhur AMI menggunakan metode berikut.

Console

Untuk melihat nenek moyang AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI dan pilih tab keturunan AMI.
4. Tabel entri leluhur AMI mencantumkan semua yang ada AMIs dalam daftar leluhur.
   - ID AMI — Pengidentifikasi setiap AMI dalam daftar leluhur. Entri pertama dalam tabel adalah AMI yang dipilih, diikuti oleh leluhurnya.
   - Sumber AMI ID — ID AMI dari mana AMI di kolom ID AMI dibuat. Tanda hubung (-) menunjukkan akhir dari daftar keturunan AMI.
   - Sumber AMI Region — AWS Region Tempat sumber AMI berada.
   - Tingkat leluhur — Posisi dalam daftar leluhur, di mana:
     - 0 (masukan AMI) menunjukkan AMI yang dipilih yang nenek moyangnya ingin Anda ketahui.
     - Jumlah yang meningkat menunjukkan leluhur yang lebih tua.
     - ***n***(AMI asli) menunjukkan AMI root, dengan nomor yang menunjukkan seberapa jauh daftar leluhur berjalan.
   - Tanggal pembuatan - Saat AMI dibuat, dalam format UTC.

- Alias pemilik — Alias pemilik AMI (misalnya,`amazon`). Tanda hubung (-) menunjukkan bahwa AMI tidak memiliki alias pemilik.

AWS CLI

Untuk melihat nenek moyang AMI

Gunakan perintah get-image-ancestry dan sebutkan ID AMI.

```
aws ec2 get-image-ancestry \
    --image-id ami-1111111111EXAMPLE \
    --region us-east-1
```

Berikut ini adalah output contoh. Daftar keluaran AMIs dalam urutan leluhur: entri pertama adalah AMI (input) yang ditentukan, diikuti oleh induknya, induk induk, dan sebagainya, dan diakhiri dengan root AMI.

```
{
    "ImageAncestryEntries": [
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-1111111111EXAMPLE", // Input AMI
            "SourceImageId": "ami-2222222222EXAMPLE",
            "SourceImageRegion": "us-east-1"

        },
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-2222222222EXAMPLE", // Parent AMI
            "SourceImageId": "ami-3333333333EXAMPLE",
            "SourceImageRegion": "us-east-1"
        },
        ...
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-8888888888EXAMPLE", // Root AMI
            "ImageOwnerAlias": "aws-marketplace",
            "SourceImageId": "ami-9999999999EXAMPLE",
            "SourceImageRegion": "us-east-2"
        }
    ]
```

```
}
```

PowerShell

Untuk melihat nenek moyang AMI

Gunakan Get-EC2ImageAncestrycmdlet.

```
Get-EC2ImageAncestry -ImageId ami-1111111111EXAMPLE
```

Berikut ini adalah output contoh. Daftar keluaran AMIs dalam urutan leluhur: entri pertama adalah AMI (input) yang ditentukan, diikuti oleh induknya, induk induk, dan sebagainya, dan diakhiri dengan root AMI.

```
ImageAncestryEntries : {
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-1111111111EXAMPLE"    # Input AMI
        SourceImageId = "ami-2222222222EXAMPLE"
        SourceImageRegion = "us-east-1"
    },
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-2222222222EXAMPLE"    # Parent AMI
        SourceImageId = "ami-3333333333EXAMPLE"
        SourceImageRegion = "us-east-1"
    },
    ...
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-8888888888EXAMPLE"    # Root AMI
        ImageOwnerAlias = "aws-marketplace"
        SourceImageId = "ami-9999999999EXAMPLE"
        SourceImageRegion = "us-east-2"
    }
}
```

Identifikasi sumber AMI

Jika Anda hanya perlu mengidentifikasi induk langsung (sumber) AMI yang digunakan untuk membuat AMI, Anda dapat menggunakan metode berikut.

Console

Untuk mengidentifikasi sumber AMI yang digunakan untuk membuat AMI yang dipilih

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI untuk melihat detailnya.

   Informasi sumber AMI muncul di bidang berikut: Sumber AMI ID dan Sumber AMI Region

AWS CLI

Untuk mengidentifikasi sumber AMI yang digunakan untuk membuat AMI yang ditentukan

Gunakan perintah describe-images.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-0abcdef1234567890 \
    --query "Images[].{ID:SourceImageId,Region:SourceImageRegion}"
```

Berikut ini adalah output contoh.

```
[
    {
        "ID": "ami-0abcdef1234567890",
        "Region": "us-west-2"
    }
}
```

PowerShell

Untuk mengidentifikasi sumber AMI yang digunakan untuk membuat AMI yang ditentukan

Gunakan Get-EC2Imagecmdlet.

```
Get-EC2Image -ImageId ami-0abcdef1234567890 | Select SourceImageId,
 SourceImageRegion
```

Berikut ini adalah output contoh.

```
SourceImageId           SourceImageRegion
-------------           -----------------
ami-0abcdef1234567890 us-west-2
```

Kelola dan pantau penggunaan AMI

AWS menyediakan beberapa fitur untuk membantu Anda mengelola dan memantau penggunaan AMI Anda secara efektif. Anda dapat melacak akun mana yang menggunakan akun bersama Anda AMIs, mengidentifikasi kapan terakhir kali AMIs digunakan, dan menemukan sumber daya yang spesifik AMIs dalam referensi Anda Akun AWS .

Tabel berikut memberikan ikhtisar fitur untuk mengelola dan memantau penggunaan AMI:

Fitur	Kasus penggunaan	Manfaat utama
Laporan penggunaan AMI	Dapatkan visibilitas ke mana Akun AWS yang menggunak an Anda AMIs dan berapa banyak setiap AMI digunakan.	• Identifikasi Akun AWS dan jenis sumber daya yang mereferensikan Anda AMIs sehingga Anda dapat membatalkan pendaftaran atau menonaktifkan dengan aman. AMIs • Identifikasi yang tidak digunakan AMIs untuk deregistrasi untuk mengurangi biaya penyimpanan. • Identifikasi yang paling sering Anda gunakan AMIs.
Pelacakan terakhir digunakan	Periksa kapan AMI Anda terakhir digunakan.	• Identifikasi yang tidak digunakan AMIs sehingga

Fitur	Kasus penggunaan	Manfaat utama
		Anda dapat membatalkan pendaftaran AMIs dengan aman. • Identifikasi yang tidak digunakan AMIs untuk deregistrasi untuk mengurangi biaya penyimpanan.
Pemeriksaan referensi AMI	Pastikan AWS sumber daya Anda menggunakan kepatuhan AMIs terbaru.	• Audit penggunaan AMIs di akun Anda. • Periksa di mana spesifik AMIs sedang direferensikan. • Pertahankan kepatuhan dengan memperbarui sumber daya Anda untuk referensi terbaruAMIs.

Topik

- Lihat penggunaan AMI Anda
- Periksa kapan Amazon EC2 AMI terakhir digunakan
- Identifikasi referensi sumber daya Anda yang ditentukan AMIs

Lihat penggunaan AMI Anda

Jika Anda membagikan Amazon Machine Images (AMIs) dengan yang Akun AWS lain—baik dengan organisasi Akun AWS, organisasi, unit organisasi (OUs), atau publik—Anda dapat melihat bagaimana ini AMIs digunakan dengan membuat laporan penggunaan AMI. Laporan memberikan visibilitas ke:

- Akun AWS Yang menggunakan EC2 contoh Anda AMIs atau meluncurkan templat

- Berapa banyak EC2 instance atau template peluncuran yang mereferensikan setiap AMI

Laporan penggunaan AMI membantu Anda mengelola secara AMIs lebih efektif dengan membantu Anda:

- Identifikasi Akun AWS dan jenis sumber daya yang mereferensikan Anda AMIs sehingga Anda dapat membatalkan pendaftaran atau menonaktifkan dengan aman. AMIs
- Identifikasi yang tidak digunakan AMIs untuk deregistrasi untuk mengurangi biaya penyimpanan.
- Identifikasi yang paling sering Anda gunakan AMIs.

Daftar Isi

- Cara kerja laporan penggunaan AMI
- Membuat laporan penggunaan AMI
- Lihat laporan penggunaan AMI
- Menghapus laporan penggunaan AMI
- Laporkan kuota

Cara kerja laporan penggunaan AMI

Saat membuat laporan penggunaan AMI, Anda menentukan:

- AMI untuk melaporkannya.
- Akun AWS Untuk memeriksa (akun tertentu atau semua akun).
- Jenis sumber daya yang akan diperiksa (EC2 instance, template peluncuran, atau keduanya).
- Untuk template peluncuran, jumlah versi yang akan diperiksa (default ke 20 versi terbaru).

Amazon EC2 membuat laporan terpisah untuk setiap AMI. Setiap laporan menyediakan:

- Daftar Akun AWS menggunakan AMI.
- Hitungan sumber daya yang mereferensikan AMI berdasarkan jenis sumber daya per akun. Perhatikan bahwa untuk template peluncuran, jika AMI direferensikan dalam beberapa versi template peluncuran, hitungannya hanya 1.

> **Important**
>
> Saat Anda membuat laporan penggunaan AMI, laporan tersebut mungkin tidak berisi aktivitas terbaru. Aktivitas instans dari 24 jam terakhir dan aktivitas peluncuran template dari beberapa hari terakhir mungkin tidak muncul dalam laporan.

Amazon EC2 secara otomatis menghapus laporan 30 hari setelah pembuatan. Anda dapat mengunduh laporan dari EC2 konsol untuk disimpan secara lokal.

Membuat laporan penggunaan AMI

Untuk melihat bagaimana AMI Anda digunakan, Anda harus terlebih dahulu membuat laporan penggunaan AMI, menentukan akun dan jenis sumber daya yang akan dilaporkan. Setelah laporan dibuat, Anda dapat melihat isi laporan. Anda juga dapat mengunduh laporan dari EC2 konsol.

Console

Untuk membuat laporan penggunaan AMI

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI dan pilih Tindakan, penggunaan AMI, Lihat penggunaan AMI saya.
4. Pada halaman Create my AMI usage report, lakukan hal berikut:
   a. Untuk jenis Sumber Daya, pilih satu atau beberapa jenis sumber daya yang akan dilaporkan.
   b. Untuk Akun IDs, lakukan salah satu hal berikut:
      - Pilih Tentukan akun IDs, lalu pilih Tambahkan ID akun untuk setiap akun yang akan dilaporkan.
      - Pilih Sertakan semua akun untuk melaporkan semua akun.
   c. Pilih Buat laporan penggunaan AMI saya.
5. Pada halaman AMI, pilih tab Penggunaan AMI Saya.
6. Pilih ID laporan untuk melihat detailnya.

AWS CLI

Untuk membuat laporan penggunaan AMI untuk daftar akun

Gunakan create-image-usage-reportperintah dengan parameter yang diperlukan berikut:

- `--image-id`— ID AMI untuk melaporkan.
- `--resource-types`— Jenis sumber daya untuk diperiksa. Dalam contoh berikut, jenis sumber daya yang akan diperiksa adalah EC2 instance dan template peluncuran. Selain itu, jumlah versi template peluncuran yang akan diperiksa juga ditentukan (`version-depth=100`).

Untuk melaporkan akun tertentu, gunakan `--account-ids` parameter untuk menentukan ID setiap akun yang akan dilaporkan.

```
aws ec2 create-image-usage-report \
    --image-id ami-0abcdef1234567890 \
    --account-ids 111122223333 444455556666 123456789012 \
    --resource-types ResourceType=ec2:Instance \
      'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=100}]'
```

Untuk membuat laporan penggunaan AMI dari semua akun

Untuk melaporkan semua akun menggunakan AMI yang ditentukan, gunakan perintah yang sama tetapi hilangkan `--account-ids` parameternya.

```
aws ec2 create-image-usage-report \
    --image-id ami-0abcdef1234567890 \
    --resource-types ResourceType=ec2:Instance \
      'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=100}]'
```

Berikut ini adalah output contoh.

```
{
    "ReportId": "amiur-00b877d192f6b02d0"
}
```

Untuk memantau status pembuatan laporan

Gunakan describe-image-usage-reportsperintah dan tentukan ID laporan.

```
aws ec2 describe-image-usage-reports --report-ids amiur-00b877d192f6b02d0
```

Berikut ini adalah output contoh. Nilai awal `State` bidang tersebut adalah`pending`. Untuk dapat melihat entri laporan, negara harus`available`.

```
{
    "ImageUsageReports": [
        {
            "ImageId": "ami-0e9ae3dc21c2b3a64",
            "ReportId": "amiur-abcae3dc21c2b3999",
            "ResourceTypes": [
                {"ResourceType": "ec2:Instance"}
            ],
            "State": "pending",
            "CreationTime": "2025-09-29T13:27:12.322000+00:00",
            "ExpirationTime": "2025-10-28T13:27:12.322000+00:00"
        }
    ]
}
```

PowerShell

Untuk membuat laporan penggunaan AMI untuk daftar akun

Gunakan New-EC2ImageUsageReportcmdlet dengan parameter yang diperlukan berikut:

- `-ImageId`— ID AMI untuk melaporkan.
- `-ResourceType`— Jenis sumber daya untuk diperiksa. Dalam contoh berikut, jenis sumber daya yang akan diperiksa adalah EC2 instance dan template peluncuran. Selain itu, jumlah versi template peluncuran yang akan diperiksa juga ditentukan (`'version-depth' = 100`).

Untuk melaporkan akun tertentu, gunakan `-AccountId` parameter untuk menentukan ID setiap akun yang akan dilaporkan.

```
New-EC2ImageUsageReport `
    -ImageId ami-0abcdef1234567890 `
    -AccountId 111122223333 444455556666 123456789012 `
    -ResourceType @(
        @{ResourceType = 'ec2:Instance'},
        @{ResourceType = 'ec2:LaunchTemplate'ResourceTypeOptions = @{'version-depth'
 = 100}
```

```
        })
```

Untuk membuat laporan penggunaan AMI dari semua akun

Untuk melaporkan semua akun menggunakan AMI yang ditentukan, gunakan perintah yang sama tetapi hilangkan `-AccountId` parameternya.

```
New-EC2ImageUsageReport `
    -ImageId ami-0abcdef1234567890 `
    -ResourceType @(
        @{ResourceType = 'ec2:Instance'},
        @{ResourceType = 'ec2:LaunchTemplate'ResourceTypeOptions = @{'version-depth'
 = 100}
        })
```

Berikut ini adalah output contoh.

```
ReportId
--------
amiur-00b877d192f6b02d0
```

Untuk memantau status pembuatan laporan

Gunakan Get-EC2ImageUsageReportperintah dan tentukan ID laporan.

```
Get-EC2ImageUsageReport -ReportId amiur-00b877d192f6b02d0
```

Berikut ini adalah output contoh. Nilai awal `State` bidang tersebut adalah`pending`. Untuk dapat melihat entri laporan, negara harus`available`.

```
ImageUsageReports
-----------------
{@{ImageId=ami-0e9ae3dc21c2b3a64; ReportId=amiur-abcae3dc21c2b3999;
 ResourceTypes=System.Object[]; State=pending; CreationTime=2025-09-29;
 ExpirationTime=2025-10-28}}
```

Lihat laporan penggunaan AMI

Anda dapat melihat semua laporan penggunaan yang Anda buat untuk AMI dalam 30 hari terakhir. Amazon EC2 secara otomatis menghapus laporan 30 hari setelah pembuatan.

Untuk setiap laporan, Anda dapat melihat Akun AWS yang menggunakan AMI, dan untuk setiap akun, hitungan sumber daya yang mereferensikan AMI berdasarkan jenis sumber daya. Anda juga dapat melihat kapan pembuatan laporan dimulai. Informasi ini hanya tersedia jika laporan berada dalam status Lengkap (konsol) atau `available` (AWS CLI).

> **Important**
>
> Saat Anda membuat laporan penggunaan AMI, laporan tersebut mungkin tidak berisi aktivitas terbaru. Aktivitas instans dari 24 jam terakhir dan aktivitas peluncuran template dari beberapa hari terakhir mungkin tidak muncul dalam laporan.

Console

Untuk melihat laporan penggunaan AMI

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI.
4. Pilih tab Laporan penggunaan saya.

   Daftar laporan menunjukkan:

   - Semua laporan yang dihasilkan dalam 30 hari terakhir untuk AMI yang dipilih.
   - Untuk setiap laporan, kolom waktu yang dimulai Laporan menunjukkan tanggal laporan dibuat.
5. Pilih ID laporan untuk melihat isinya.
6. Untuk kembali ke tab Laporan penggunaan saya di halaman detail AMI, pilih Lihat semua laporan untuk AMI ini.

AWS CLI

Untuk mencantumkan semua laporan penggunaan AMI untuk AMI yang ditentukan

Gunakan describe-image-usage-reportsperintah dan tentukan ID AMI untuk mendapatkan daftar laporannya.

```
aws ec2 describe-image-usage-reports --image-ids ami-0abcdef1234567890
```

Berikut ini adalah output contoh. Setiap ID laporan dicantumkan bersama dengan jenis sumber daya yang dipindai dan pembuatan laporan serta tanggal kedaluwarsa. Anda dapat menggunakan informasi ini untuk mengidentifikasi laporan yang entrinya ingin Anda lihat.


```
{
  "ImageUsageReports": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ReportId": "amiur-1111111111111111",
      "ResourceTypes": [
        {
          "ResourceType": "ec2:Instance"
        }
      ],
      "State": "available",
      "CreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ExpirationTime": "2025-10-28T13:27:12.322000+00:00",
      "Tags": []
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ReportId": "amiur-22222222222222222",
      "ResourceTypes": [
        {
          "ResourceType": "ec2:Instance"
        },
        {
          "ResourceType": "ec2:LaunchTemplate"
        }
      ],
      "State": "available",
      "CreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ExpirationTime": "2025-10-30T13:27:12.322000+00:00",
      "Tags": []
    }
  ],
  "NextToken": "opaque"
}
```


Untuk melihat isi laporan penggunaan AMI untuk AMI yang ditentukan

Gunakan perintah describe-image-usage-report-entries dan tentukan ID AMI. Respons mengembalikan semua laporan untuk AMI yang ditentukan, menunjukkan akun yang telah menggunakan AMI dan jumlah sumber dayanya.

```
aws ec2 describe-image-usage-report-entries --image-ids ami-0abcdef1234567890
```

Berikut ini adalah output contoh.

```
{
  "ImageUsageReportEntries": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 15,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 2,
      "ReportCreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ReportId": "amiur-22222222222222222"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "001100110011",
      "UsageCount": 39,
      "ReportCreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ReportId": "amiur-22222222222222222"
    }
  ],
  "NextToken": "opaque"
}
```

Untuk melihat isi laporan penggunaan AMI untuk laporan yang ditentukan

Gunakan perintah describe-image-usage-report-entries dan tentukan ID laporan. Respons menampilkan semua entri untuk laporan yang ditentukan, menampilkan akun yang telah menggunakan AMI dan jumlah sumber dayanya.

```
aws ec2 describe-image-usage-report-entries --report-ids amiur-1111111111111111
```

Berikut ini adalah output contoh.

```
{
  "ImageUsageReportEntries": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 15,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:LaunchTemplate",
      "AccountId": "123412341234",
      "UsageCount": 4,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:LaunchTemplate",
      "AccountId": "001100110011",
      "UsageCount": 2,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    }
  ],
  "NextToken": "opaque"
}
```

PowerShell

Untuk mencantumkan semua laporan penggunaan AMI untuk AMI yang ditentukan

Gunakan Get-EC2ImageUsageReportcmdlet dan tentukan ID AMI untuk mendapatkan daftar laporannya.

```
Get-EC2ImageUsageReport -ImageId ami-0abcdef1234567890
```

Berikut ini adalah output contoh. Setiap ID laporan dicantumkan bersama dengan jenis sumber daya yang dipindai dan pembuatan laporan serta tanggal kedaluwarsa. Anda dapat menggunakan informasi ini untuk mengidentifikasi laporan yang entrinya ingin Anda lihat.

```
@{
    ImageUsageReports = @(
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-1111111111111111"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-09-29T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-28T13:27:12.322000+00:00"
        },
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-2222222222222222"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-09-30T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-29T13:27:12.322000+00:00"
        },
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-3333333333333333"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
```

```
            State = "available"
            CreationTime = "2025-10-01T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-30T13:27:12.322000+00:00"
        }
    )
    NextToken = "opaque"
}
```

Untuk melihat isi laporan penggunaan AMI untuk AMI yang ditentukan

Gunakan Get-EC2ImageUsageReportEntrycmdlet dan tentukan ID AMI. Respons mengembalikan semua laporan untuk AMI yang ditentukan, menunjukkan akun yang telah menggunakan AMI dan jumlah sumber dayanya.

```
Get-EC2ImageUsageReportEntry -ImageId ami-0abcdef1234567890
```

Berikut ini adalah output contoh.

```
ImageUsageReportEntries : {@{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 15
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-1111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 7
    ReportCreationTime = "2025-09-30T13:27:12.322000+00:00"
    ReportId = "amiur-2222222222222222"
    }...}
NextToken : opaque
```

Untuk melihat isi laporan penggunaan AMI untuk laporan yang ditentukan

Gunakan Get-EC2ImageUsageReportEntrycmdlet dan tentukan ID laporan. Respons menampilkan semua entri untuk laporan yang ditentukan, menampilkan akun yang telah menggunakan AMI dan jumlah sumber dayanya.

```
Get-EC2ImageUsageReportEntry -ReportId amiur-1111111111111111
```

Berikut ini adalah output contoh.

```
ImageUsageReportEntries : {@{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 15
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:LaunchTemplate"
    AccountId = "123412341234"
    UsageCount = 4
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:LaunchTemplate"
    AccountId = "************"
    UsageCount = 2
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }}
NextToken : opaque
```

Menghapus laporan penggunaan AMI

Amazon EC2 secara otomatis menghapus laporan 30 hari setelah dibuat. Anda dapat menghapusnya secara manual sebelum waktu itu.

Console

Untuk menghapus laporan penggunaan AMI

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI.

4. Pilih tab Penggunaan AMI Saya.
5. Pilih tombol opsi di sebelah laporan yang akan dihapus, lalu pilih Hapus.

AWS CLI

Untuk menghapus laporan penggunaan AMI

Gunakan delete-image-usage-reportperintah dan tentukan ID laporan.

```
aws ec2 delete-image-usage-report --report-id amiur-0123456789abcdefg
```

PowerShell

Untuk menghapus laporan penggunaan AMI

Gunakan Remove-EC2ImageUsageReportcmdlet dan tentukan ID laporan.

```
Remove-EC2ImageUsageReport -ReportId amiur-0123456789abcdefg
```

Laporkan kuota

Kuota berikut berlaku untuk membuat laporan penggunaan AMI. Kuota berlaku per AWS Region.

Deskripsi	Kuota
Laporan penggunaan AMI dalam proses (`pending`) per Akun AWS	2.000
Laporan penggunaan AMI dalam proses (`pending`) per AMI	1

Periksa kapan Amazon EC2 AMI terakhir digunakan

Amazon EC2 secara otomatis melacak tanggal dan waktu ketika AMI terakhir digunakan untuk meluncurkan instance. Jika Anda memiliki AMI yang sudah lama tidak digunakan untuk meluncurkan instance, pertimbangkan apakah AMI adalah kandidat yang baik untuk deregistrasi atau penghentian.

Pertimbangan-pertimbangan

- Ketika AMI digunakan untuk meluncurkan instans, ada penundaan 24 jam sebelum penggunaan tersebut dilaporkan.
- Anda harus menjadi pemilik AMI untuk mendapatkan waktu peluncuran terakhir.
- Data penggunaan AMI tersedia mulai April 2017.

Console

Untuk melihat waktu peluncuran AMI terakhir

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih AMIs.
3. Dari bilah filter, pilih Dimiliki oleh saya.
4. Pilih kotak centang untuk AMI.
5. Pada tab Detail, temukan Waktu peluncuran terakhir.

AWS CLI

Untuk melihat waktu peluncuran terakhir dengan menjelaskan AMI

Gunakan perintah describe-images. Jika tidak `LastLaunchedTime` ada dalam output, verifikasi bahwa Anda memiliki AMI.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[].LastLaunchedTime \
    --output text
```

Berikut ini adalah output contoh.

```
2025-02-17T20:22:19Z
```

Untuk melihat atribut waktu peluncuran terakhir dari AMI

Gunakan perintah describe-image-attribute. Anda harus menjadi pemilik AMI yang ditentukan.

```
aws ec2 describe-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --attribute lastLaunchedTime \
    --query LastLaunchedTime.Value \
    --output text
```

Berikut ini adalah output contoh.

```
2025-02-17T20:22:19Z
```

PowerShell

Untuk melihat waktu peluncuran terakhir dengan menjelaskan AMI

Gunakan Get-EC2Imagecmdlet. Jika tidak `LastLaunchedTime` ada dalam output, verifikasi bahwa Anda memiliki AMI.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).LastLaunchedTime
```

Berikut ini adalah output contoh.

```
2025-02-17T20:22:19Z
```

Untuk melihat atribut waktu peluncuran terakhir dari AMI

Gunakan Get-EC2ImageAttributecmdlet. Anda harus menjadi pemilik AMI yang ditentukan.

```
(Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute LastLaunchedTime).LastLaunchedTime
```

Berikut ini adalah output contoh.

```
2025-02-17T20:22:19Z
```

Identifikasi referensi sumber daya Anda yang ditentukan AMIs

Anda dapat mengidentifikasi AWS sumber daya yang mereferensikan Amazon Machine Images (AMIs) tertentu, terlepas dari AMIs apakah itu publik atau pribadi, atau siapa yang memilikinya.

Visibilitas ini membantu Anda memastikan sumber daya Anda menggunakan kepatuhan AMIs terbaru.

Manfaat utama

Memeriksa referensi AMI membantu Anda:

- Audit penggunaan AMIs di akun Anda.
- Periksa di mana spesifik AMIs sedang direferensikan.
- Pertahankan kepatuhan dengan memperbarui sumber daya Anda untuk referensi terbaruAMIs.

Topik

- Sumber daya yang didukung
- Cara kerja pemeriksaan referensi AMI
- Izin IAM yang diperlukan
- Langkah-langkah untuk memeriksa referensi AMI

Sumber daya yang didukung

Referensi AMI dapat diperiksa di:

- Instans EC2
- Templat peluncuran
- Parameter SSM
- Resep gambar Image Builder
- Resep wadah Image Builder

Cara kerja pemeriksaan referensi AMI

Operasi dasar

Saat Anda menjalankan pemeriksaan referensi AMI, Anda:

- Tentukan mana yang AMIs harus diperiksa.
- Pilih jenis sumber daya yang akan dipindai.

- Terima daftar sumber daya Anda yang mereferensikan yang ditentukan AMIs.

Pemilihan jenis sumber daya

Di konsol, Anda memilih jenis sumber daya untuk dipindai.

Di CLI, Anda menentukan jenis sumber daya untuk dipindai menggunakan salah satu atau kedua parameter CLI berikut:

- `IncludeAllResourceTypes`: Memindai semua jenis sumber daya yang didukung.
- `ResourceTypes`: Memindai jenis sumber daya yang Anda tentukan.

Pelingkupan respons

Anda dapat mencakup respons untuk instans EC2 dan meluncurkan templat dengan menyesuaikan `ResourceTypeOptions` nilai menggunakan parameter. `ResourceTypes` Konsol dan `IncludeAllResourceTypes` parameter keduanya menggunakan nilai opsi default. Kapan `ResourceTypes` dan `IncludeAllResourceTypes` digunakan bersama-sama, nilai `ResourceTypes` opsi lebih diutamakan daripada default.

Berikut ini adalah nilai default:

Tipe sumber daya	Opsi pelingkupan () **`OptionName`**	Tujuan	Nilai default untuk **`OptionValue`** dan konsol
Instans EC2	`state-name`	Filter berdasarkan status instans	`pending`,`running`,`shutting down` ,`terminated` ,`stopping`, `stopped` (semua negara bagian)
Templat peluncuran	`version-depth`	Tentukan jumlah versi template peluncuran yang akan diperiksa (mulai dari versi terbaru)	`10`(versi terbaru)

Izin IAM yang diperlukan

Untuk menggunakan DescribeImageReferences API untuk mengidentifikasi sumber daya yang direferensikan ditentukan AMIs, Anda memerlukan izin IAM berikut untuk menjelaskan sumber daya:

- `ec2:DescribeInstances`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeLaunchTemplateVersions`
- `ssm:DescribeParameters`
- `ssm:GetParameters`
- `imagebuilder:ListImageRecipes`
- `imagebuilder:ListContainerRecipes`
- `imagebuilder:GetContainerRecipe`

Contoh kebijakan IAM untuk menggunakan API DescribeImageReferences

Contoh kebijakan berikut memberi Anda izin untuk menggunakan DescribeImageReferences API, yang mencakup izin untuk mendeskripsikan instans EC2, template peluncuran, parameter Systems Manager, resep gambar Image Builder, dan resep wadah Image Builder.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeImageReferences",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ssm:DescribeParameters",
    "ssm:GetParameters",
    "imagebuilder:ListImageRecipes",
```

```
    "imagebuilder:ListContainerRecipes",
    "imagebuilder:GetContainerRecipe"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ec2-images.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

Important

Kami sangat menyarankan untuk menggunakan kebijakan AWS terkelola `AmazonEC2ImageReferencesAccessPolicy`daripada membuat kebijakan sendiri. Membuat kebijakan IAM khusus yang hanya menyediakan izin yang diperlukan memerlukan waktu dan keahlian, dan akan memerlukan pembaruan saat jenis sumber daya baru tersedia. Kebijakan `AmazonEC2ImageReferencesAccessPolicy` terkelola:

- Memberikan semua izin yang diperlukan untuk menggunakan DescribeImageReferences API (ini termasuk izin untuk mendeskripsikan instans EC2, template peluncuran, parameter Systems Manager, dan wadah Image Builder dan resep gambar).
- Secara otomatis mendukung jenis sumber daya baru saat tersedia (terutama penting saat menggunakan `IncludeAllResourceTypes` parameter).

Anda dapat melampirkan `AmazonEC2ImageReferencesAccessPolicy` kebijakan ke identitas IAM Anda (pengguna, grup, dan peran).
Untuk melihat izin yang disertakan dalam kebijakan ini, lihat `AmazonEC2ImageReferencesAccessPolicy`di Referensi Kebijakan AWS Terkelola.

Langkah-langkah untuk memeriksa referensi AMI

Gunakan prosedur berikut untuk mengidentifikasi AWS sumber daya mana yang Anda referensikan ditentukan AMIs.

Console

Untuk mengidentifikasi referensi sumber daya yang ditentukan AMIs

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih satu atau lebih AMIs untuk memeriksa referensi.
4. Pilih Tindakan, penggunaan AMI, Lihat sumber daya yang direferensikan.
5. Pada Lihat sumber daya yang merujuk AMIs halaman yang dipilih:
   a. Untuk jenis Sumber Daya, pilih satu atau beberapa jenis sumber daya.
   b. Pilih Lihat sumber daya.
6. AMIsBagian referensi Resources yang dipilih akan muncul. Daftar ini menampilkan sumber daya yang mereferensikan yang ditentukan AMIs. Setiap baris memberikan informasi berikut:
   - ID AMI — ID AMI yang direferensikan.
   - Jenis sumber daya — Jenis sumber daya dari sumber daya yang mereferensikan AMI.
   - Resource ID — ID sumber daya yang mereferensikan AMI.

AWS CLI

Untuk memeriksa referensi AMI untuk jenis sumber daya tertentu

Gunakan describe-image-referencesperintah dengan `--resource-types` parameter. Contoh berikut memeriksa instans EC2 (pelingkupan berdasarkan status instans), templat peluncuran (pelingkupan ke 20 versi templat peluncuran terbaru), dan jenis sumber daya spesifik lainnya.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --resource-types \
        'ResourceType=ec2:Instance,ResourceTypeOptions=[{OptionName=state-
name,OptionValues=[running,pending]}]' \
        'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=[20]}]' \
```

```
        'ResourceType=ssm:Parameter' \
        'ResourceType=imagebuilder:ImageRecipe' \
        'ResourceType=imagebuilder:ContainerRecipe'
```

Berikut ini adalah output contoh.

```
{
    "ImageReferences": [
        {
            "ImageId": "ami-0abcdef1234567890",
            "ResourceType": "ec2:Instance",
            "Arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
        },
        {
            "ImageId": "ami-1234567890abcdef0",
            "ResourceType": "ec2:LaunchTemplate",
            "Arn": "arn:aws:ec2:us-east-1:123456789012:launch-template/
lt-1234567890abcdef0"
        }
    ]
}
```

Untuk memeriksa referensi AMI untuk semua jenis sumber daya yang didukung

Gunakan describe-image-referencesperintah dengan `--include-all-resource-types` parameter.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --include-all-resource-types
```

Untuk memeriksa referensi AMI untuk semua jenis sumber daya yang didukung dan opsi spesifik

Gunakan describe-image-referencesperintah dengan parameter `--include-all-resource-types` dan `--resource-types` parameter. Contoh ini memeriksa semua jenis sumber daya sambil melingkupi respons untuk instans EC2 ke instance yang sedang berjalan atau tertunda.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --include-all-resource-types \
```

```
    --resource-types
 'ResourceType=ec2:Instance,ResourceTypeOptions=[{OptionName=state-
name,OptionValues=[running,pending]}]'
```

PowerShell

Untuk memeriksa referensi AMI untuk jenis sumber daya tertentu

Gunakan Get-EC2ImageReferencecmdlet dengan parameter. `-ResourceType` Contoh berikut memeriksa instans EC2 (pelingkupan berdasarkan status instans), templat peluncuran (pelingkupan ke 20 versi templat peluncuran terbaru), dan jenis sumber daya spesifik lainnya.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -ResourceType @(
        @{
            ResourceType = 'ec2:Instance'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'state-name'
                    OptionValues = @('running', 'pending')
                }
            )
        },
        @{
            ResourceType = 'ec2:LaunchTemplate'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'version-depth'
                    OptionValues = @('20')
                }
            )
        },
        @{
            ResourceType = 'ssm:Parameter'
        },
        @{
            ResourceType = 'imagebuilder:ImageRecipe'
        },
        @{
            ResourceType = 'imagebuilder:ContainerRecipe'
        }
    )
```

Untuk memeriksa referensi AMI untuk semua jenis sumber daya yang didukung

Gunakan Get-EC2ImageReferencecmdlet dengan parameter. `-IncludeAllResourceTypes`

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -IncludeAllResourceTypes
```

Untuk memeriksa referensi AMI untuk semua jenis sumber daya yang didukung dan opsi spesifik

Gunakan Get-EC2ImageReferencecmdlet dengan parameter `-IncludeAllResourceTypes` dan `-ResourceType` parameter. Contoh ini memeriksa semua jenis sumber daya sambil melingkupi respons untuk instans EC2 ke instance yang sedang berjalan atau tertunda.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -IncludeAllResourceTypes `
    -ResourceType @(
        @{
            ResourceType = 'ec2:Instance'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'state-name'
                    OptionValues = @('running', 'pending')
                }
            )
        }
    )
```

Menghentikan Amazon AMI EC2

Anda dapat mengusangkan AMI untuk menunjukkan bahwa AMI sudah kedaluwarsa dan tidak boleh digunakan. Anda juga dapat menentukan tanggal pengusangan di masa depan untuk AMI, yang menunjukkan kapan AMI akan kedaluwarsa. Misalnya, Anda mungkin mengusangkan AMI yang tidak lagi dipelihara secara aktif, atau Anda mungkin mengusangkan AMI yang telah digantikan oleh versi yang lebih baru. Secara default, usang AMIs tidak muncul di daftar AMI, mencegah pengguna baru menggunakan. out-of-date AMIs Namun, pengguna dan layanan peluncuran yang ada, seperti templat peluncuran dan grup Auto Scaling, dapat terus menggunakan AMI usang tersebut dengan menentukan ID-nya. Untuk menghapus AMI sehingga pengguna dan layanan tidak dapat menggunakannya, Anda harus membatalkan pendaftaran AMI.

Setelah AMI sudah usang:

- Untuk pengguna AMI, AMI yang tidak digunakan lagi tidak muncul DescribeImagesdalam panggilan API kecuali Anda menentukan ID-nya atau menentukan bahwa yang tidak digunakan lagi harus muncul AMIs . Pemilik AMI terus melihat tidak digunakan lagi AMIs dalam DescribeImagespanggilan API.
- Untuk pengguna AMI, AMI yang tidak digunakan lagi tidak tersedia untuk dipilih melalui EC2 konsol. Sebagai contoh, AMI usang tidak muncul di katalog AMI dalam wizard peluncuran instans. Pemilik AMI terus melihat usang AMIs di konsol. EC2
- Untuk pengguna AMI, jika Anda mengetahui ID AMI yang tidak digunakan lagi, Anda dapat terus meluncurkan instance menggunakan AMI yang tidak digunakan lagi dengan menggunakan API, CLI, atau file. SDKs
- Layanan peluncuran, seperti templat peluncuran dan grup Auto Scaling, dapat melanjutkan referensi yang tidak digunakan lagi. AMIs
- EC2 instance yang diluncurkan menggunakan AMI yang kemudian tidak digunakan lagi tidak terpengaruh, dan dapat dihentikan, dimulai, dan di-boot ulang.

Anda dapat menghentikan baik pribadi maupun publik. AMIs

Daftar Isi

- Biaya
- Pertimbangan-pertimbangan
- Membuat usang sebuah AMI
- Jelaskan usang AMIs
- Batalkan penghentian AMI

Biaya

Ketika Anda mengusangkan AMI, AMI tersebut tidak dihapus. Pemilik AMI terus membayar untuk snapshot AMI. Untuk berhenti membayar snapshot, pemilik AMI harus menghapus AMI dengan membatalkan pendaftaran AMI tersebut.

Pertimbangan-pertimbangan

- Untuk mengusangkan AMI, Anda harus merupakan pemilik AMI tersebut.

- AMIs yang belum digunakan baru-baru ini untuk meluncurkan instance mungkin merupakan kandidat yang baik untuk penghentian atau deregister. Untuk informasi selengkapnya, lihat the section called “Periksa kapan AMI terakhir digunakan”.
- Anda dapat membuat kebijakan AMI yang didukung Amazon Data Lifecycle Manager EBS untuk mengotomatiskan penghentian EBS yang didukung. AMIs Untuk informasi selengkapnya, lihat Membuat kebijakan siklus hidup AMI.
- Secara default, tanggal penghentian semua publik AMIs diatur ke dua tahun dari tanggal pembuatan AMI. Anda dapat mengatur tanggal pengusangan menjadi lebih awal dari dua tahun. Untuk membatalkan tanggal usang, atau memundurkan tanggal usang, Anda harus menjadikan AMI privat dengan hanya membagikannya dengan akun AWS tertentu.

Membuat usang sebuah AMI

Anda dapat mengusangkan AMI pada tanggal dan waktu tertentu. Anda harus menjadi pemilik AMI.

Batas atas untuk tanggal penghentian adalah 10 tahun dari sekarang, kecuali untuk publik AMIs, di mana batas atas adalah 2 tahun sejak tanggal pembuatan. Anda tidak dapat menentukan tanggal di masa lalu.

Console

Untuk mengusangkan AMI pada tanggal tertentu

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di navigator kiri, pilih AMIs.
3. Dari bilah filter, pilih Dimiliki oleh saya.
4. Pilih AMI, lalu pilih Tindakan, Kelola Pengusangan AMI. Anda dapat memilih beberapa AMIs untuk mengatur tanggal penghentian yang sama dari beberapa AMIs sekaligus.
5. Pilih kotak centang Aktifkan, lalu masukkan tanggal dan waktu penghentian.
6. Pilih Simpan.

AWS CLI

Untuk mengusangkan AMI pada tanggal tertentu

Gunakan perintah enable-image-deprecation. Jika Anda menentukan nilai untuk detik, Amazon EC2 membulatkan detik ke menit terdekat.

```
aws ec2 enable-image-deprecation \
    --image-id ami-0abcdef1234567890 \
    --deprecate-at "2025-04-15T13:17:12.000Z"
```

PowerShell

Untuk mengusangkan AMI pada tanggal tertentu

Gunakan Enable-EC2ImageDeprecationcmdlet. Jika Anda menentukan nilai untuk detik, Amazon EC2 membulatkan detik ke menit terdekat.

```
Enable-EC2ImageDeprecation `
    -ImageId ami-0abcdef1234567890 `
    -DeprecateAt 2025-04-15T13:17:12.000Z
```

Jelaskan usang AMIs

Anda dapat melihat tanggal dan waktu penghentian AMI, dan memfilter AMIs berdasarkan tanggal penghentian.

Console

Untuk melihat tanggal pengusangan dari AMI

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di navigator kiri, pilih AMIs, lalu pilih AMI.
3. Centang bidang Waktu penghentian (jika Anda memilih kotak centang di sebelah AMI, itu terletak di tab Detail). Kolom ini menunjukkan tanggal dan waktu pengusangan AMI. Jika bidang kosong, AMI tidak usang.

Untuk memfilter AMIs berdasarkan tanggal penghentian

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di navigator kiri, pilih AMIs.
3. Dari bilah filter, pilih Dimiliki oleh saya atau Gambar pribadi (gambar pribadi termasuk AMIs yang dibagikan dengan Anda serta dimiliki oleh Anda).
4. Di bilah Pencarian, masukkan **`Deprecation time`** (saat Anda memasukkan huruf, akan muncul filter Waktu pengusangan), lalu pilih operator serta tanggal dan waktu.

AWS CLI

Ketika Anda menjelaskan semuanya AMIs, hasilnya tergantung pada apakah Anda pengguna AMI atau pemilik AMI.

- Pengguna AMI - Secara default, ketika Anda menjelaskan semua AMIs, usang AMIs yang dibagikan dengan Anda tetapi tidak dimiliki oleh Anda dikecualikan. Untuk menyertakan usang AMIs dalam hasil, tentukan opsi. `--include-deprecated`
- Pemilik AMI — Ketika Anda menjelaskan semua AMIs, semua AMIs yang Anda miliki, termasuk usang AMIs, disertakan. Anda tidak dapat mengecualikan usang AMIs yang Anda miliki dengan menggunakan opsi. `--no-include-deprecated`

Untuk menyertakan usang AMIs saat menjelaskan semua untuk akun AMIs

Gunakan perintah deskripsi-gambar berikut.

```
aws ec2 describe-images
    --owners 123456789012 \
    --include-deprecated
```

Untuk mendeskripsikan akun Anda yang tidak digunakan lagi AMIs

Gunakan perintah deskripsi-gambar berikut.

```
aws ec2 describe-images \
    --owners self \
    --query "Images[?DeprecationTime!=null].ImageId" \
    --output text
```

Berikut ini adalah output contoh.

```
ami-0abcdef1234567890
```

Untuk melihat tanggal pengusangan sebuah AMI

Gunakan perintah deskripsi-gambar berikut. Jika tidak `DeprecationTime` ada dalam output, AMI tidak akan digunakan lagi atau disetel ke usang di masa mendatang.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
```

```
    --query Images[].DeprecationTime \
    --output text
```

Berikut ini adalah output contoh.

```
2025-05-01T00:00:00.000Z
```

PowerShell

Untuk mencantumkan akun Anda yang tidak digunakan lagi AMIs

Gunakan Get-EC2Imagecmdlet.

```
(Get-EC2Image -Owner self | Where-Object {$_.DeprecationTime -ne $null}).ImageId
```

Berikut ini adalah output contoh.

```
ami-0abcdef1234567890
```

Untuk melihat tanggal pengusangan sebuah AMI

Gunakan Get-EC2Imagecmdlet. Jika tidak `DeprecationTime` ada dalam output, AMI tidak akan digunakan lagi atau disetel ke usang di masa mendatang.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).DeprecationTime
```

Berikut ini adalah output contoh.

```
2025-05-01T00:00:00.000Z
```

Batalkan penghentian AMI

Anda dapat membatalkan penghentian AMI, yang menghapus tanggal dan waktu penghentian. Anda harus merupakan pemilik AMI untuk melakukan prosedur ini.

Console

Untuk membatalkan pengusangan AMI

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.

2. Di navigator kiri, pilih AMIs.
3. Dari bilah filter, pilih Dimiliki oleh saya.
4. Pilih AMI, lalu pilih Tindakan, Kelola Pengusangan AMI. Anda dapat memilih beberapa AMIs untuk membatalkan penghentian beberapa AMIs sekaligus.
5. Kosongkan kotak centang Aktifkan, lalu pilih Simpan.

AWS CLI

Untuk membatalkan pengusangan AMI

Gunakan perintah berikut disable-image-deprecation.

```
aws ec2 disable-image-deprecation --image-id ami-0abcdef1234567890
```

PowerShell

Untuk membatalkan pengusangan AMI

Gunakan Disable-EC2ImageDeprecationcmdlet.

```
Disable-EC2ImageDeprecation -ImageId ami-0abcdef1234567890
```

Nonaktifkan Amazon EC2 AMI

Anda dapat menonaktifkan AMI untuk mencegahnya digunakan untuk peluncuran instans. Anda tidak dapat meluncurkan instans baru dari AMI yang dinonaktifkan. Anda dapat mengaktifkan kembali AMI yang dinonaktifkan sehingga dapat digunakan lagi untuk peluncuran instans.

Anda dapat menonaktifkan pribadi dan publik AMIs.

Untuk mengurangi biaya penyimpanan untuk dukungan EBS yang dinonaktifkan AMIs yang jarang digunakan, tetapi yang perlu dipertahankan dalam jangka panjang, Anda dapat mengarsipkan snapshot terkait mereka. Untuk informasi selengkapnya, lihat Mengarsipkan snapshot Amazon EBS di Panduan Pengguna Amazon EBS.

Daftar Isi

- Cara kerja AMI disable

- Biaya
- Prasyarat
- Izin IAM yang diperlukan
- Menonaktifkan AMI
- Jelaskan dinonaktifkan AMIs
- Aktifkan kembali AMI yang dinonaktifkan

Cara kerja AMI disable

> **Warning**
>
> Menonaktifkan AMI akan menghapus semua izin peluncurannya.

Saat AMI dinonaktifkan:

- Status AMI berubah menjadi `disabled`.
- AMI yang dinonaktifkan tidak dapat dibagikan. Jika AMI bersifat publik atau sebelumnya dibagikan, AMI tersebut akan dijadikan privat. Jika AMI dibagikan dengan Akun AWS, organisasi, atau Unit Organisasi, mereka kehilangan akses ke AMI yang dinonaktifkan.
- AMI yang dinonaktifkan tidak muncul dalam panggilan API DescribeImages secara default.
- AMI yang dinonaktifkan tidak muncul di bawah filter konsol Dimiliki oleh saya. Untuk menemukan yang dinonaktifkan AMIs, gunakan filter konsol gambar yang dinonaktifkan.
- AMI yang dinonaktifkan tidak tersedia untuk memilih misalnya peluncuran di EC2 konsol. Misalnya, AMI yang dinonaktifkan tidak muncul di katalog AMI di wizard peluncuran instans atau saat membuat templat peluncuran.
- Layanan peluncuran, seperti template peluncuran dan grup Auto Scaling, dapat terus menonaktifkan referensi. AMIs Peluncuran instance berikutnya dari AMI yang dinonaktifkan akan gagal, jadi sebaiknya perbarui templat peluncuran dan grup Auto Scaling agar referensi AMIs hanya tersedia.
- EC2 instance yang sebelumnya diluncurkan menggunakan AMI yang kemudian dinonaktifkan tidak terpengaruh, dan dapat dihentikan, dimulai, dan di-boot ulang.
- Anda tidak dapat menghapus snapshot yang terkait dengan dinonaktifkan AMIs. Mencoba menghapus hasil snapshot terkait pada kesalahan `snapshot is currently in use`.

Saat AMI diaktifkan kembali:

- Status AMI berubah menjadi `available`, dan dapat digunakan untuk meluncurkan instans.
- AMI dapat dibagikan.
- Akun AWS, organisasi, dan Unit Organisasi yang kehilangan akses ke AMI saat dinonaktifkan tidak akan otomatis mendapatkan kembali akses, tetapi AMI dapat dibagikan lagi dengan mereka.

Biaya

Saat Anda menonaktifkan sebuah AMI, AMI tersebut tidak dihapus. Jika AMI adalah AMI yang didukung oleh EBS, Anda terus membayar snapshot EBS AMI. Jika Anda ingin menyimpan AMI, Anda mungkin dapat mengurangi biaya penyimpanan dengan mengarsipkan snapshot. Untuk informasi selengkapnya, lihat Mengarsipkan snapshot Amazon EBS di Panduan Pengguna Amazon EBS. Jika Anda tidak ingin menyimpan AMI dan snapshot, Anda harus membatalkan pendaftaran AMI dan menghapus snapshot. Untuk informasi selengkapnya, lihat Membatalkan pendaftaran AMI.

Prasyarat

Untuk menonaktifkan atau mengaktifkan kembali AMI, Anda harus menjadi pemilik AMI.

Izin IAM yang diperlukan

Untuk menonaktifkan dan mengaktifkan kembali AMI, Anda harus memiliki izin IAM berikut:

- `ec2:DisableImage`
- `ec2:EnableImage`

Menonaktifkan AMI

Anda dapat menonaktifkan AMI dengan menggunakan EC2 konsol atau AWS Command Line Interface (AWS CLI). Anda harus merupakan pemilik AMI untuk melakukan prosedur ini.

Console

Untuk menonaktifkan AMI

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi kiri, pilih AMIs.

3. Dari bilah filter, pilih Dimiliki oleh saya.
4. Pilih AMI, lalu pilih Tindakan, Nonaktifkan AMI. Anda dapat memilih beberapa AMIs untuk menonaktifkan sekaligus.
5. Di jendela Nonaktifkan AMI, pilih Nonaktifkan AMI.

AWS CLI

Untuk menonaktifkan AMI

Gunakan perintah berikut disable-image.

```
aws ec2 disable-image --image-id ami-0abcdef1234567890
```

PowerShell

Untuk menonaktifkan AMI

Gunakan Disable-EC2Imagecmdlet.

```
Disable-EC2Image -ImageId ami-0abcdef1234567890
```

Jelaskan dinonaktifkan AMIs

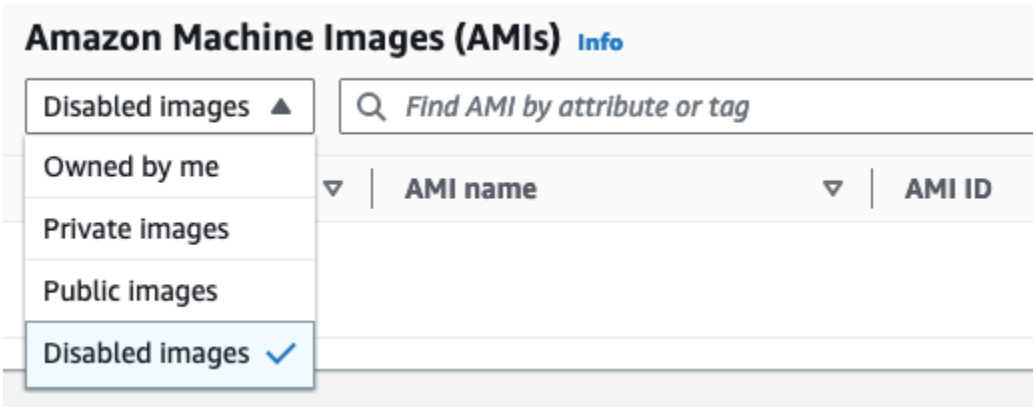
Anda dapat melihat dinonaktifkan AMIs di EC2 konsol dan dengan menggunakan file AWS CLI.

Anda harus menjadi pemilik AMI untuk melihat dinonaktifkan AMIs. Karena dinonaktifkan AMIs dibuat pribadi, Anda tidak dapat melihat dinonaktifkan AMIs jika Anda bukan pemiliknya.

Console

Untuk melihat dinonaktifkan AMIs

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi kiri, pilih AMIs.
3. Dari bilah filter, pilih Gambar yang dinonaktifkan.



AWS CLI

Secara default, ketika Anda menjelaskan semua AMIs, AMIs yang dinonaktifkan tidak termasuk dalam hasil. Untuk memasukkan dinonaktifkan AMIs dalam hasil, tentukan `--include-disabled` opsi. `State`Bidang untuk AMI adalah `disabled` jika AMI dinonaktifkan.

Untuk menyertakan dinonaktifkan AMIs saat menjelaskan semua AMIs untuk akun

Gunakan perintah berikut describe-images.

```
aws ec2 describe-images \
    --owners 123456789012 \
    --include-disabled
```

Untuk daftar yang dinonaktifkan AMIs untuk akun Anda

Gunakan perintah describe-images berikut ini.

```
aws ec2 describe-images \
    --owners self \
    --include-disabled \
    --filters Name=state,Values=disabled \
    --query Images[].ImageId \
    --output text
```

Berikut ini adalah output contoh.

```
ami-0abcdef1234567890
```

Untuk menggambarkan status AMI

Gunakan perintah berikut describe-images. Jika tidak `DeprecationTime` ada dalam output, AMI tidak akan digunakan lagi atau disetel ke usang di masa mendatang.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].State \
    --output text
```

Berikut ini adalah output contoh.

```
disabled
```

PowerShell

Secara default, ketika Anda menjelaskan semua AMIs, AMIs yang dinonaktifkan tidak termasuk dalam hasil. Untuk memasukkan dinonaktifkan AMIs dalam hasil, tentukan `-IncludeDisabled` parameter. `State`Bidang untuk AMI adalah `disabled` jika AMI dinonaktifkan.

Untuk daftar yang dinonaktifkan AMIs untuk akun Anda

Gunakan Get-EC2Imagecmdlet.

```
(Get-EC2Image `
    -Owner self `
    -IncludeDisabled $true | Where-Object {$_.State -eq "disabled"}).ImageId
```

Berikut ini adalah output contoh.

```
ami-0abcdef1234567890
```

Untuk menggambarkan status AMI

Gunakan Get-EC2Imagecmdlet.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).State.Value
```

Berikut ini adalah output contoh.

```
disabled
```

Aktifkan kembali AMI yang dinonaktifkan

Anda dapat megaktifkan kembali AMI yang dinonaktifkan. Anda harus merupakan pemilik AMI untuk melakukan prosedur ini.

Console

Untuk mengaktifkan kembali AMI yang dinonaktifkan

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi kiri, pilih AMIs.
3. Dari bilah filter, pilih Gambar yang dinonaktifkan.
4. Pilih AMI, lalu pilih Tindakan, Nonaktifkan AMI. Anda dapat memilih beberapa AMIs untuk mengaktifkan kembali beberapa AMIs sekaligus.
5. Di jendela Aktifkan AMI, pilih Aktifkan.

AWS CLI

Untuk mengaktifkan kembali AMI yang dinonaktifkan

Gunakan perintah berikut enable-image.

```
aws ec2 enable-image --image-id ami-0abcdef1234567890
```

PowerShell

Untuk mengaktifkan kembali AMI yang dinonaktifkan

Gunakan Enable-EC2Imagecmdlet.

```
Enable-EC2Image -ImageId ami-0abcdef1234567890
```

Membatalkan pendaftaran ke Amazon EC2 AMI

Saat Anda membatalkan pendaftaran AMI, Amazon EC2 menghapusnya secara permanen. Setelah Anda membatalkan pendaftaran AMI, maka Anda tidak dapat menggunakan AMI tersebut untuk meluncurkan instans baru. Anda dapat mempertimbangkan untuk membatalkan pendaftaran AMI setelah Anda selesai menggunakannya.

Untuk melindungi dari deregistrasi AMI yang tidak disengaja atau berbahaya, Anda dapat mengaktifkan perlindungan deregistrasi. Jika Anda secara tidak sengaja membatalkan pendaftaran AMI yang didukung EBS, Anda dapat menggunakan Recycle Bin untuk memulihkannya hanya jika Anda memulihkannya dalam jangka waktu yang diizinkan sebelum dihapus secara permanen.

Saat membatalkan pendaftaran AMI, Anda dapat menghapus snapshot terkait secara opsional secara bersamaan. Namun, jika snapshot dikaitkan dengan beberapa AMIs, snapshot tidak akan dihapus meskipun ditentukan untuk penghapusan, meskipun AMI masih akan dideregistrasi. Setiap snapshot yang tidak dihapus akan terus menimbulkan biaya penyimpanan.

Membatalkan pendaftaran AMI tidak berpengaruh pada instans apa pun yang diluncurkan dari AMI. Anda dapat terus menggunakan contoh ini. Secara default, membatalkan pendaftaran AMI juga tidak berpengaruh pada snapshot apa pun yang dibuat selama proses pembuatan AMI. Anda akan terus mengeluarkan biaya penggunaan untuk instans ini dan biaya penyimpanan untuk snapshot. Oleh karena itu, untuk menghindari biaya yang tidak perlu, kami sarankan Anda menghentikan instance apa pun dan menghapus snapshot apa pun yang tidak Anda perlukan. Anda dapat menghapus snapshot baik secara otomatis selama deregistrasi atau secara manual setelah deregistrasi. Untuk informasi selengkapnya, lihat Hindari biaya dari sumber daya yang tidak terpakai.

Untuk contoh yang diluncurkan dari AMI yang kemudian dideregistrasi, Anda masih dapat melihat beberapa informasi tingkat tinggi tentang AMI dengan menggunakan perintah. `describe-instance-image-metadata` AWS CLI Untuk informasi selengkapnya, lihat describe-instance-image-metadata.

Daftar Isi

- Pertimbangan-pertimbangan
- Membatalkan pendaftaran AMI
- Hindari biaya dari sumber daya yang tidak terpakai
- Lindungi Amazon EC2 AMI dari deregistrasi

Pertimbangan-pertimbangan

- Anda tidak dapat membatalkan pendaftaran AMI yang tidak dimiliki oleh akun Anda.
- Anda tidak dapat menggunakan Amazon EC2 untuk membatalkan pendaftaran AMI yang dikelola oleh layanan. AWS Backup Sebagai gantinya, gunakan AWS Backup untuk menghapus titik pemulihan yang sesuai di brankas cadangan. Untuk informasi selengkapnya, lihat Menghapus cadangan di dalam Panduan Developer AWS Backup .

Membatalkan pendaftaran AMI

Anda dapat membatalkan pendaftaran yang didukung EBS dan didukung Amazon S3 AMIs . AMIs Untuk EBS yang didukung AMIs, Anda dapat menghapus snapshot terkait secara opsional secara bersamaan. Namun, jika snapshot dikaitkan dengan yang lain AMIs, itu tidak akan dihapus bahkan jika ditentukan untuk penghapusan.

Console

Untuk membatalkan pendaftaran AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Dari bilah filter, pilih Dimiliki oleh saya untuk mencantumkan yang tersedia AMIs, atau pilih Gambar yang dinonaktifkan untuk mencantumkan gambar yang dinonaktifkan AMIs.
4. Pilih AMI untuk membatalkan pendaftaran.
5. Pilih Tindakan, Batalkan pendaftaran AMI.
6. (Opsional) Untuk menghapus snapshot terkait selama deregistrasi, pilih kotak centang Hapus snapshot terkait.

   > **Note**
   >
   > Jika snapshot dikaitkan dengan yang lain AMIs, itu tidak dihapus, bahkan jika kotak centang dipilih.

7. Pilih Deregister AMI.

   Mungkin perlu waktu beberapa menit sebelum konsol menghapus AMI dari daftar. Pilih Segarkan untuk menyegarkan status.

AWS CLI

Untuk membatalkan pendaftaran AMI

Gunakan perintah deregister-image berikut.

```
aws ec2 deregister-image --image-id ami-0abcdef1234567890
```

Untuk membatalkan pendaftaran AMI dan menghapus snapshot yang terkait

Gunakan perintah deregister-image berikut dan tentukan parameternya. `--delete-associated-snapshots` Perhatikan bahwa jika snapshot dikaitkan dengan yang lain AMIs, itu tidak dihapus, bahkan jika Anda menentukan parameter ini.

```
aws ec2 deregister-image \
    --image-id ami-0abcdef1234567890 \
    --delete-associated-snapshots
```

PowerShell

Untuk membatalkan pendaftaran AMI

Gunakan Unregister-EC2Imagecmdlet.

```
Unregister-EC2Image -ImageId ami-0abcdef1234567890
```

Untuk membatalkan pendaftaran AMI dan menghapus snapshot yang terkait

Gunakan Unregister-EC2Imagecmdlet dan tentukan parameternya`-DeleteAssociatedSnapshots`. Perhatikan bahwa jika snapshot dikaitkan dengan yang lain AMIs, itu tidak dihapus, bahkan jika Anda menentukan parameter ini.

```
Unregister-EC2Image `
    -ImageId ami-0abcdef1234567890 `
    -DeleteAssociatedSnapshots
```

Hindari biaya dari sumber daya yang tidak terpakai

Membatalkan pendaftaran AMI tidak, secara default, menghapus semua sumber daya yang terkait dengan AMI. Sumber daya ini termasuk snapshot untuk EBS yang didukung AMIs dan file di Amazon S3 untuk Amazon S3 yang didukung. AMIs Saat Anda membatalkan pendaftaran AMI, Anda juga tidak menghentikan atau menghentikan instans apa pun yang diluncurkan dari AMI.

Anda akan terus mengeluarkan biaya untuk menyimpan snapshot dan file, dan Anda akan dikenakan biaya untuk setiap instance yang berjalan.

Untuk menghindari timbulnya jenis biaya yang tidak perlu ini, kami sarankan untuk menghapus sumber daya apa pun yang tidak Anda perlukan.

Didukung EBS AMIs

- Hapus snapshot terkait saat membatalkan pendaftaran AMI. Untuk informasi selengkapnya, lihat Membatalkan pendaftaran AMI.
- Jika Anda membatalkan pendaftaran AMI tanpa menghapus snaphots terkait, Anda dapat menghapus snapshot secara manual. Cuplikan volume root instance yang dibuat selama pembuatan AMI memiliki format deskripsi berikut:

```
Created by CreateImage(i-1234567890abcdef0) for ami-0abcdef1234567890
```

- Jika Anda tidak lagi membutuhkan instans yang diluncurkan dari AMI, Anda dapat menghentikan atau menghentikannya. Untuk membuat daftar instance, filter berdasarkan ID AMI.

Didukung Amazon S3 AMIs

- Hapus bundel di Amazon S3 dengan menggunakan perintah (ec2-delete-bundleAMI tools).
- Jika bucket Amazon S3 kosong setelah Anda menghapus bundel, dan Anda tidak lagi menggunakan bucket tersebut, Anda dapat menghapus bucket tersebut.
- Jika Anda tidak lagi membutuhkan instans yang diluncurkan dari AMI, Anda dapat menghentikannya. Untuk membuat daftar instance, filter berdasarkan ID AMI.

Lindungi Amazon EC2 AMI dari deregistrasi

Anda dapat mengaktifkan perlindungan deregistrasi pada AMI untuk mencegah penghapusan yang tidak disengaja atau berbahaya. Saat Anda mengaktifkan perlindungan deregistrasi, AMI tidak dapat dideregistrasi oleh pengguna mana pun, terlepas dari izin IAM mereka. Jika Anda ingin membatalkan pendaftaran AMI, Anda harus mematikan perlindungan deregistrasi terlebih dahulu.

Saat Anda mengaktifkan perlindungan deregistrasi pada AMI, Anda memiliki opsi untuk menyertakan periode cooldown 24 jam. Periode cooldown ini adalah waktu di mana perlindungan deregistrasi tetap berlaku setelah Anda mematikannya. Selama periode cooldown ini, AMI tidak dapat dideregistrasi. Ketika periode cooldown berakhir, AMI dapat dideregistrasi.

Perlindungan deregistrasi dimatikan secara default pada semua yang ada dan yang baru. AMIs

Aktifkan perlindungan deregistrasi

Gunakan prosedur berikut untuk mengaktifkan perlindungan deregistrasi.

Console

Untuk mengaktifkan perlindungan deregistrasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Dari bilah filter, pilih Dimiliki oleh saya untuk mencantumkan yang tersedia AMIs, atau pilih Gambar yang dinonaktifkan untuk mencantumkan gambar yang dinonaktifkan AMIs.
4. Pilih AMI tempat Anda ingin mengaktifkan perlindungan deregistrasi, lalu pilih Tindakan, Kelola perlindungan deregistrasi AMI.
5. Di kotak dialog Kelola perlindungan deregistrasi AMI, Anda dapat mengaktifkan perlindungan deregistrasi dengan atau tanpa periode cooldown. Pilih salah satu opsi berikut:
   - Aktifkan dengan periode cooldown 24 jam — Dengan periode cooldown, AMI tidak dapat dideregistrasi selama 24 jam saat perlindungan deregistrasi dimatikan.
   - Aktifkan tanpa cooldown — Tanpa periode cooldown, AMI dapat segera dideregistrasi saat perlindungan deregistrasi dimatikan.
6. Pilih Simpan.

AWS CLI

Untuk mengaktifkan perlindungan deregistrasi

Gunakan perintah enable-image-deregistration-protection. Untuk mengaktifkan periode cooldown opsional, sertakan `--with-cooldown` opsi.

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0abcdef1234567890 \
    --with-cooldown
```

PowerShell

Untuk mengaktifkan perlindungan deregistrasi

Gunakan Enable-EC2ImageDeregistrationProtectioncmdlet. Untuk mengaktifkan periode cooldown opsional, atur `-WithCooldown` parameter `ketrue`.

```
Enable-EC2ImageDeregistrationProtection `
```

```
    -ImageId ami-0abcdef1234567890 `
    -WithCooldown $true
```

Matikan perlindungan deregistrasi

Gunakan prosedur berikut untuk mematikan perlindungan deregistrasi.

Jika Anda memilih untuk menyertakan periode cooldown 24 jam ketika Anda mengaktifkan perlindungan deregistrasi untuk AMI, maka, ketika Anda mematikan perlindungan deregistrasi, Anda tidak akan segera dapat membatalkan pendaftaran AMI. Periode cooldown adalah periode waktu 24 jam di mana perlindungan deregistrasi tetap berlaku bahkan setelah Anda mematikannya. Selama periode cooldown ini, AMI tidak dapat dideregistrasi. Setelah periode cooldown berakhir, AMI dapat dideregistrasi.

Console

Untuk mematikan perlindungan deregistrasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Dari bilah filter, pilih Dimiliki oleh saya untuk mencantumkan yang tersedia AMIs, atau pilih Gambar yang dinonaktifkan untuk mencantumkan gambar yang dinonaktifkan AMIs.
4. Pilih AMI untuk mematikan perlindungan deregistrasi, lalu pilih Tindakan, Kelola perlindungan deregistrasi AMI.
5. Di kotak dialog Kelola perlindungan deregistrasi AMI, pilih Nonaktifkan.
6. Pilih Simpan.

AWS CLI

Untuk mematikan perlindungan deregistrasi

Gunakan perintah disable-image-deregistration-protection.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0abcdef1234567890
```

PowerShell

Untuk mematikan perlindungan deregistrasi

Gunakan Disable-EC2ImageDeregistrationProtectioncmdlet.

```
Disable-EC2ImageDeregistrationProtection -ImageId ami-0abcdef1234567890
```

Perilaku peluncuran instans dengan mode boot Amazon EC2

Ketika komputer melakukan boot, perangkat lunak pertama yang berjalan bertanggung jawab untuk menginisialisasi platform dan menyediakan antarmuka bagi sistem operasi untuk melakukan operasi spesifik platform.

Di Amazon EC2, ada dua varian perangkat lunak mode boot yang didukung: Unified Extensible Firmware Interface (UEFI) dan Legacy BIOS.

Parameter mode boot yang mungkin terjadi pada AMI

AMI dapat memiliki salah satu nilai parameter mode boot berikut: `uefi`, `legacy-bios`, atau `uefi-preferred`. Parameter mode boot AMI bersifat opsional. Untuk AMIs tanpa parameter mode boot, instance yang diluncurkan dari ini AMIs menggunakan nilai mode boot default dari jenis instance.

Tujuan parameter mode boot AMI

Parameter mode boot AMI memberi tanda ke Amazon EC2 tentang mode boot mana yang digunakan saat meluncurkan instans. Saat parameter mode boot diatur ke `uefi`, EC2 mencoba untuk meluncurkan instans di UEFI. Jika sistem operasi tidak dikonfigurasi untuk mendukung UEFI, peluncuran instans tidak akan berhasil.

Parameter mode boot UEFI yang disukai

Anda dapat membuat AMIs yang mendukung UEFI dan Legacy BIOS dengan menggunakan parameter mode `uefi-preferred` boot. Saat parameter mode boot diatur ke `uefi-preferred`, dan jika tipe instans mendukung UEFI, instans akan diluncurkan di UEFI. Jika tipe instans tidak mendukung UEFI, instans akan diluncurkan di Legacy BIOS.

> **Warning**
>
> Beberapa fitur, seperti UEFI Secure Boot, hanya tersedia pada instans yang di-boot di UEFI. Saat Anda menggunakan parameter mode boot AMI `uefi-preferred` dengan tipe instans yang tidak mendukung UEFI, instans akan diluncurkan sebagai Legacy BIOS dan fitur yang

bergantung pada UEFI akan dinonaktifkan. Jika Anda mengandalkan ketersediaan fitur yang bergantung pada UEFI, atur parameter mode boot AMI Anda ke `uefi`.

Mode boot default sesuai tipe instans

- Tipe instans Graviton: UEFI
- Tipe instans Intel dan AMD: Legacy BIOS

Dukungan zona

Boot UEFI tidak didukung di Wavelength Zones.

Topik mode boot

- Persyaratan untuk meluncurkan instans EC2 dalam mode boot UEFI
- Tentukan parameter mode boot dari Amazon EC2 AMI
- Tentukan mode boot yang didukung dari jenis instans EC2
- Tentukan mode boot dari instans EC2
- Tentukan mode boot sistem operasi untuk instans EC2 Anda
- Mengatur mode boot Amazon EC2 AMI
- Variabel UEFI untuk instans Amazon EC2
- Boot Aman UEFI untuk instans Amazon EC2

Persyaratan untuk meluncurkan instans EC2 dalam mode boot UEFI

Mode boot instance ditentukan oleh konfigurasi AMI, sistem operasi yang terkandung di dalamnya, dan jenis instance. Untuk meluncurkan instance dalam mode boot UEFI, Anda harus memenuhi persyaratan berikut.

AMI

AMI harus dikonfigurasi untuk UEFI sebagai berikut:

- Sistem operasi – sistem operasi yang terdapat dalam AMI harus dikonfigurasi untuk menggunakan UEFI; jika tidak, peluncuran instans akan gagal. Untuk informasi selengkapnya, lihat Tentukan mode boot sistem operasi untuk instans EC2 Anda.

- Parameter mode boot AMI – Parameter mode boot AMI harus diatur ke `uefi` atau `uefi-preferred`. Untuk informasi selengkapnya, lihat Tentukan parameter mode boot dari Amazon EC2 AMI.

  Linux — Linux berikut AMIs mendukung UEFI:

  - Amazon Linux 2023
  - Amazon Linux 2 (hanya jenis instans Graviton)

  Untuk Linux lain AMIs, Anda harus mengkonfigurasi AMI, mengimpor AMI melalui VM Import/Export, atau mengimpor AMI melalui. CloudEndure

  Windows — Windows berikut AMIs mendukung UEFI:

  - Windows_Server-2025-* (kecuali dengan awalan nama) AMIs `BIOS-`
  - TPM-Windows_Server-2022-English-Full-Base
  - TPM-Windows_Server-2022-English-Core-Base
  - TPM-Windows_Server-2019-English-Full-Base
  - TPM-Windows_Server-2019-English-Core-Base
  - TPM-Windows_Server-2016-English-Full-Base
  - TPM-Windows_Server-2016-English-Core-Base

Tipe instans

  Semua instans yang dibangun di atas Sistem AWS Nitro mendukung UEFI dan Legacy BIOS, kecuali yang berikut: instans bare metal,, G4ad, P4, u-3tb1, u-6tb1, u-9tb1 DL1, u-12tb1, u-18tb1, u-24tb1, dan. VT1 Untuk informasi selengkapnya, lihat the section called “Mode boot tipe instans”.

Tabel berikut menunjukkan bahwa mode boot suatu instans (ditunjukkan oleh kolom Mode boot instans yang dihasilkan) ditentukan oleh kombinasi parameter mode boot AMI (kolom 1), konfigurasi mode boot dari sistem operasi yang berada dalam AMI (kolom 2), dan dukungan mode boot dari tipe instans tersebut (kolom 3).

Parameter mode boot AMI	Konfigurasi mode boot sistem operasi	Dukungan mode boot tipe instans	Mode boot instans yang dihasilkan
UEFI	UEFI	UEFI	UEFI
Legacy BIOS	Legacy BIOS	Legacy BIOS	Legacy BIOS

Parameter mode boot AMI	Konfigurasi mode boot sistem operasi	Dukungan mode boot tipe instans	Mode boot instans yang dihasilkan
UEFI Diutamakan	UEFI	UEFI	UEFI
UEFI Diutamakan	UEFI	UEFI dan Legacy BIOS	UEFI
UEFI Diutamakan	Legacy BIOS	Legacy BIOS	Legacy BIOS
UEFI Diutamakan	Legacy BIOS	UEFI dan Legacy BIOS	Legacy BIOS
Tidak ada mode boot yang ditentukan - ARM	UEFI	UEFI	UEFI
Tidak ada mode boot yang ditentukan - x86	Legacy BIOS	UEFI dan Legacy BIOS	Legacy BIOS

Tentukan parameter mode boot dari Amazon EC2 AMI

Parameter mode boot AMI bersifat opsional. AMI dapat memiliki salah satu nilai parameter mode boot berikut: `uefi`, `legacy-bios`, atau `uefi-preferred`.

Beberapa AMIs tidak memiliki parameter mode boot. Ketika AMI tidak memiliki parameter mode boot, instans yang diluncurkan dari AMI akan menggunakan nilai default dari tipe instans tersebut, yaitu `uefi` di Graviton, dan `legacy-bios` pada tipe instans Intel dan AMD.

Console

Untuk menentukan parameter mode boot AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs, lalu pilih AMI.
3. Periksa bidang Mode boot.
   - Nilai uefi menunjukkan bahwa AMI mendukung UEFI.
   - Nilai uefi-preferred menunjukkan bahwa AMI mendukung UEFI dan Legacy BIOS.

- Jika tidak ada nilai, instans yang diluncurkan dari AMI menggunakan nilai default dari tipe instans tersebut.

Untuk menentukan parameter mode boot AMI saat meluncurkan instance

Saat meluncurkan sebuah instans menggunakan wizard peluncuran instans, pada langkah untuk memilih AMI, periksa bidang Mode boot. Untuk informasi selengkapnya, lihat Aplikasi dan Gambar OS (Gambar Mesin Amazon).

AWS CLI

Untuk menentukan parameter mode boot AMI

Gunakan describe-imagesperintah untuk menentukan mode boot AMI.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-id ami-0abcdef1234567890 \
    --query Images[].BootMode \
    --output text
```

Berikut ini adalah output contoh.

```
uefi
```

Dalam output, nilai `uefi` menunjukkan bahwa AMI mendukung UEFI. Nilai `uefi-preferred` menunjukkan bahwa AMI mendukung UEFI dan Legacy BIOS. Jika tidak ada nilai, instans yang diluncurkan dari AMI menggunakan nilai default dari tipe instans tersebut.

PowerShell

Untuk menentukan parameter mode boot AMI

Gunakan Get-EC2Imagecmdlet untuk menentukan mode boot AMI.

```
Get-EC2Image -Region us-east-1 `
    -ImageId ami-0abcdef1234567890 | Format-List Name, BootMode, TpmSupport
```

Berikut ini adalah output contoh.

```
Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
```

```
BootMode   : uefi
TpmSupport : v2.0
```

Dalam output, nilai `BootMode` menunjukkan mode boot AMI. Nilai `uefi` menunjukkan bahwa AMI mendukung UEFI. Nilai `uefi-preferred` menunjukkan bahwa AMI mendukung UEFI dan Legacy BIOS. Jika tidak ada nilai, instans yang diluncurkan dari AMI menggunakan nilai default dari tipe instans tersebut.

Tentukan mode boot yang didukung dari jenis instans EC2

Anda dapat menentukan mode boot yang didukung dari jenis instance.

Konsol Amazon EC2 tidak menampilkan mode boot yang didukung dari jenis instans.

AWS CLI

Gunakan describe-instance-typesperintah untuk menentukan mode boot yang didukung dari jenis instance. `--query`Parameter menyaring output untuk mengembalikan hanya mode boot yang didukung.

Contoh berikut menunjukkan bahwa jenis instance yang ditentukan mendukung mode boot UEFI dan Legacy BIOS.

```
aws ec2 describe-instance-types \
    --instance-types m5.2xlarge \
    --query "InstanceTypes[*].SupportedBootModes"
```

Berikut ini adalah output contoh.

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

Contoh berikut menunjukkan bahwa `t2.xlarge` hanya mendukung Legacy BIOS.

```
aws ec2 describe-instance-types \
    --instance-types t2.xlarge \
```

```
    --query "InstanceTypes[*].SupportedBootModes"
```

Berikut ini adalah output contoh.

```
[
    [
        "legacy-bios"
    ]
]
```

PowerShell

Gunakan Get-EC2InstanceTypecmdlet untuk menentukan mode boot yang didukung dari jenis instance.

Contoh berikut menunjukkan bahwa `m5.2xlarge` mendukung mode boot UEFI dan Legacy BIOS.

```
Get-EC2InstanceType -InstanceType m5.2xlarge | Format-List InstanceType,
 SupportedBootModes
```

Berikut ini adalah output contoh.

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

Contoh berikut menunjukkan bahwa `t2.xlarge` hanya mendukung Legacy BIOS.

```
Get-EC2InstanceType -InstanceType t2.xlarge | Format-List InstanceType,
 SupportedBootModes
```

Berikut ini adalah output contoh.

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Untuk menentukan jenis instans yang mendukung UEFI

Anda dapat menentukan jenis instans yang mendukung UEFI. Konsol Amazon EC2 tidak menampilkan dukungan UEFI dari jenis instans.

AWS CLI

Tipe instans yang tersedia berbeda-beda menurut AWS Region. Untuk melihat jenis instance yang tersedia yang mendukung UEFI di Region, gunakan perintah. describe-instance-types Sertakan parameter `--filters` untuk cakupan hasil ke tipe instans yang mendukung UEFI dan parameter `--query` untuk cakupan output ke nilai `InstanceType`.

```
aws ec2 describe-instance-types \
    --filters Name=supported-boot-mode,Values=uefi \
    --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

PowerShell

Tipe instans yang tersedia berbeda-beda menurut AWS Region. Untuk melihat jenis instans yang tersedia yang mendukung UEFI di Wilayah, gunakan cmdlet. Get-EC2InstanceType

```
Get-EC2InstanceType | `
 Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration
```

Untuk menentukan jenis instans yang mendukung UEFI Secure Boot dan mempertahankan variabel non-volatile

Instans bare metal tidak mendukung UEFI Secure Boot dan variabel non-volatile, jadi contoh-contoh ini mengecualikan mereka dari output. Untuk informasi tentang UEFI Secure Boot, lihat Boot Aman UEFI untuk instans Amazon EC2.

AWS CLI

Gunakan describe-instance-typesperintah, dan kecualikan instance bare metal dari output.

```
aws ec2 describe-instance-types \
    --filters Name=supported-boot-mode,Values=uefi Name=bare-metal,Values=false \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Gunakan Get-EC2InstanceTypecmdlet, dan kecualikan instance bare metal dari output.

```
Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal, `
        @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}
```

Tentukan mode boot dari instans EC2

Mode boot sebuah instans ditampilkan di bidang Mode boot di konsol Amazon EC2, dan oleh parameter `currentInstanceBootMode` di AWS CLI.

Apabila sebuah instans diluncurkan, nilai untuk parameter mode boot-nya ditentukan oleh nilai parameter mode boot AMI yang digunakan untuk meluncurkannya, seperti berikut:

- AMI dengan parameter mode boot `uefi` menciptakan sebuah instans dengan parameter `currentInstanceBootMode` `uefi`.
- AMI dengan parameter mode boot `legacy-bios` menciptakan sebuah instans dengan parameter `currentInstanceBootMode` `legacy-bios`.
- AMI dengan parameter mode boot `uefi-preferred` menciptakan instans dengan parameter `currentInstanceBootMode` `uefi` jika tipe instans mendukung UEFI; jika tidak, ia membuat instans dengan parameter `currentInstanceBootMode` `legacy-bios`.
- AMI tanpa nilai parameter mode boot akan menciptakan instans dengan nilai parameter `currentInstanceBootMode` yang bergantung pada apakah arsitektur AMI adalah ARM atau x86 dan mode boot yang didukung tipe instans tersebut. Mode boot default adalah `uefi` pada tipe instans Graviton, dan `legacy-bios` pada tipe instans Intel dan AMD.

Console

Untuk menentukan mode boot dari sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Instans, kemudian pilih instans Anda.
3. Di tab Detail, periksa bidang Mode boot.

AWS CLI

Untuk menentukan mode boot dari sebuah instance

Gunakan perintah describe-instances untuk menentukan mode boot sebuah instans. Anda juga dapat menentukan mode boot AMI yang digunakan untuk membuat instans.

```
aws ec2 describe-instances \
    --region us-east-1 \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BootMode \
    --output text
```

Berikut ini adalah output contoh.

```
uefi
```

PowerShell

Untuk menentukan mode boot dari sebuah instance

Gunakan Get-EC2Imagecmdlet untuk menentukan mode boot sebuah instance. Anda juga dapat menentukan mode boot AMI yang digunakan untuk membuat instans.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId
```

Berikut ini adalah output contoh.

```
BootMode                : uefi
CurrentInstanceBootMode : uefi
InstanceType            : c5a.large
ImageId                 : ami-0abcdef1234567890
```

Tentukan mode boot sistem operasi untuk instans EC2 Anda

Mode boot AMI memandu Amazon EC2 tentang mode boot apa yang digunakan untuk melakukan boot instans. Untuk melihat apakah sistem operasi instans Anda dikonfigurasi untuk UEFI, Anda harus terhubung ke instans Anda menggunakan SSH (instance Linux) atau RDP (instance Windows).

Gunakan instruksi untuk sistem operasi instans Anda.

Linux

Untuk menentukan mode boot sistem operasi instans

1. Sambungkan ke instans Linux Anda menggunakan SSH.
2. Untuk melihat mode boot sistem operasi, coba salah satu hal berikut ini:

   - Jalankan perintah berikut.

     ```
     [ec2-user ~]$ sudo /usr/sbin/efibootmgr
     ```

     Output yang diharapkan dari sebuah instans yang diboot dalam mode boot UEFI

     ```
     BootCurrent: 0001
     Timeout: 0 seconds
     BootOrder: 0000,0001
     Boot0000* UiApp
     Boot0001* UEFI Amazon Elastic Block Store vol-xyz
     ```

   - Jalankan perintah berikut untuk memverifikasi keberadaan direktori `/sys/firmware/efi`. Direktori ini hanya ada jika instans boot menggunakan UEFI. Jika direktori ini tidak ada, perintah akan menampilkan `Legacy BIOS Boot Detected`.

     ```
     [ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo
      "Legacy BIOS Boot Detected"
     ```

     Output yang diharapkan dari sebuah instans yang diboot dalam mode boot UEFI

     ```
     UEFI Boot Detected
     ```

     Output yang diharapkan dari instans yang boot dalam mode boot Legacy BIOS

     ```
     Legacy BIOS Boot Detected
     ```

   - Jalankan perintah berikut untuk memverifikasi bahwa EFI muncul di output `dmesg`.

     ```
     [ec2-user ~]$ dmesg | grep -i "EFI"
     ```

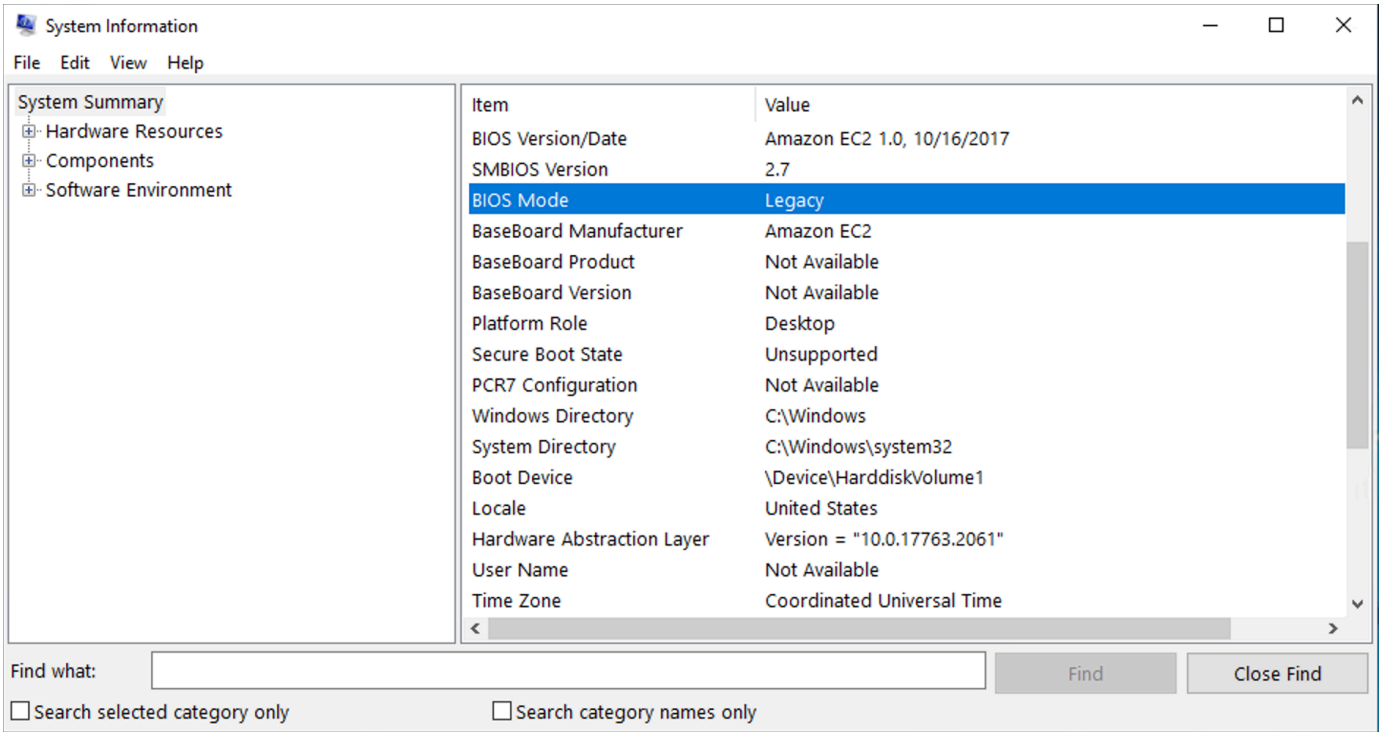
Output yang diharapkan dari sebuah instans yang diboot dalam mode boot UEFI

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

Windows

Untuk menentukan mode boot sistem operasi instans

1. Sambungkan ke instans Windows Anda menggunakan RDP.
2. Pergi ke Informasi Sistem dan periksa baris Mode BIOS.



Mengatur mode boot Amazon EC2 AMI

Secara default, AMI mewarisi mode boot instans EC2 yang digunakan untuk membuat AMI. Misalnya, jika Anda membuat AMI dari instans EC2 yang berjalan di Legacy BIOS, mode boot AMI baru adalah. `legacy-bios` Jika Anda membuat AMI dari instans EC2 dengan mode boot`uefi-preferred`, mode boot AMI baru adalah`uefi-preferred`.

Saat Anda mendaftarkan AMI, Anda dapat mengatur mode boot AMI keuefi,legacy-bios, atauuefi-preferred.

Ketika mode boot AMI diatur ke uefi-preferred, instans akan melakukan boot sebagai berikut:

- Untuk tipe instans yang mendukung UEFI dan Legacy BIOS (misalnya, m5.large), instans boot menggunakan UEFI.
- Untuk tipe instans yang hanya mendukung Legacy BIOS (misalnya, m4.large), instans boot menggunakan Legacy BIOS.

Jika Anda mengatur mode boot AMI ke uefi-preferred, sistem operasi harus mendukung kemampuan untuk melakukan boot UEFI dan Legacy BIOS.

Untuk mengonversi instans berbasis BioS Legacy yang ada ke UEFI, atau instans berbasis UEFI yang ada ke Legacy BIOS, Anda harus terlebih dahulu memodifikasi volume dan sistem operasi instans untuk mendukung mode boot yang dipilih. Kemudian, buat snapshot volume. Terakhir, buat AMI dari snapshot.

Pertimbangan-pertimbangan

- Menetapkan parameter mode boot AMI tidak secara otomatis mengonfigurasi sistem operasi untuk mode boot tersebut. Anda harus terlebih dahulu membuat modifikasi yang sesuai dengan volume instans dan sistem operasi untuk mendukung booting menggunakan mode boot yang dipilih. Jika tidak, AMI yang dihasilkan tidak dapat digunakan. Misalnya, jika Anda mengonversi instance Windows berbasis BioS Legacy ke UEFI, Anda dapat menggunakan MBR2alat GPT dari Microsoft untuk mengonversi disk sistem dari MBR ke GPT. Perubahan yang diperlukan adalah perubahan khusus sistem operasi. Untuk informasi lebih lanjut, lihat manual untuk sistem operasi Anda.
- Anda tidak dapat menggunakan register-imageperintah atau Register-EC2Imagecmdlet untuk membuat AMI yang mendukung NitRotPM dan UEFI Preferred.
- Beberapa fitur, seperti UEFI Secure Boot, hanya tersedia pada instans yang di-boot di UEFI. Saat Anda menggunakan parameter mode boot uefi-preferred AMI dengan tipe instans yang tidak mendukung UEFI, instance akan diluncurkan sebagai Legacy BIOS dan fitur yang bergantung pada UEFI dinonaktifkan. Jika Anda mengandalkan ketersediaan fitur yang bergantung pada UEFI, atur parameter mode boot AMI Anda ke uefi.

AWS CLI

Untuk mengatur mode boot AMI

1. Buat perubahan yang sesuai dengan volume instans dan sistem operasi untuk mendukung boot melalui mode boot yang dipilih. Perubahan yang diperlukan adalah perubahan khusus sistem operasi. Untuk informasi lebih lanjut, lihat manual untuk sistem operasi Anda.

   > **Warning**
   >
   > Jika Anda tidak melakukan langkah ini, AMI tidak akan dapat digunakan.

2. Untuk menemukan ID volume instans, gunakan perintah describe-instances. Anda akan membuat snapshot volume ini di langkah berikutnya.

   ```
   aws ec2 describe-instances \
       --instance-ids i-1234567890abcdef0 \
       --query Reservations[].Instances[].BlockDeviceMappings
   ```

   Berikut ini adalah output contoh.

   ```
   [
       [
           {
               "DeviceName": "/dev/xvda",
               "Ebs": {
                   "AttachTime": "2024-07-11T01:05:51+00:00",
                   "DeleteOnTermination": true,
                   "Status": "attached",
                   "VolumeId": "vol-1234567890abcdef0"
               }
           }
       ]
   ]
   ```

3. Untuk membuat snapshot volume, gunakan perintah create-snapshot. Gunakan ID volume dari langkah sebelumnya.

   ```
   aws ec2 create-snapshot \
       --volume-id vol-01234567890abcdef \
   ```

```
    --description "my snapshot"
```

Berikut ini adalah output contoh.

```
{
    "Description": "my snapshot",
    "Encrypted": false,
    "OwnerId": "123456789012",
    "Progress": "",
    "SnapshotId": "snap-0abcdef1234567890",
    "StartTime": "",
    "State": "pending",
    "VolumeId": "vol-01234567890abcdef",
    "VolumeSize": 30,
    "Tags": []
}
```

4. Tunggu sampai status snapshot `completed` sebelum Anda pergi ke langkah berikutnya. Untuk mendapatkan status snapshot, gunakan describe-snapshotsperintah dengan ID snapshot dari langkah sebelumnya.

```
aws ec2 describe-snapshots \
    --snapshot-ids snap-0abcdef1234567890 \
    --query Snapshots[].State \
    --output text
```

Berikut ini adalah output contoh.

```
completed
```

5. Untuk membuat AMI baru, gunakan perintah register-image. Gunakan nilai `SnapshotId` dari dari outputCreateSnapshot.

   - Untuk mengatur mode boot ke UEFI, tambahkan `--boot-mode` parameter dengan nilai. `uefi`

```
aws ec2 register-image \
   --description "my image" \
   --name "my-image" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-0abcdef1234567890,DeleteOnTermination=true}" \
```

```
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

- Untuk mengatur mode boot keuefi-preferred, atur nilai --boot-mode ke uefi-preferred

```
aws ec2 register-image \
   --description "my description" \
   --name "my-image" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-0abcdef1234567890,DeleteOnTermination=true}" \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi-preferred
```

6. (Opsional) Untuk memverifikasi bahwa AMI yang baru dibuat memiliki mode boot yang Anda tentukan, gunakan perintah. describe-images

```
aws ec2 describe-images \
    --image-id ami-1234567890abcdef0 \
    --query Images[].BootMode \
    --output text
```

Berikut ini adalah output contoh.

```
uefi
```

PowerShell

Untuk mengatur mode boot AMI

1. Buat perubahan yang sesuai dengan volume instans dan sistem operasi untuk mendukung boot melalui mode boot yang dipilih. Perubahan yang diperlukan adalah perubahan khusus sistem operasi. Untuk informasi lebih lanjut, lihat manual untuk sistem operasi Anda.

> **Warning**
>
> Jika Anda tidak melakukan langkah ini, AMI tidak akan dapat digunakan.

2. Untuk menemukan ID volume instance, gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Berikut ini adalah output contoh.

```
AssociatedResource  :
AttachTime          : 7/11/2024 1:05:51 AM
DeleteOnTermination : True
Operator            :
Status              : attached
VolumeId            : vol-01234567890abcdef
```

3. Untuk membuat snapshot volume, gunakan New-EC2Snapshotcmdlet. Gunakan ID volume dari langkah sebelumnya.

```
New-EC2Snapshot `
    -VolumeId vol-01234567890abcdef `
    -Description "my snapshot"
```

Berikut ini adalah output contoh.

```
AvailabilityZone          :
Description               : my snapshot
Encrypted                 : False
FullSnapshotSizeInBytes   : 0
KmsKeyId                  :
OwnerId                   : 123456789012
RestoreExpiryTime         :
SnapshotId                : snap-0abcdef1234567890
SseType                   :
StartTime                 : 4/25/2025 6:08:59 PM
State                     : pending
StateMessage              :
VolumeId                  : vol-01234567890abcdef
```

```
VolumeSize                : 30
```

4. Tunggu sampai status snapshot `completed` sebelum Anda pergi ke langkah berikutnya. Untuk mendapatkan status snapshot, gunakan Get-EC2Snapshotcmdlet dengan ID snapshot dari langkah sebelumnya.

```
(Get-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890).State.Value
```

Berikut ini adalah output contoh.

```
completed
```

5. Untuk membuat AMI baru, gunakan Register-EC2Imagecmdlet. Gunakan nilai `SnapshotId` dari dari outputNew-EC2Snapshot.

- Untuk mengatur mode boot ke UEFI, tambahkan `-BootMode` parameter dengan nilai. `uefi`

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
   -Description "my image" `
   -Name "my-image" `
   -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
   -RootDeviceName /dev/xvda `
   -EnaSupport $true `
   -BootMode uefi
```

- Untuk mengatur mode boot keuefi-preferred, atur nilai `-BootMode` ke `uefi-preferred`

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
   -Description "my image" `
   -Name "my-image" `
   -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
   -RootDeviceName /dev/xvda `
   -EnaSupport $true `
   -BootMode uefi-preferred
```

6. (Opsional) Untuk memverifikasi bahwa AMI yang baru dibuat memiliki mode boot yang Anda tentukan, gunakan cmdlet. Get-EC2Image

```
(Get-EC2Image `
    -ImageId ami-1234567890abcdef0).BootMode.Value
```

Berikut ini adalah output contoh.

```
uefi
```

Variabel UEFI untuk instans Amazon EC2

Saat Anda meluncurkan instans di mana mode boot diatur ke UEFI, penyimpanan nilai kunci untuk variabel akan dibuat. Penyimpanan dapat digunakan oleh UEFI dan sistem operasi instans untuk menyimpan variabel UEFI.

Variabel UEFI digunakan oleh boot loader dan sistem operasi untuk mengonfigurasi startup sistem awal. Variabel ini memungkinkan sistem operasi untuk mengelola pengaturan tertentu dari proses boot, seperti urutan boot, atau mengelola kunci untuk UEFI Secure Boot.

> **Warning**
>
> Siapa pun yang dapat terhubung ke instance (dan berpotensi perangkat lunak apa pun yang berjalan pada instance), atau siapa pun yang memiliki izin untuk menggunakan GetInstanceUefiDataAPI pada instance dapat membaca variabel. Anda tidak boleh menyimpan data sensitif, seperti sandi atau informasi identitas pribadi, di penyimpanan variabel UEFI.

Persistensi variabel UEFI

- Untuk instans yang diluncurkan pada atau sebelum 10 Mei 2022, variabel UEFI dihapus saat boot ulang atau berhenti.
- Untuk instans yang diluncurkan pada atau setelah 11 Mei 2022, variabel UEFI yang ditandai sebagai non-volatile akan dipertahankan saat boot ulang dan berhenti/mulai.
- Instans bare metal tidak mempertahankan variabel non-volatile UEFI di seluruh operasi berhenti/memulai instans.

Boot Aman UEFI untuk instans Amazon EC2

UEFI Secure Boot dibangun di atas proses boot aman lama Amazon EC2, dan menyediakan tambahan yang membantu pelanggan mengamankan perangkat lunak dari ancaman defense-in-depth yang bertahan selama reboot. UEFI Secure Boot memastikan bahwa instans hanya melakukan boot perangkat lunak yang diberi tanda dengan kunci kriptografi. Kunci disimpan dalam basis data kunci di penyimpanan variabel non-volatile UEFI. UEFI Secure Boot mencegah modifikasi yang tidak sah dari aliran boot instans.

Daftar Isi

- Cara kerja Boot Aman UEFI dengan instans Amazon EC2
- Persyaratan untuk Boot Aman UEFI di Amazon EC2
- Verifikasi apakah instans Amazon EC2 diaktifkan untuk Boot Aman UEFI
- Buat AMI Linux dengan tombol Boot Aman UEFI kustom
- Buat gumpalan AWS biner untuk UEFI Secure Boot

Cara kerja Boot Aman UEFI dengan instans Amazon EC2

UEFI Secure Boot adalah fitur yang ditentukan dalam UEFI, yang menyediakan verifikasi tentang keadaan rantai boot. UEFI Secure Boot dirancang untuk memastikan bahwa hanya binari UEFI yang terverifikasi secara kriptografis yang akan dieksekusi setelah inisialisasi mandiri pada firmware. Binari ini termasuk driver UEFI dan bootloader utama, serta komponen yang dimuat rantai.

UEFI Secure Boot menetapkan empat basis data utama, yang digunakan dalam rantai kepercayaan. Basis data disimpan di penyimpanan variabel UEFI.

Rantai kepercayaan tersebut adalah sebagai berikut:

Basis data kunci platform (PK)

> Basis data PK adalah root kepercayaan. Basis data ini berisi satu kunci PK publik yang digunakan dalam rantai kepercayaan untuk memperbarui basis data kunci untuk pertukaran kunci (KEK).
>
> Untuk mengubah basis data PK, Anda harus memiliki kunci PK privat untuk menandatangani permintaan pembaruan. Ini termasuk menghapus basis data PK dengan menulis kunci PK kosong.

Basis data kunci untuk pertukaran kunci (KEK)

Basis data KEK adalah daftar kunci KEK publik yang digunakan dalam rantai kepercayaan untuk memperbarui basis data tanda tangan (db) dan denylist (dbx).

Untuk mengubah basis data KEK publik, Anda harus memiliki kunci PK privat untuk menandatangani permintaan pembaruan.

Basis data tanda tangan (db)

Basis data db adalah daftar kunci publik dan hash yang digunakan dalam rantai kepercayaan untuk memvalidasi semua binari boot UEFI.

Untuk mengubah basis data db, Anda harus memiliki kunci PK privat atau salah satu kunci KEK privat untuk menandatangani permintaan pembaruan.

Basis data denylist tanda tangan (dbx)

Basis data dbx adalah daftar kunci publik dan hash biner yang tidak tepercaya, dan digunakan dalam rantai kepercayaan sebagai file pencabutan.

Basis data dbx selalu diutamakan daripada semua basis data kunci lainnya.

Untuk mengubah basis data dbx, Anda harus memiliki kunci PK privat atau kunci KEK privat apa pun untuk menandatangani permintaan pembaruan.

Forum UEFI mengelola dbx yang tersedia untuk umum untuk banyak biner dan sertifikat yang diketahui buruk di https://uefi.org/revocationlistfile.

Important

UEFI Secure Boot memberlakukan validasi tanda tangan pada binari UEFI apa pun. Untuk mengizinkan eksekusi biner UEFI di UEFI Secure Boot, Anda menandatanganinya dengan salah satu kunci db privat yang dijelaskan di atas.

Secara default, UEFI Secure Boot dinonaktifkan dan sistem ada pada `SetupMode`. Ketika sistem ada di `SetupMode`, semua variabel kunci dapat diperbarui tanpa tanda tangan kriptografis. Ketika PK diatur, UEFI Secure Boot diaktifkan dan keluar. SetupMode

Persyaratan untuk Boot Aman UEFI di Amazon EC2

Saat Anda meluncurkan instans Amazon EC2 dengan AMI yang didukung dan jenis instans yang didukung, instans tersebut akan secara otomatis memvalidasi binari boot UEFI terhadap database Boot Aman UEFI. Tidak diperlukan konfigurasi tambahan. Anda juga dapat mengonfigurasi UEFI Secure Boot pada sebuah instans setelah diluncurkan.

> **Note**
>
> UEFI Secure Boot melindungi instans Anda dan sistem operasinya dari perubahan aliran boot. Jika Anda membuat AMI baru dari sumber AMI yang mengaktifkan UEFI Secure Boot dan memodifikasi parameter tertentu selama proses penyalinan, seperti mengubah bagian `UefiData` dalam AMI, Anda dapat menonaktifkan Boot Aman UEFI.

Daftar Isi

- Didukung AMIs
- Tipe instans yang didukung

Didukung AMIs

Linux AMIs

Untuk meluncurkan instance Linux, AMI Linux harus mengaktifkan UEFI Secure Boot.

Amazon Linux mendukung UEFI Secure Boot dimulai dengan AL2023 rilis 2023.1. Namun, Boot Aman UEFI tidak diaktifkan secara default. AMIs Untuk informasi selengkapnya, lihat Boot Aman UEFI di AL2023 Panduan Pengguna. Versi lama Amazon Linux AMIs tidak diaktifkan untuk UEFI Secure Boot. Agar dapat menggunakan AMI yang didukung, Anda harus melakukan sejumlah langkah konfigurasi pada Linux AMI Anda sendiri. Untuk informasi selengkapnya, lihat Buat AMI Linux dengan tombol Boot Aman UEFI kustom.

Jendela AMIs

Untuk meluncurkan instance Windows, AMI Windows harus mengaktifkan UEFI Secure Boot. Untuk menemukan AMI AWS Windows yang telah dikonfigurasi sebelumnya untuk Boot Aman UEFI dengan kunci Microsoft, lihat Temukan Windows Server yang AMIs dikonfigurasi dengan NitRotPM dan UEFI Secure Boot di Referensi Windows.AWS AMIs

Saat ini, kami tidak mendukung mengimpor Windows dengan UEFI Secure Boot dengan menggunakan perintah import-image.

Tipe instans yang didukung

Semua jenis instans virtual yang mendukung UEFI juga mendukung UEFI Secure Boot. Untuk tipe instans yang mendukung UEFI Secure Boot, lihat Persyaratan untuk mode boot UEFI.

> **Note**
>
> Tipe instans bare metal tidak mendukung UEFI Secure Boot.

Verifikasi apakah instans Amazon EC2 diaktifkan untuk Boot Aman UEFI

Anda dapat menggunakan prosedur berikut untuk menentukan apakah Amazon EC2 diaktifkan untuk Boot Aman UEFI.

Instans Linux

Anda dapat menggunakan utilitas `mokutil` untuk memverifikasi apakah instans Linux diaktifkan untuk UEFI Secure Boot. Jika `mokutil` tidak diinstal pada instans Anda, Anda harus menginstalnya. Untuk petunjuk penginstalan Amazon Linux 2, lihat Menemukan dan menginstal paket perangkat lunak pada instans Amazon Linux 2. Untuk distribusi Linux lainnya, lihat dokumentasi spesifiknya.

Untuk memverifikasi apakah sebuah instans Linux diaktifkan untuk UEFI Secure Boot

Connect ke instance Anda dan jalankan perintah berikut seperti `root` pada jendela terminal.

```
mokutil --sb-state
```

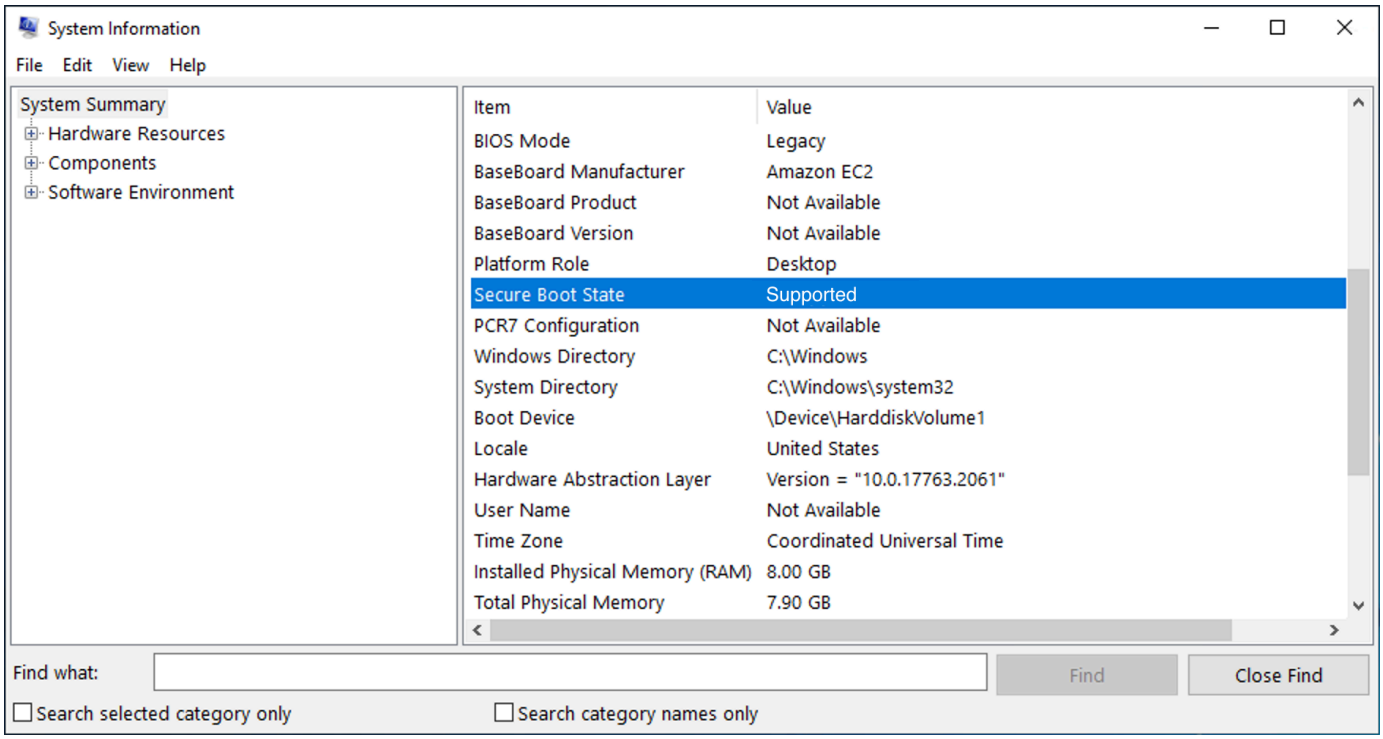
Berikut ini adalah output contoh.

- Jika UEFI Secure Boot diaktifkan, output berisi `SecureBoot enabled`.
- Jika UEFI Secure Boot tidak diaktifkan, output berisi `SecureBoot disabled` atau `Failed to read SecureBoot`.

Instans Windows

Untuk memverifikasi apakah sebuah instans Windows diaktifkan untuk UEFI Secure Boot

1. Terhubung ke instans Anda.
2. Buka alat msinfo32.
3. Periksa bidang Kondisi Secure Boot. Jika UEFI Secure Boot diaktifkan, nilainya Didukung, seperti yang ditunjukkan pada gambar berikut.



Anda juga dapat menggunakan Windows PowerShell Cmdlet `Confirm-SecureBootUEFI` untuk memeriksa status Boot Aman. Untuk informasi selengkapnya tentang cmdlet, lihat Konfirmasi-SecureBoot UEFI di Dokumentasi Microsoft.

Buat AMI Linux dengan tombol Boot Aman UEFI kustom

Petunjuk ini menunjukkan kepada Anda cara membuat AMI Linux dengan UEFI Secure Boot dan kunci pribadi yang dibuat khusus. Amazon Linux mendukung UEFI Secure Boot dimulai dengan AL2023 rilis 2023.1. Untuk informasi selengkapnya, lihat Boot Aman UEFI aktif AL2023 di Panduan Pengguna Amazon Linux 2023.

> **Important**
>
> Prosedur berikut ditujukan untuk pengguna tingkat lanjut saja. Anda harus memiliki pengetahuan yang cukup tentang alur boot distribusi SSL dan Linux untuk menggunakan prosedur ini.

Prasyarat

- Alat-alat berikut akan digunakan:
  - OpenSSL – https://www.openssl.org/
  - efivar — efivar https://github.com/rhboot/
  - efitools - https://git.kernel. org/pub/scm/linux/kernel/git/jejb/efitools.git/
  - Perintah get-instance-uefi-data
- Instans Linux Anda harus telah diluncurkan dengan AMI Linux yang mendukung mode boot UEFI, dan memiliki data non-volatile.

Instans yang baru dibuat tanpa kunci UEFI Secure Boot akan dibuat di `SetupMode`, yang memungkinkan Anda untuk mendaftarkan kunci Anda sendiri. Beberapa AMIs datang pra-konfigurasi dengan UEFI Secure Boot dan Anda tidak dapat mengubah kunci yang ada. Jika Anda ingin mengubah kunci, Anda harus membuat AMI baru berdasarkan AMI yang asli.

Anda memiliki dua cara untuk menyebarkan kunci di penyimpanan variabel, yang dijelaskan dalam Opsi A dan Opsi B di bawah ini. Opsi A menjelaskan bagaimana melakukan ini dari dalam instans, meniru aliran perangkat keras nyata. Opsi B menjelaskan cara membuat gumpalan biner, yang kemudian diteruskan sebagai file base64 saat Anda membuat AMI. Untuk kedua opsi, Anda harus terlebih dahulu membuat tiga pasang kunci, yang digunakan untuk rantai kepercayaan.

Untuk membuat AMI Linux yang mendukung UEFI Secure Boot, pertama-tama buat tiga pasangan kunci, lalu selesaikan Opsi A atau Opsi B, tetapi tidak keduanya:

- Tugas 1: Buat pasangan kunci
- Tugas 2 - Opsi A: Tambahkan kunci ke toko variabel dari dalam instance
- Tugas 2 - Opsi B: Buat gumpalan biner yang berisi penyimpanan variabel yang telah diisi sebelumnya

Tugas 1: Buat pasangan kunci

UEFI Secure Boot didasarkan pada tiga basis data utama berikut, yang digunakan dalam rantai kepercayaan: kunci platform (PK), kunci untuk pertukaran kunci (KEK), dan basis data (db) tanda tangan.[1]

Anda membuat setiap kunci pada instans. Untuk menyiapkan kunci publik dalam format yang valid untuk standar UEFI Secure Boot, Anda membuat sertifikat untuk setiap kunci. `DER` mendefinisikan format SSL (pengodean biner suatu format). Anda kemudian mengonversi setiap sertifikat menjadi daftar tanda tangan UEFI, yang merupakan format biner yang dipahami oleh UEFI Secure Boot. Terakhir, Anda menandatangani setiap sertifikat dengan kunci yang relevan.

Tugas

- Bersiap untuk membuat pasangan kunci
- Pasangan kunci 1: Buat kunci platform (PK)
- Pasangan kunci 2: Buat kunci untuk pertukaran kunci (KEK)
- Pasangan kunci 3: Buat basis data (db) tanda tangan
- Tanda tangani gambar boot (kernel) dengan kunci privat

Bersiap untuk membuat pasangan kunci

Sebelum membuat pasangan kunci, buat pengidentifikasi unik global (GUID) untuk digunakan dalam pembuatan kunci.

1. Hubungkan ke instans.
2. Jalankan perintah berikut di prompt shell.

```
uuidgen --random > GUID.txt
```

Pasangan kunci 1: Buat kunci platform (PK)

PK adalah root kepercayaan untuk instans UEFI Secure Boot. PK privat digunakan untuk memperbarui KEK, yang nantinya dapat digunakan untuk menambahkan kunci resmi ke basis data (db) tanda tangan.

Standar X.509 digunakan untuk membuat pasangan kunci. Untuk informasi tentang standar yang digunakan, lihat X.509 di Wikipedia.

Untuk membuat PK

1. Buat kunci. Anda harus memberi nama variabel PK.

   ```
   openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
   subj "/CN=Platform key/" -out PK.crt
   ```

   Parameter berikut ditentukan:

   - `-keyout PK.key` – File kunci privat.
   - `-days 3650` – Jumlah hari sertifikat tersebut valid.
   - `-out PK.crt` – Sertifikat yang digunakan untuk membuat variabel UEFI.
   - `CN=Platform key` – Nama umum (CN) untuk kunci. Anda dapat memasukkan nama organisasi Anda sendiri alih-alih*Platform key*.
2. Buat sertifikat.

   ```
   openssl x509 -outform DER -in PK.crt -out PK.cer
   ```
3. Konversi sertifikat menjadi daftar tanda tangan UEFI.

   ```
   cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
   ```
4. Tanda tangani daftar tanda tangan UEFI dengan PK privat (yang ditandatangani sendiri).

   ```
   sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
   ```

Pasangan kunci 2: Buat kunci untuk pertukaran kunci (KEK)

KEK privat digunakan untuk menambahkan kunci ke db, yang merupakan daftar tanda tangan resmi untuk boot pada sistem.

Untuk membuat PK

1. Buat kunci.

   ```
   openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
   subj "/CN=Key Exchange Key/" -out KEK.crt
   ```
2. Buat sertifikat.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Konversi sertifikat menjadi daftar tanda tangan UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Tanda tangani daftar tanda tangan dengan PK privat.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Pasangan kunci 3: Buat basis data (db) tanda tangan

Daftar db berisi kunci resmi yang diizinkan untuk di-boot pada sistem. Untuk memodifikasi daftar ini, diperlukan KEK privat. Gambar boot akan ditandatangani dengan kunci privat yang dibuat pada langkah ini.

Untuk membuat PK

1. Buat kunci.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Buat sertifikat.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Konversi sertifikat menjadi daftar tanda tangan UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Tanda tangani daftar tanda tangan dengan KEK privat.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Tanda tangani gambar boot (kernel) dengan kunci privat

Untuk Ubuntu 22.04, gambar berikut memerlukan tanda tangan.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

Untuk menandatangani gambar

Gunakan sintaksis berikut untuk menandatangani gambar.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Anda harus menandatangani semua kernel baru. */boot/vmlinuz* biasanya akan symlink ke kernel yang terakhir diinstal.

Lihat dokumentasi distribusi Anda untuk menemukan rantai boot dan gambar yang diperlukan.

[1] Terima kasih kepada ArchWiki komunitas untuk semua pekerjaan yang telah mereka lakukan. Perintah untuk membuat PK, membuat KEK, membuat DB, dan menandatangani gambar berasal dari Creating keys, yang ditulis oleh Tim ArchWiki and/or Pemeliharaan kontributor. ArchWiki

Tugas 2 - Opsi A: Tambahkan kunci ke toko variabel dari dalam instance

Setelah Anda membuat tiga pasang kunci, Anda dapat terhubung ke instans Anda dan menambahkan kunci ke penyimpanan variabel dari dalam instans dengan menyelesaikan langkah-langkah berikut. Atau, selesaikan langkah-langkahnyathe section called “Tugas 2 - Opsi B: Buat gumpalan biner yang berisi penyimpanan variabel yang telah diisi sebelumnya”.

Langkah-langkah Opsi A:

- Langkah 1: Luncurkan instans yang akan mendukung UEFI Secure Boot
- Langkah 2: Konfigurasikan instans untuk mendukung UEFI Secure Boot
- Langkah 3: Buat AMI dari instans

Langkah 1: Luncurkan instans yang akan mendukung UEFI Secure Boot

Ketika Anda meluncurkan sebuah instans dengan prasyarat berikut, instans kemudian akan siap untuk dikonfigurasi untuk mendukung UEFI Secure Boot. Anda hanya dapat mengaktifkan dukungan untuk UEFI Secure Boot pada instans saat peluncuran; Anda tidak dapat mengaktifkannya nanti.

Prasyarat

- AMI – AMI Linux harus mendukung mode boot UEFI. Untuk memverifikasi bahwa AMI mendukung mode boot UEFI, parameter mode boot AMI harus uefi. Untuk informasi selengkapnya, lihat Tentukan parameter mode boot dari Amazon EC2 AMI.

  Perhatikan bahwa AWS hanya menyediakan Linux yang AMIs dikonfigurasi untuk mendukung UEFI untuk jenis instans berbasis Graviton. AWS saat ini tidak menyediakan x86_64 Linux AMIs yang mendukung mode boot UEFI. Anda dapat mengonfigurasi AMI Anda sendiri untuk mendukung mode boot UEFI untuk semua arsitektur. Untuk mengonfigurasi AMI Anda sendiri untuk mendukung mode boot UEFI, Anda harus melakukan sejumlah langkah konfigurasi pada AMI Anda sendiri. Untuk informasi selengkapnya, lihat Mengatur mode boot Amazon EC2 AMI.
- Tipe instans – Semua tipe instans virtual yang mendukung UEFI juga mendukung UEFI Secure Boot. Tipe instans bare metal tidak mendukung UEFI Secure Boot. Untuk tipe instans yang mendukung UEFI Secure Boot, lihat Persyaratan untuk mode boot UEFI.
- Luncurkan instans Anda setelah rilis UEFI Secure Boot. Hanya instans yang diluncurkan setelah 10 Mei 2022 (saat UEFI Secure Boot dirilis) yang dapat mendukung UEFI Secure Boot.

Setelah Anda meluncurkan instans Anda, Anda dapat memverifikasi bahwa instans siap dikonfigurasi untuk mendukung UEFI Secure Boot (dengan kata lain, Anda dapat melanjutkan ke Langkah 2) dengan memeriksa apakah tersedia data UEFI. Keberadaan data UEFI menunjukkan bahwa data non-volatile tetap ada.

Untuk memverifikasi apakah instans Anda siap untuk Langkah 2

Gunakan perintah get-instance-uefi-data dan tentukan ID instans.

```
aws ec2 get-instance-uefi-data --instance-id i-1234567890abcdef0
```

Instans siap untuk Langkah 2 jika data UEFI sudah tersedia dalam output. Jika output kosong, instans tidak dapat dikonfigurasi untuk mendukung UEFI Secure Boot. Hal ini dapat terjadi jika instans Anda diluncurkan sebelum dukungan UEFI Secure Boot tersedia. Luncurkan instans baru dan coba lagi.

Langkah 2: Konfigurasikan instans untuk mendukung UEFI Secure Boot

Daftarkan pasangan kunci di penyimpanan variabel UEFI Anda pada instans

> **Warning**
>
> Anda harus menandatangani gambar boot Anda setelah Anda mendaftarkan kunci, jika tidak, Anda tidak akan dapat melakukan boot instans Anda.

Setelah Anda membuat daftar tanda tangan UEFI yang ditandatangani (`PK`, `KEK`, dan `db`), tanda tangan tersebut harus terdaftar ke firmware UEFI.

Penulisan ke variabel `PK` hanya dapat dilakukan jika:

- Belum ada PK yang terdaftar, yang ditunjukkan jika variabel `SetupMode` nya `1`. Periksa ini dengan menggunakan perintah berikut. Outputnya adalah `1` atau `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- PK yang baru ditandatangani oleh kunci privat dari PK yang ada.

Untuk mendaftarkan kunci di penyimpanan variabel UEFI Anda

Perintah berikut harus dijalankan pada instans.

Jika SetupMode diaktifkan (nilainya1), kunci dapat didaftarkan dengan menjalankan perintah berikut pada instance:

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

Untuk memverifikasi bahwa UEFI Secure Boot diaktifkan

Untuk memverifikasi bahwa UEFI Secure Boot diaktifkan, ikuti langkah-langkah di Verifikasi apakah instans Amazon EC2 diaktifkan untuk Boot Aman UEFI.

Anda sekarang dapat mengekspor penyimpanan variabel UEFI Anda dengan perintah CLI get-instance-uefi-data, atau Anda melanjutkan ke langkah berikutnya dan menandatangani gambar boot Anda untuk boot ulang ke instans dengan UEFI Secure Boot diaktifkan.

Langkah 3: Buat AMI dari instans

Untuk membuat AMI dari instance, Anda dapat menggunakan konsol atau `CreateImage` API, CLI, atau. SDKs Untuk instruksi konsol, lihat Buat AMI yang didukung Amazon EBS-Backed. Untuk petunjuk API, lihat CreateImage.

> **Note**
>
> API `CreateImage` secara otomatis menyalin penyimpanan variabel UEFI dari instans ke AMI. Konsol menggunakan API `CreateImage`. Setelah Anda meluncurkan instans menggunakan AMI ini, instans akan memiliki penyimpanan variabel UEFI yang sama.

Tugas 2 - Opsi B: Buat gumpalan biner yang berisi penyimpanan variabel yang telah diisi sebelumnya

Setelah Anda membuat tiga pasangan kunci, Anda dapat membuat gumpalan biner yang berisi penyimpanan variabel yang telah diisi sebelumnya yang berisi kunci UEFI Secure Boot. Atau, selesaikan langkah-langkahnyathe section called “Tugas 2 - Opsi A: Tambahkan kunci ke toko variabel dari dalam instance”.

> **Warning**
>
> Anda harus menandatangani gambar boot Anda sebelum mendaftarkan kunci, jika tidak, Anda tidak akan dapat melakukan boot instans Anda.

Langkah-langkah Opsi B:

- Langkah 1: Buat penyimpanan variabel baru atau perbarui yang sudah ada
- Langkah 2: Unggah gumpalan biner pada pembuatan AMI

Langkah 1: Buat penyimpanan variabel baru atau perbarui yang sudah ada

Anda dapat membuat penyimpanan variabel offline tanpa instans yang berjalan dengan menggunakan python-uefivars. Alat ini dapat membuat penyimpanan variabel baru dari kunci Anda.

Skrip saat ini mendukung EDK2 format, AWS format, dan representasi JSON yang lebih mudah diedit dengan perkakas tingkat yang lebih tinggi.

Untuk membuat penyimpanan variabel offline tanpa instans yang berjalan

1. Unduh alat di tautan berikut.

   ```
   https://github.com/awslabs/python-uefivars
   ```

2. Buat penyimpanan variabel baru dari kunci Anda dengan menjalankan perintah berikut. Ini akan membuat gumpalan biner berenkode base64 di.bin. *your_binary_blob* Alat ini juga mendukung pembaruan gumpalan biner melalui parameter `-I`.

   ```
   ./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
    db.esl --dbx dbx.esl
   ```

Langkah 2: Unggah gumpalan biner pada pembuatan AMI

Gunakan register-image untuk meneruskan data penyimpanan variabel UEFI Anda. Untuk parameter `--uefi-data`, tentukan gumpalan biner Anda, dan untuk parameter `--boot-mode`, tentukan `uefi`.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

Buat gumpalan AWS biner untuk UEFI Secure Boot

Anda dapat menggunakan langkah-langkah berikut untuk mengkustomisasi variabel UEFI Secure Boot selama pembuatan AMI. KEK yang digunakan dalam langkah-langkah ini berlaku per September 2021. Jika Microsoft memperbarui KEK, Anda harus menggunakan KEK terbaru.

Untuk membuat gumpalan AWS biner

1. Buat daftar tanda tangan PK kosong.

```
touch empty_key.crt
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Unduh sertifikat KEK.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Bungkus sertifikat KEK dalam daftar tanda tangan UEFI (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Unduh sertifikat db Microsoft.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Hasilkan daftar tanda tangan db.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. Unified Extensible Firmware Interface Forum tidak lagi menyediakan file DBX. Mereka sekarang disediakan oleh Microsoft di GitHub. Unduh pembaruan DBX terbaru dari repositori pembaruan Microsoft Secure Boot di secureboot_objects. https://github.com/microsoft/

7. Buka paket biner pembaruan yang ditandatangani.

   Buat `SplitDbxContent.ps1` dengan konten skrip di bawah ini. Atau, Anda dapat menginstal skrip dari PowerShell Galeri menggunakan`Install-Script -Name SplitDbxContent`.

```
<#PSScriptInfo

.VERSION 1.0
```

```
.GUID ec45a3fc-5e87-4d90-b55e-bdea083f732d

.AUTHOR Microsoft Secure Boot Team

.COMPANYNAME Microsoft

.COPYRIGHT Microsoft

.TAGS Windows Security

.LICENSEURI

.PROJECTURI

.ICONURI

.EXTERNALMODULEDEPENDENCIES

.REQUIREDSCRIPTS

.EXTERNALSCRIPTDEPENDENCIES

.RELEASENOTES
Version 1.0: Original published version.

#>

<#
.DESCRIPTION
 Splits a DBX update package into the new DBX variable contents and the signature
 authorizing the change.
 To apply an update using the output files of this script, try:
 Set-SecureBootUefi -Name dbx -ContentFilePath .\content.bin -SignedFilePath .
\signature.p7 -Time 2010-03-06T19:17:21Z -AppendWrite'
.EXAMPLE
.\SplitDbxAuthInfo.ps1 DbxUpdate_x64.bin
#>


# Get file from script input
$file  = Get-Content -Encoding Byte $args[0]

# Identify file signature
$chop = $file[40..($file.Length - 1)]
```

```
if (($chop[0] -ne 0x30) -or ($chop[1] -ne 0x82 )) {
    Write-Error "Cannot find signature"
    exit 1
}

# Signature is known to be ASN size plus header of 4 bytes
$sig_length = ($chop[2] * 256) + $chop[3] + 4
$sig = $chop[0..($sig_length - 1)]

if ($sig_length -gt ($file.Length + 40)) {
    Write-Error "Signature longer than file size!"
    exit 1
}

# Content is everything else
$content = $file[0..39] + $chop[$sig_length..($chop.Length - 1)]

# Write signature and content to files
Set-Content -Encoding Byte signature.p7 $sig
Set-Content -Encoding Byte content.bin $content
```

Gunakan skrip untuk membongkar file DBX yang ditandatangani.

```
PS C:\Windows\system32> SplitDbxContent.ps1 .\dbx.bin
```

Ini menghasilkan dua file — `signature.p7` dan`content.bin`. Gunakan `content.bin` pada langkah berikutnya.

8. Buat penyimpanan variabel UEFI menggunakan skrip `uefivars.py`.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/content.bin
```

9. Periksa gumpalan biner dan penyimpanan variabel UEFI.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. Anda dapat memperbarui gumpalan dengan meneruskannya ke alat yang sama lagi.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/content.bin
```

Keluaran yang diharapkan

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Gunakan enkripsi dengan dukungan EBS AMIs

AMIs yang didukung oleh snapshot Amazon EBS dapat memanfaatkan enkripsi Amazon EBS. Snapshot data dan volume root dapat dienkripsi dan dilampirkan ke AMI. Anda dapat meluncurkan instans dan menyalin gambar dengan disertai dukungan enkripsi EBS lengkap. Parameter enkripsi untuk operasi ini didukung di semua Wilayah AWS KMS jika tersedia.

Instans EC2 dengan volume EBS terenkripsi diluncurkan dengan cara yang sama seperti instans lainnya. AMIs Selain itu, saat Anda meluncurkan instans dari AMI yang didukung oleh snapshot EBS yang tidak dienkripsi, Anda dapat mengenkripsi beberapa atau semua volume saat peluncuran.

Seperti volume EBS, snapshot di AMIs dapat dienkripsi baik oleh default Anda AWS KMS key, atau ke kunci terkelola pelanggan yang Anda tentukan. Anda harus selalu memiliki izin untuk menggunakan kunci KMS yang dipilih.

AMIs dengan snapshot terenkripsi dapat dibagikan di seluruh akun. AWS Untuk informasi selengkapnya, lihat Memahami penggunaan AMI bersama di Amazon EC2.

Enkripsi dengan topik yang didukung EBS AMIs

- Skenario peluncuran instans
- Skenario penyalinan gambar

Skenario peluncuran instans

Instans Amazon EC2 diluncurkan dari AMIs penggunaan `RunInstances` tindakan dengan parameter yang disediakan melalui pemetaan perangkat blok, baik melalui Konsol Manajemen AWS atau langsung menggunakan Amazon EC2 API atau CLI. Untuk informasi selengkapnya, lihat Blokir pemetaan perangkat untuk volume di instans Amazon EC2. Untuk contoh mengontrol pemetaan blok perangkat dari AWS CLI, lihat Meluncurkan, Membuat Daftar, dan Mengakhiri Instans EC2.

Secara default, tanpa parameter enkripsi yang eksplisit, tindakan `RunInstances` mempertahankan status enkripsi snapshot sumber AMI sambil memulihkan volume EBS darinya. Jika enkripsi secara default diaktifkan, semua volume yang dibuat dari AMI (baik dari snapshot terenkripsi atau tidak terenkripsi) dienkripsi. Jika enkripsi secara default tidak diaktifkan, instance mempertahankan status enkripsi AMI.

Anda juga dapat meluncurkan instans dan sekaligus menerapkan status enkripsi baru ke volume yang dihasilkan dengan menyediakan parameter enkripsi. Sebagai hasil, perilaku berikut akan muncul:

Meluncurkan tanpa parameter enkripsi

- Snapshot yang tidak terenkripsi dipulihkan ke volume yang tidak dienkripsi, kecuali jika enkripsi secara default diaktifkan, dalam hal ini semua volume yang baru dibuat akan dienkripsi.
- Snapshot terenkripsi yang Anda miliki dipulihkan ke volume yang dienkripsi ke kunci KMS yang sama.
- Snapshot terenkripsi yang tidak Anda miliki (misalnya, AMI dibagikan dengan Anda) dikembalikan ke volume yang dienkripsi oleh kunci KMS default AWS akun Anda.

Perilaku default ini dapat ditimpa dengan menyediakan parameter enkripsi. Parameter yang tersedia adalah `Encrypted` dan `KmsKeyId`. Menetapkan hanya Hasil parameter `Encrypted` dalam:

Perilaku peluncuran instans dengan **`Encrypted`** ditetapkan, tetapi tidak ada **`KmsKeyId`** yang ditentukan

- Snapshot yang tidak dienkripsi dipulihkan ke volume EBS yang dienkripsi oleh kunci KMS default akun AWS Anda.
- Snapshot terenkripsi yang Anda miliki dipulihkan ke volume yang dienkripsi ke kunci KMS yang sama. (Dengan kata lain, parameter `Encrypted` tidak memiliki efek.)
- Snapshot terenkripsi yang tidak Anda miliki (yaitu, AMI dibagikan dengan Anda) dikembalikan ke volume yang dienkripsi oleh kunci KMS default AWS akun Anda. (Dengan kata lain, parameter `Encrypted` tidak memiliki efek.)

Mengatur parameter `Encrypted` dan `KmsKeyId` memungkinkan Anda menentukan kunci KMS non-default untuk operasi enkripsi. Perilaku berikut menghasilkan:

Instans dengan **`Encrypted`** dan **`KmsKeyId`** ditetapkan

- Snapshot yang tidak dienkripsi dipulihkan ke volume EBS yang dienkripsi oleh kunci KMS yang ditentukan.
- Snapshot terenkripsi dipulihkan ke volume EBS yang dienkripsi bukan ke kunci KMS awal, melainkan ke kunci KMS yang ditentukan.

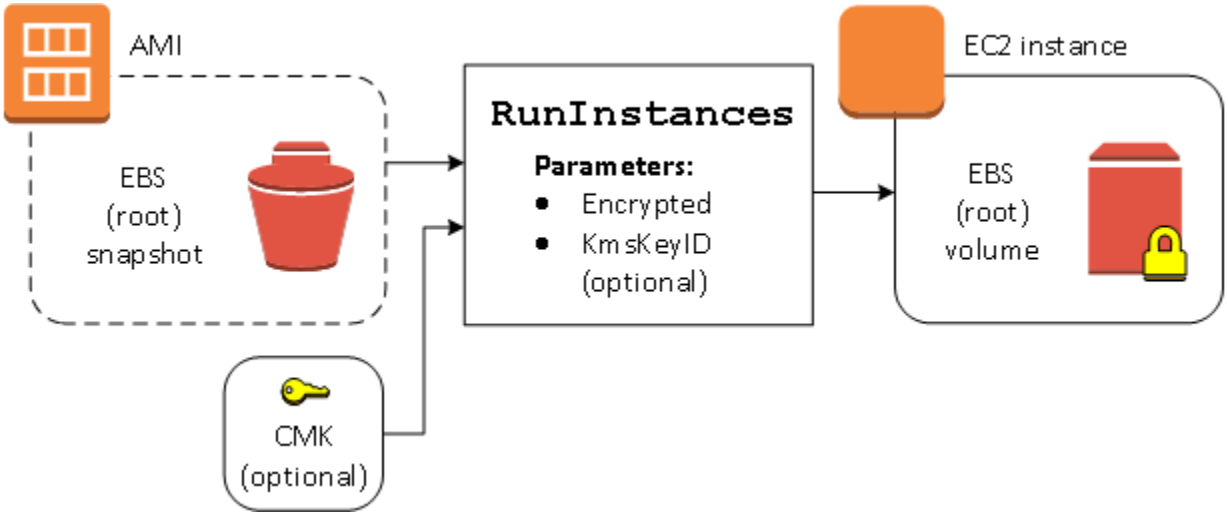
Mengirim `KmsKeyId` tanpa mengatur parameter `Encrypted` akan mengakibatkan kesalahan.

Bagian berikut memberikan contoh peluncuran instance dari AMIs menggunakan parameter enkripsi non-default. Dalam setiap skenario ini, parameter yang diberikan ke tindakan `RunInstances` akan menghasilkan perubahan status enkripsi selama pemulihan volume dari snapshot.

Untuk informasi selengkapnya tentang meluncurkan instans dari AMI, lihat Luncurkan instans Amazon EC2.

Mengenkripsi volume saat peluncuran

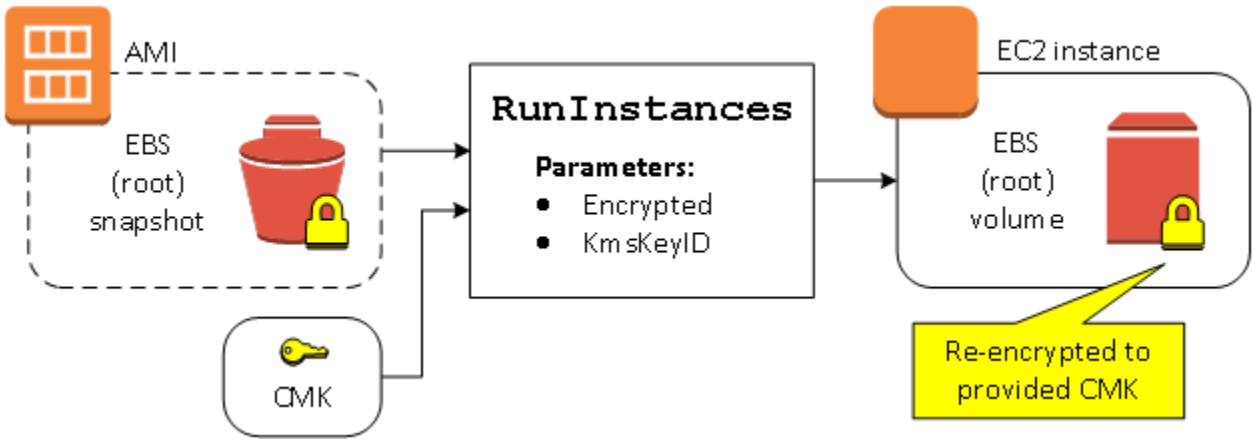
Dalam contoh ini, AMI yang didukung oleh snapshot tidak terenkripsi digunakan untuk meluncurkan instans EC2 dengan volume EBS terenkripsi.



Parameter `Encrypted` saja menyebabkan volume untuk instans ini dienkripsi. Memberikan parameter `KmsKeyId` bersifat opsional. Jika tidak ada ID kunci KMS yang ditentukan, kunci KMS default AWS akun digunakan untuk mengenkripsi volume. Untuk mengenkripsi volume ke kunci KMS berbeda yang Anda miliki, sediakan parameter `KmsKeyId`.

Mengenkripsi ulang volume saat peluncuran

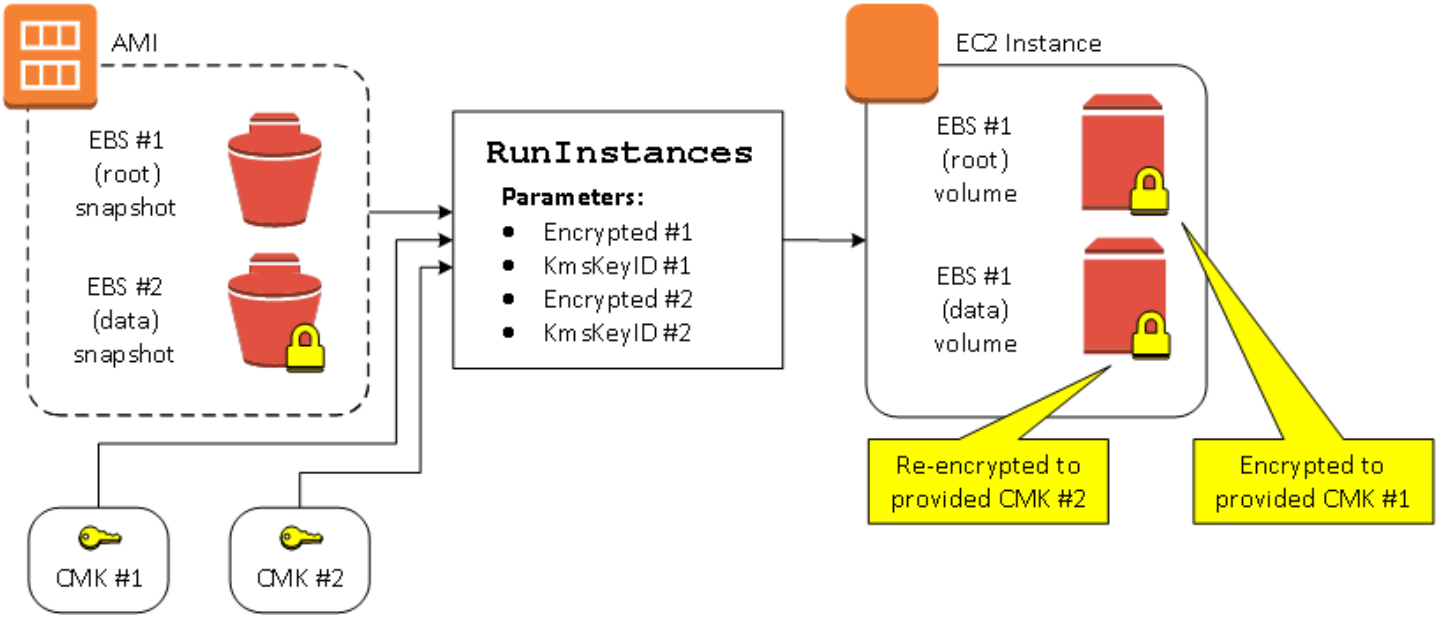
Dalam contoh ini, AMI yang didukung oleh snapshot terenkripsi digunakan untuk meluncurkan instans EC2 dengan volume EBS yang dienkripsi oleh kunci KMS baru.



Jika Anda memiliki AMI dan tidak menyediakan parameter enkripsi, instans yang dihasilkan memiliki volume yang dienkripsi oleh kunci KMS yang sama dengan snapshot. Jika AMI adalah AMI bersama, bukan milik Anda, dan Anda tidak menyediakan parameter enkripsi, volume dienkripsi oleh kunci KMS default Anda. Dengan parameter enkripsi yang disediakan seperti yang ditunjukkan, volume dienkripsi oleh kunci KMS tertentu.

Mengubah status enkripsi beberapa volume saat peluncuran

Dalam contoh yang lebih kompleks ini, AMI yang didukung oleh beberapa snapshot (masing-masing menggunakan status enkripsi tersendiri) digunakan untuk meluncurkan instans EC2 dengan volume yang baru dienkripsi dan volume yang dienkripsi ulang.



Dalam skenario ini, tindakan `RunInstances` diberi parameter enkripsi untuk setiap snapshot sumber. Ketika semua kemungkinan parameter enkripsi ditentukan, instans yang dihasilkan adalah sama terlepas dari apakah AMI merupakan milik Anda.

Skenario penyalinan gambar

Amazon EC2 AMIs disalin menggunakan `CopyImage` tindakan, baik melalui atau langsung menggunakan Amazon EC2 API Konsol Manajemen AWS atau CLI.

Secara default, tanpa parameter enkripsi yang eksplisit, tindakan `CopyImage` mempertahankan status enkripsi snapshot sumber AMI selama penyalinan. Anda juga dapat menyalin AMI dan sekaligus menerapkan status enkripsi baru ke snapshot EBS terkait dengan menyediakan parameter enkripsi. Sebagai hasil, perilaku berikut akan muncul:

Menyalin tanpa parameter enkripsi

- Snapshot yang tidak terenkripsi dipulihkan ke snapshot lain yang tidak terenkripsi, kecuali jika enkripsi secara default diaktifkan, dalam hal ini semua volume yang baru dibuat akan dienkripsi.
- Snapshot terenkripsi yang Anda miliki disalin ke snapshot yang dienkripsi dengan kunci KMS yang sama.
- Snapshot terenkripsi yang tidak Anda miliki (yaitu, AMI dibagikan dengan Anda) disalin ke snapshot yang dienkripsi oleh kunci KMS default akun Anda. AWS

Perilaku default ini dapat ditimpa dengan menyediakan parameter enkripsi. Parameter yang tersedia adalah `Encrypted` dan `KmsKeyId`. Jika hanya menetapkan parameter `Encrypted`, hal berikut terjadi:

Perilaku copy-image dengan **`Encrypted`** diatur, tetapi tidak ada **`KmsKeyId`** yang ditentukan

- Snapshot yang tidak dienkripsi disalin ke snapshot yang dienkripsi oleh kunci KMS default akun AWS .
- Snapshot terenkripsi disalin ke snapshot yang dienkripsi oleh kunci KMS yang sama. (Dengan kata lain, parameter `Encrypted` tidak memiliki efek.)
- Snapshot terenkripsi yang tidak Anda miliki (yaitu, AMI dibagikan dengan Anda) disalin ke volume yang dienkripsi oleh kunci KMS default akun Anda AWS . (Dengan kata lain, parameter `Encrypted` tidak memiliki efek.)

Mengatur parameter `Encrypted` dan `KmsKeyId` memungkinkan Anda menentukan kunci KMS yang dikelola pelanggan untuk operasi enkripsi. Perilaku berikut menghasilkan:

Perilaku copy-image dengan **`Encrypted`** dan **`KmsKeyId`** diatur

- Snapshot yang tidak dienkripsi disalin ke snapshot yang dienkripsi oleh kunci KMS yang ditentukan.
- Snapshot terenkripsi disalin ke snapshot terenkripsi bukan ke kunci KMS awal, melainkan ke kunci KMS yang ditentukan.

Mengirim `KmsKeyId` tanpa turut mengatur parameter `Encrypted` akan mengakibatkan kesalahan.

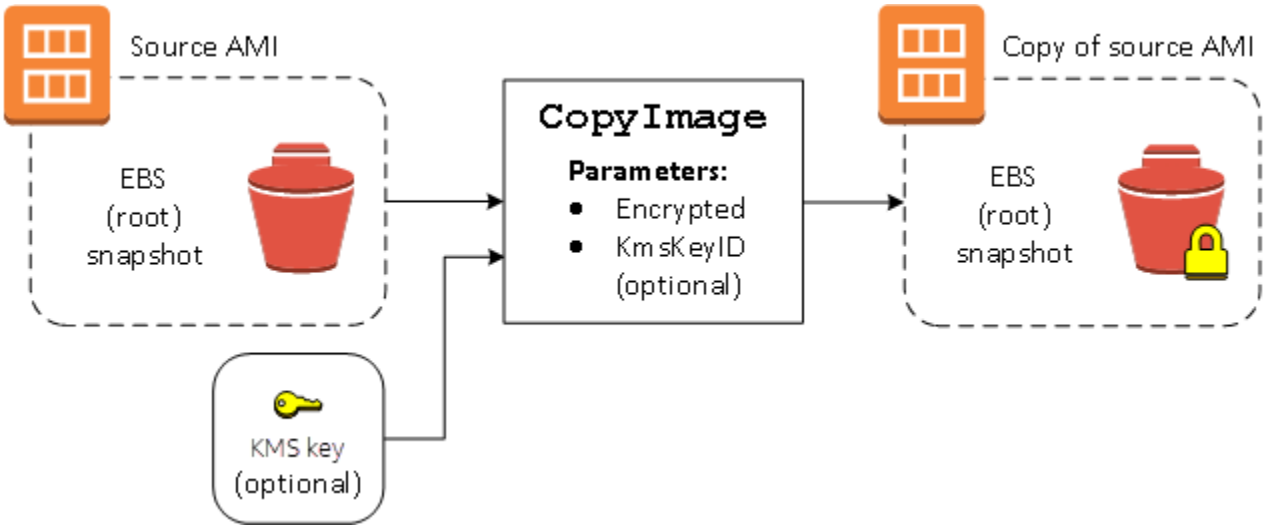
Bagian berikut ini memberikan contoh penyalinan AMI menggunakan parameter enkripsi non-default, yang menghasilkan perubahan status enkripsi.

Untuk petunjuk detail menggunakan konsol, lihat Salin Amazon EC2 AMI.

Mengenkripsikan gambar yang tidak dienkripsi selama penyalinan

Dalam skenario ini, AMI yang didukung oleh snapshot root yang tidak dienkripsi disalin ke AMI dengan snapshot root yang dienkripsi. Tindakan `CopyImage` diinvokasi dengan dua parameter enkripsi, termasuk kunci yang dikelola konsumen. Hasilnya, status enkripsi root snapshot berubah sehingga AMI target didukung oleh snapshot root yang berisi data yang sama dengan snapshot sumber, tetapi dienkripsi menggunakan kunci yang ditentukan. Anda dikenakan biaya penyimpanan untuk snapshot di keduanyaAMIs, serta biaya untuk setiap instance yang Anda luncurkan dari AMI.

> **Note**
>
> Mengaktifkan enkripsi secara default memiliki efek yang sama seperti mengatur `Encrypted` parameter `true` untuk semua snapshot di AMI.



Mengatur parameter `Encrypted` akan mengenkripsi snapshot tunggal untuk instans ini. Jika Anda tidak menentukan parameter `KmsKeyId`, kunci default yang dikelola konsumen akan digunakan untuk mengenkripsi salinan snapshot.

> **Note**
>
> Anda juga dapat menyalin gambar dengan beberapa snapshot dan mengonfigurasi status enkripsi masing-masing gambar secara terpisah.

Memahami penggunaan AMI bersama di Amazon EC2

AMI bersama adalah AMI yang dibuat oleh developer dan disediakan untuk digunakan oleh orang lain. Salah satu cara termudah untuk memulai Amazon EC2 adalah menggunakan AMI bersama yang memiliki komponen yang Anda butuhkan, lalu menambahkan konten kustom. Anda juga dapat membuat AMIs dan membagikannya kepada yang lain.

Anda menggunakan AMI bersama dengan risiko Anda sendiri. Amazon tidak dapat menjamin integritas atau keamanan AMI yang dibagikan oleh pengguna Amazon EC2 lainnya. Oleh karena itu, Anda harus memperlakukan shared AMIs seperti halnya kode asing yang mungkin Anda pertimbangkan untuk diterapkan di pusat data Anda sendiri, dan melakukan uji tuntas yang sesuai. Kami menyarankan Anda mendapatkan AMI dari sumber tepercaya, seperti penyedia yang terverifikasi.

Penyedia AMI terverifikasi

Di konsol Amazon EC2, publik AMIs yang dimiliki oleh Amazon atau mitra Amazon terverifikasi ditandai Penyedia terverifikasi.

Anda juga dapat menggunakan AWS CLI perintah deskripsi-gambar untuk mengidentifikasi publik AMIs yang berasal dari penyedia terverifikasi. Gambar publik yang dimiliki oleh Amazon atau mitra terverifikasi memiliki pemilik alias, yaitu `amazon`aws-backup-vault, atauaws-marketplace. Dalam output CLI, nilai-nilai ini muncul untuk `ImageOwnerAlias`. Pengguna lain tidak dapat membuat alias AMIs. Ini memungkinkan Anda untuk dengan mudah menemukan AMIs dari Amazon atau mitra terverifikasi.

Untuk menjadi penyedia terverifikasi, Anda harus mendaftar sebagai penjual di AWS Marketplace. Setelah terdaftar, Anda dapat mendaftarkan AMI Anda di AWS Marketplace. Untuk informasi selengkapnya, lihat Memulai sebagai penjual dan produk berbasis AMI di Panduan Penjual AWS Marketplace .

Topik AMI bersama

- Temukan AMI bersama untuk digunakan untuk instans Amazon EC2
- Bersiaplah untuk menggunakan shared AMIs untuk Linux
- Kontrol penemuan dan penggunaan AMI di Amazon EC2 dengan Diizinkan AMIs
- Jadikan AMI Anda tersedia untuk umum untuk digunakan di Amazon EC2
- Memahami memblokir akses publik untuk AMIs
- Bagikan AMI dengan organisasi dan unit organisasi
- Bagikan AMI dengan AWS akun tertentu
- Batalkan memiliki AMI yang dibagikan dengan Anda Akun AWS
- Rekomendasi untuk membuat Linux bersama AMIs

Jika Anda mencari informasi tentang topik lain

- Untuk informasi tentang membuat AMI, lihat the section called “Buat AMI yang didukung Amazon S3” atauthe section called “Membuat AMI”.
- Untuk informasi tentang membangun, mengirim, dan memelihara aplikasi Anda di AWS Marketplace, lihat Dokumentasi AWS Marketplace.

Temukan AMI bersama untuk digunakan untuk instans Amazon EC2

Anda dapat menggunakan konsol Amazon EC2 atau baris perintah untuk menemukan AMI bersama publik atau pribadi untuk digunakan dengan instans Amazon EC2 Anda.

AMIs adalah sumber daya regional. Saat Anda mencari AMI bersama (publik atau privat), Anda harus mencarinya dari Wilayah di mana AMI tersebut dibagikan. Agar AMI tersedia di Wilayah yang berbeda, salin AMI ke Wilayah, lalu bagikan. Untuk informasi selengkapnya, lihat Salin Amazon EC2 AMI.

Console

Konsol menyediakan bidang filter AMI. Anda juga dapat membuat cakupan pencarian menggunakan filter yang disediakan di kolom Pencarian.

Untuk menemukan bersama atau AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Di filter pertama, pilih salah satu opsi berikut:
   - Gambar pribadi - Daftar semua AMIs yang dibagikan dengan Anda.
   - Gambar publik - Daftar semua publik AMIs.
4. (Opsional) Untuk hanya menampilkan gambar publik dari Amazon, pilih bidang Pencarian dan kemudian, dari opsi menu, pilih alias Pemilik, lalu =, dan kemudian amazon.
5. (Opsional) Tambahkan filter untuk cakupan pencarian Anda AMIs yang memenuhi persyaratan Anda.

Untuk menemukan AMI publik bersama dari penyedia terverifikasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Katalog AMI.
3. Pilih Komunitas AMIs.
4. Di panel Perbaiki hasil, pilih Penyedia terverifikasi. Label penyedia terverifikasi menunjukkan bahwa itu AMIs berasal dari Amazon atau mitra terverifikasi.

AWS CLI

Gunakan perintah deskripsi-gambar untuk daftar. AMIs Anda dapat membuat cakupan daftar ke jenis AMIs yang Anda minati, seperti yang ditunjukkan pada contoh berikut.

Untuk daftar semua publik AMIs

Perintah berikut mencantumkan semua publik AMIs, termasuk publik AMIs yang Anda miliki.

```
aws ec2 describe-images --executable-users all
```

Untuk daftar AMIs dengan izin peluncuran eksplisit

Perintah berikut mencantumkan izin peluncuran eksplisit yang Anda miliki. AMIs Daftar ini tidak termasuk AMIs yang Anda miliki.

```
aws ec2 describe-images --executable-users self
```

Untuk daftar yang AMIs dimiliki oleh penyedia terverifikasi

Perintah berikut mencantumkan yang AMIs dimiliki oleh penyedia terverifikasi. Publik yang AMIs dimiliki oleh penyedia terverifikasi (baik Amazon atau mitra terverifikasi) memiliki pemilik alias, yang muncul sebagai `amazonaws-backup-vault`,, atau `aws-marketplace` di bidang akun. Ini membantu Anda menemukan dengan mudah AMIs dari penyedia terverifikasi. Pengguna lain tidak dapat membuat alias AMIs.

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Untuk daftar AMIs yang dimiliki oleh akun

Perintah berikut mencantumkan yang AMIs dimiliki oleh yang ditentukan Akun AWS.

```
aws ec2 describe-images --owners 123456789012
```

Untuk cakupan AMIs menggunakan filter

Untuk mengurangi jumlah yang ditampilkan AMIs, gunakan filter untuk mencantumkan hanya jenis AMIs yang menarik bagi Anda. Misalnya, gunakan filter berikut untuk menampilkan hanya didukung EBS AMIs.

```
--filters "Name=root-device-type,Values=ebs"
```

PowerShell

Gunakan Get-EC2Imagecmdlet (Alat untuk Windows PowerShell) untuk daftar. AMIs Anda dapat membuat cakupan daftar ke jenis AMIs yang Anda minati, seperti yang ditunjukkan pada contoh berikut.

Untuk daftar semua publik AMIs

Perintah berikut mencantumkan semua publik AMIs, termasuk publik AMIs yang Anda miliki.

```
Get-EC2Image -ExecutableUser all
```

Untuk daftar AMIs dengan izin peluncuran eksplisit

Perintah berikut mencantumkan izin peluncuran eksplisit yang Anda miliki. AMIs Daftar ini tidak termasuk AMIs yang Anda miliki.

```
Get-EC2Image -ExecutableUser self
```

Untuk daftar yang AMIs dimiliki oleh penyedia terverifikasi

Perintah berikut mencantumkan yang AMIs dimiliki oleh penyedia terverifikasi. Publik yang AMIs dimiliki oleh penyedia terverifikasi (baik Amazon atau mitra terverifikasi) memiliki pemilik alias, yang muncul sebagai `amazon`aws-backup-vault,, atau `aws-marketplace` di bidang akun. Ini membantu Anda menemukan dengan mudah AMIs dari penyedia terverifikasi. Pengguna lain tidak dapat membuat alias AMIs.

```
Get-EC2Image -Owner amazon aws-marketplace
```

Untuk daftar AMIs yang dimiliki oleh akun

Perintah berikut mencantumkan yang AMIs dimiliki oleh yang ditentukan Akun AWS.

```
Get-EC2Image -Owner 123456789012
```

Untuk cakupan AMIs menggunakan filter

Untuk mengurangi jumlah yang ditampilkan AMIs, gunakan filter untuk mencantumkan hanya jenis AMIs yang menarik bagi Anda. Misalnya, gunakan filter berikut untuk menampilkan hanya didukung EBS AMIs.

```
-Filter @{Name="root-device-type"; Values="ebs"}
```

Bersiaplah untuk menggunakan shared AMIs untuk Linux

Sebelum Anda menggunakan AMI bersama untuk Linux, lakukan langkah-langkah berikut untuk mengonfirmasi bahwa tidak ada kredensil pra-instal yang memungkinkan akses yang tidak diinginkan ke instans Anda oleh pihak ketiga dan tidak ada pencatatan jarak jauh yang telah dikonfigurasi sebelumnya yang dapat mengirimkan data sensitif ke pihak ketiga. Periksa dokumentasi untuk distribusi Linux yang digunakan oleh AMI untuk informasi tentang meningkatkan keamanan sistem.

Untuk memastikan Anda tidak kehilangan akses ke instans Anda tanpa sengaja, kami sarankan Anda memulai dua sesi SSH dan membuka sesi kedua hingga Anda menghapus kredensial yang tidak Anda kenali dan mengonfirmasi bahwa Anda masih dapat masuk ke aplikasi menggunakan SSH.

1. Mengidentifikasi dan menonaktifkan kunci SSH publik yang tidak sah. Satu-satunya kunci dalam file harus menjadi kunci yang Anda gunakan untuk meluncurkan AMI. Perintah berikut mencari file `authorized_keys`:

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. Menonaktifkan autentikasi berbasis kata sandi untuk pengguna root. Buka file `sshd_config` dan ubah baris `PermitRootLogin` sebagai berikut:

   ```
   PermitRootLogin without-password
   ```

   Atau, Anda dapat menonaktifkan kemampuan untuk masuk ke instans sebagai pengguna root:

   ```
   PermitRootLogin No
   ```

   Memulai ulang layanan sshd.

3. Periksa apakah ada pengguna lain yang dapat masuk ke instans Anda. Pengguna dengan hak istimewa superuser sangat berbahaya. Hapus atau kunci kata sandi akun yang tidak dikenal.

4. Periksa port terbuka yang tidak Anda gunakan dan layanan jaringan yang mendengarkan koneksi masuk.
5. Untuk mencegah logging jarak jauh terkonfigurasi, Anda harus menghapus file konfigurasi yang ada dan memulai ulang layanan `rsyslog`. Sebagai contoh:

```
[ec2-user ~]$ sudo rm /etc/rsyslog.conf
[ec2-user ~]$ sudo service rsyslog restart
```

6. Pastikan bahwa semua pekerjaan cron sah.

Jika Anda menemukan AMI publik yang Anda rasa menimbulkan risiko keamanan, kontak tim keamanan AWS . Untuk informasi selengkapnya, lihat Pusat Keamanan AWS.

Kontrol penemuan dan penggunaan AMI di Amazon EC2 dengan Diizinkan AMIs

Untuk mengontrol penemuan dan penggunaan Amazon Machine Images (AMIs) oleh pengguna di Anda Akun AWS, Anda dapat menggunakan AMIs fitur Diizinkan. Anda menentukan kriteria yang AMIs harus dipenuhi agar terlihat dan tersedia dalam akun Anda. Ketika kriteria diaktifkan, pengguna yang meluncurkan instance hanya akan melihat dan memiliki akses ke AMIs yang sesuai dengan kriteria yang ditentukan. Misalnya, Anda dapat menentukan daftar penyedia AMI tepercaya sebagai kriteria, dan hanya AMIs dari penyedia ini yang akan terlihat dan tersedia untuk digunakan.

Sebelum mengaktifkan AMIs pengaturan Diizinkan, Anda dapat mengaktifkan mode audit untuk melihat pratinjau yang AMIs akan atau tidak akan terlihat dan tersedia untuk digunakan. Ini memungkinkan Anda menyempurnakan kriteria yang diperlukan untuk memastikan bahwa hanya yang dimaksudkan AMIs yang terlihat dan tersedia bagi pengguna di akun Anda. Selain itu, gunakan describe-instance-image-metadataperintah untuk menemukan instance yang diluncurkan dengan AMIs yang tidak memenuhi kriteria yang ditentukan. Informasi ini dapat memandu keputusan Anda untuk memperbarui konfigurasi peluncuran agar sesuai dengan penggunaan AMIs (misalnya, menentukan AMI yang berbeda dalam templat peluncuran) atau menyesuaikan kriteria Anda untuk mengizinkannya. AMIs

Anda menentukan AMIs pengaturan Diizinkan di tingkat akun, baik secara langsung di akun atau dengan menggunakan kebijakan deklaratif. Pengaturan ini harus dikonfigurasi di setiap AWS Region tempat Anda ingin mengontrol penggunaan AMI. Menggunakan kebijakan deklaratif memungkinkan Anda menerapkan pengaturan di beberapa Wilayah secara bersamaan, serta di beberapa akun secara bersamaan. Saat kebijakan deklaratif sedang digunakan, Anda tidak dapat mengubah

pengaturan secara langsung di dalam akun. Topik ini menjelaskan cara mengonfigurasi pengaturan secara langsung di dalam akun. Untuk informasi tentang penggunaan kebijakan deklaratif, lihat Kebijakan deklaratif di AWS Organizations Panduan Pengguna.

> **Note**
>
> AMIs Fitur yang Diizinkan hanya mengontrol penemuan dan penggunaan publik AMIs atau AMIs dibagikan dengan akun Anda. Itu tidak membatasi yang AMIs dimiliki oleh akun Anda. Terlepas dari kriteria yang Anda tetapkan, yang AMIs dibuat oleh akun Anda selalu dapat ditemukan dan dapat digunakan oleh pengguna di akun Anda.

Manfaat utama dari Diizinkan AMIs

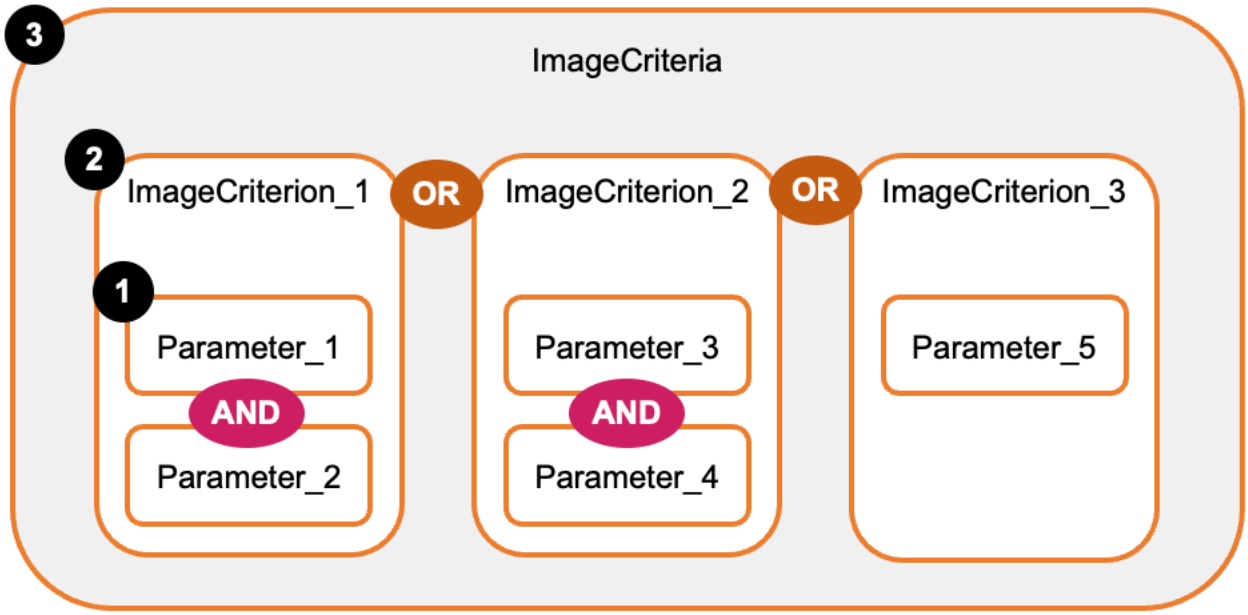
- Kepatuhan dan keamanan: Pengguna hanya dapat menemukan dan menggunakan AMIs yang memenuhi kriteria yang ditentukan, sehingga mengurangi risiko penggunaan AMI yang tidak sesuai.
- Manajemen yang efisien: Dengan mengurangi jumlah yang diizinkan AMIs, mengelola yang tersisa menjadi lebih mudah dan lebih efisien.
- Implementasi tingkat akun terpusat: Konfigurasikan AMIs pengaturan yang Diizinkan di tingkat akun, baik secara langsung di dalam akun atau melalui kebijakan deklaratif. Ini memberikan cara terpusat dan efisien untuk mengontrol penggunaan AMI di seluruh akun.

Daftar Isi

- Cara AMIs kerja yang Diizinkan
- Praktik terbaik untuk menerapkan Diizinkan AMIs
- Izin IAM yang diperlukan
- Mengelola pengaturan untuk Diizinkan AMIs

Cara AMIs kerja yang Diizinkan

Untuk mengontrol mana yang AMIs dapat ditemukan dan digunakan di akun Anda, Anda menentukan serangkaian kriteria yang digunakan untuk mengevaluasi akun Anda AMIs. Kriteria terdiri dari satu atau lebih `ImageCriterion` seperti yang ditunjukkan pada diagram berikut. Penjelasan mengikuti diagram.



Konfigurasi memiliki tiga level:

- 1 — Nilai parameter
  - Parameter multi-nilai:
    - `ImageProviders`
    - `ImageNames`
    - `MarketplaceProductCodes`

      AMI dapat mencocokkan nilai apa pun dalam parameter yang akan diizinkan.

      Contoh: `ImageProviders` = `amazon` ATAU akun `111122223333` ATAU akun `444455556666` (Logika evaluasi untuk nilai parameter tidak ditampilkan dalam diagram.)
  - Parameter nilai tunggal:
    - `CreationDateCondition`
    - `DeprecationTimeCondition`
- 2 — `ImageCriterion`
  - Kelompokkan beberapa parameter dengan logika AND.
  - AMI harus cocok dengan semua parameter dalam a `ImageCriterion` untuk diizinkan.
  - Contoh: `ImageProviders` = `amazon` AND `CreationDateCondition` = 300 hari atau kurang
- 3 — `ImageCriteria`
  - Kelompokkan beberapa `ImageCriterion` dengan logika OR.

- AMI dapat mencocokkan *ImageCriterion*apa pun yang diizinkan.
- Membentuk konfigurasi lengkap yang AMIs dievaluasi.

Topik

- AMIs Parameter yang diizinkan
- AMIs Konfigurasi yang diizinkan
- Bagaimana kriteria dievaluasi
- Batas
- AMIs Operasi yang diizinkan

AMIs Parameter yang diizinkan

Parameter berikut dapat dikonfigurasi untuk membuat`ImageCriterion`:

`ImageProviders`

Penyedia AMI AMIs yang diizinkan.

Nilai yang valid adalah alias yang didefinisikan oleh AWS, dan Akun AWS IDs, sebagai berikut:

- `amazon`— Alias yang mengidentifikasi AMIs dibuat oleh Amazon atau penyedia terverifikasi
- `aws-marketplace`— Alias yang mengidentifikasi AMIs dibuat oleh penyedia terverifikasi di AWS Marketplace
- `aws-backup-vault`— Alias yang mengidentifikasi cadangan yang berada di akun AMIs brankas Backup yang memiliki celah udara secara logis. AWS Jika Anda menggunakan fitur AWS Backup air-gapped vault secara logis, pastikan alias ini disertakan sebagai penyedia AMI.
- Akun AWS IDs — Satu atau lebih 12 digit Akun AWS IDs
- `none`— Menunjukkan bahwa hanya AMIs dibuat oleh akun Anda yang dapat ditemukan dan digunakan. Publik atau dibagikan tidak AMIs dapat ditemukan dan digunakan. Ketika ditentukan, tidak ada kriteria lain yang dapat ditentukan.

`ImageNames`

Nama-nama yang diizinkan AMIs, menggunakan kecocokan persis atau wildcard (`?`atau`*`).

`MarketplaceProductCodes`

Kode AWS Marketplace produk untuk diizinkan AMIs.

`CreationDateCondition`

Usia maksimum untuk diizinkan AMIs.

`DeprecationTimeCondition`

Periode maksimum sejak penghentian untuk diizinkan. AMIs

Untuk nilai dan batasan yang valid untuk setiap kriteria, lihat di Referensi API ImageCriterionRequestAmazon EC2.

AMIs Konfigurasi yang diizinkan

Konfigurasi inti untuk Diizinkan AMIs adalah `ImageCriteria` konfigurasi yang mendefinisikan kriteria untuk diizinkan AMIs. Struktur JSON berikut menunjukkan parameter yang dapat ditentukan:

```
{
    "State": "enabled" | "disabled" | "audit-mode",
    "ImageCriteria" : [
        {
            "ImageProviders": ["string",...],
            "MarketplaceProductCodes": ["string",...],
            "ImageNames":["string",...],
            "CreationDateCondition" : {
                "MaximumDaysSinceCreated": integer
            },
            "DeprecationTimeCondition" : {
                "MaximumDaysSinceDeprecated": integer
            }
         },
         ...
}
```

ImageCriteria contoh

`ImageCriteria`Contoh berikut mengkonfigurasi empat`ImageCriterion`. AMI diperbolehkan jika cocok dengan salah satu dari ini`ImageCriterion`. Untuk informasi tentang bagaimana kriteria dievaluasi, lihatBagaimana kriteria dievaluasi.

```
{
    "ImageCriteria": [
        // ImageCriterion 1: Allow AWS Marketplace AMIs with product code
 "abcdefg1234567890"
```

```
        {
            "MarketplaceProductCodes": [
                "abcdefg1234567890"
            ]
        },
        // ImageCriterion 2: Allow AMIs from providers whose accounts are
        // "123456789012" OR "123456789013" AND AMI age is less than 300 days
        {
            "ImageProviders": [
                "123456789012",
                "123456789013"
            ],
            "CreationDateCondition": {
                "MaximumDaysSinceCreated": 300
            }
        },
        // ImageCriterion 3: Allow AMIs from provider whose account is "123456789014"
        // AND with names following the pattern "golden-ami-*"
        {
            "ImageProviders": [
                "123456789014"
            ],
            "ImageNames": [
                "golden-ami-*"
            ]
        },
        // ImageCriterion 4: Allow AMIs from Amazon or verified providers
        // AND which aren't deprecated
        {
            "ImageProviders": [
                "amazon"
            ],
            "DeprecationTimeCondition": {
                "MaximumDaysSinceDeprecated": 0
            }
        }
    ]
}
```

Bagaimana kriteria dievaluasi

Tabel berikut menjelaskan aturan evaluasi yang menentukan apakah AMI diizinkan, yang menunjukkan bagaimana OR operator AND atau diterapkan di setiap tingkat:

Tingkat evaluasi	Operator	Persyaratan untuk menjadi AMI yang Diizinkan
Nilai parameter untuk`ImageProviders` ,`ImageNames` , dan `MarketplaceProductCodes`	`OR`	AMI harus mencocokkan setidaknya satu nilai di setiap daftar parameter
`ImageCriterion`	`AND`	AMI harus mencocokkan semua parameter di masing-masing `ImageCriterion`
`ImageCriteria`	`OR`	AMI harus cocok dengan salah satu `ImageCriterion`

Dengan menggunakan aturan evaluasi sebelumnya, mari kita lihat bagaimana menerapkannya pada: ImageCriteria contoh

- `ImageCriterion1`: Memungkinkan AMIs yang memiliki kode AWS Marketplace produk `abcdefg1234567890`

  `OR`
- `ImageCriterion2`: Memungkinkan AMIs yang memenuhi kedua kriteria ini:
  - Dimiliki oleh salah satu akun `123456789012` `OR` `123456789013`
    - `AND`
  - Dibuat dalam 300 hari terakhir

  `OR`
- `ImageCriterion3`: Memungkinkan AMIs yang memenuhi kedua kriteria ini:
  - Dimiliki oleh akun `123456789014`
    - `AND`
  - Dinamakan dengan pola `golden-ami-*`

  `OR`

- `ImageCriterion`4: Memungkinkan AMIs yang memenuhi kedua kriteria ini:
  - Diterbitkan oleh Amazon atau penyedia terverifikasi (ditentukan oleh `amazon` alias)
    - `AND`
  - Tidak usang (hari maksimum sejak penghentian) `0`

Batas

`ImageCriteria`Dapat mencakup hingga:

- 10 `ImageCriterion`

Masing-masing `ImageCriterion` dapat mencakup hingga:

- 200 nilai untuk `ImageProviders`
- 50 nilai untuk `ImageNames`
- 50 nilai untuk `MarketplaceProductCodes`

Contoh batas

Menggunakan yang sebelumnyaImageCriteria contoh:

- Ada 4`ImageCriterion`. Hingga 6 lagi dapat ditambahkan ke permintaan untuk mencapai batas 10.
- Yang pertama`ImageCriterion`, ada 1 nilai untuk`MarketplaceProductCodes`. Hingga 49 lebih dapat ditambahkan ke ini `ImageCriterion` untuk mencapai batas 50.
- Yang kedua`ImageCriterion`, ada 2 nilai untuk`ImageProviders`. Hingga 198 lebih dapat ditambahkan ke ini `ImageCriterion` untuk mencapai batas 200.
- Yang ketiga`ImageCriterion`, ada 1 nilai untuk`ImageNames`. Hingga 49 lebih dapat ditambahkan ke ini `ImageCriterion` untuk mencapai batas 50.

AMIs Operasi yang diizinkan

AMIs Fitur Diizinkan memiliki tiga status operasional untuk mengelola kriteria gambar: mode diaktifkan, dinonaktifkan, dan audit. Ini memungkinkan Anda untuk mengaktifkan atau menonaktifkan kriteria gambar, atau meninjaunya sesuai kebutuhan.

Diaktifkan

Saat Diizinkan AMIs diaktifkan:

- Itu `ImageCriteria` diterapkan.
- Hanya AMI yang diizinkan yang dapat ditemukan di konsol EC2 dan dengan APIs itu menggunakan gambar (misalnya, yang menggambarkan, menyalin, menyimpan, atau melakukan tindakan lain yang menggunakan gambar).
- Instans hanya dapat diluncurkan menggunakan diizinkan AMIs.

Nonaktif

Ketika Diizinkan AMIs dinonaktifkan:

- Itu `ImageCriteria` tidak diterapkan.
- Tidak ada batasan yang ditempatkan pada kemampuan penemuan atau penggunaan AMI.

Modus audit

Dalam mode audit:

- `ImageCriteria`Ini diterapkan, tetapi tidak ada batasan yang ditempatkan pada kemampuan penemuan atau penggunaan AMI.
- Di konsol EC2, untuk setiap AMI, bidang gambar yang Diizinkan menampilkan Ya atau Tidak untuk menunjukkan apakah AMI akan dapat ditemukan dan tersedia bagi pengguna di akun saat Diizinkan AMIs diaktifkan.
- Di baris perintah, respons untuk `describe-image` operasi mencakup `"ImageAllowed": true` atau `"ImageAllowed": false` untuk menunjukkan apakah AMI akan dapat ditemukan dan tersedia untuk pengguna di akun saat Diizinkan AMIs diaktifkan.
- Di konsol EC2, Katalog AMI menampilkan Tidak diizinkan di samping AMIs yang tidak dapat ditemukan atau tersedia bagi pengguna di akun saat Diizinkan AMIs diaktifkan.

Praktik terbaik untuk menerapkan Diizinkan AMIs

Saat menerapkan AMIs Allowed, pertimbangkan praktik terbaik ini untuk memastikan transisi yang lancar dan meminimalkan potensi gangguan pada AWS lingkungan Anda.

1. Aktifkan mode audit

   Mulailah dengan mengaktifkan Diizinkan AMIs dalam mode audit. Status ini memungkinkan Anda untuk melihat mana yang AMIs akan terpengaruh oleh kriteria Anda tanpa benar-benar membatasi akses, memberikan periode evaluasi bebas risiko.

2. Tetapkan AMIs kriteria yang Diizinkan

   Tetapkan dengan cermat penyedia AMI mana yang selaras dengan kebijakan keamanan, persyaratan kepatuhan, dan kebutuhan operasional organisasi Anda.

   > **Note**
   >
   > Saat menggunakan layanan AWS terkelola, seperti Amazon ECS, Amazon EKS, atau Instans Terkelola AWS Lambda, sebaiknya tentukan alias yang akan diizinkan dibuat `amazon` oleh. AMIs AWS Layanan ini bergantung pada Amazon yang diterbitkan AMIs untuk meluncurkan instance.
   > Berhati-hatilah saat menetapkan `CreationDateCondition` batasan untuk apa pun AMIs. Menyetel kondisi tanggal yang terlalu ketat (misalnya, AMIs harus berusia kurang dari 5 hari) dapat menyebabkan kegagalan peluncuran instance jika AMIs, baik dari AWS atau penyedia lain, tidak diperbarui dalam jangka waktu yang Anda tentukan.
   > Kami merekomendasikan pemasangan `ImageNames` dengan `ImageProviders` untuk kontrol dan spesifisitas yang lebih baik. Menggunakan `ImageNames` sendiri mungkin tidak secara unik mengidentifikasi AMI.

3. Periksa dampak pada proses bisnis yang diharapkan

   Anda dapat menggunakan konsol atau CLI untuk mengidentifikasi instance apa pun yang diluncurkan dengan yang tidak memenuhi kriteria AMIs yang ditentukan. Informasi ini dapat memandu keputusan Anda untuk memperbarui konfigurasi peluncuran agar sesuai dengan penggunaan AMIs (misalnya, menentukan AMI yang berbeda dalam templat peluncuran) atau menyesuaikan kriteria Anda untuk mengizinkannya. AMIs

   Konsol: Gunakan AWS Config aturan ec2- instance-launched-with-allowed -ami untuk memeriksa apakah instance yang sedang berjalan atau dihentikan diluncurkan dengan AMIs yang memenuhi kriteria Diizinkan Anda. AMIs Aturannya adalah NON_COMPLIANT jika AMI tidak memenuhi AMIs kriteria yang Diizinkan, dan COMPLIANT jika memang demikian. Aturan hanya beroperasi jika AMIs setelan Diizinkan disetel ke mode aktif atau audit.

CLI: Jalankan describe-instance-image-metadataperintah dan filter respons untuk mengidentifikasi instance apa pun yang diluncurkan dengan AMIs yang tidak memenuhi kriteria yang ditentukan.

Untuk instruksi konsol dan CLI, lihat. Temukan instance yang diluncurkan dari AMIs yang tidak diizinkan

4. Aktifkan Diizinkan AMIs

   Setelah Anda mengonfirmasi bahwa kriteria tidak akan mempengaruhi proses bisnis yang diharapkan, aktifkan Diizinkan AMIs.

5. Monitor peluncuran instance

   Terus memantau peluncuran instans dari AMIs seluruh aplikasi dan layanan AWS terkelola yang Anda gunakan, seperti Amazon EMR, Amazon ECR, Amazon EKS, dan. AWS Elastic Beanstalk Periksa masalah yang tidak terduga dan lakukan penyesuaian yang diperlukan pada AMIs kriteria yang Diizinkan.

6. Pilot baru AMIs

   Untuk menguji pihak ketiga AMIs yang tidak mematuhi AMIs pengaturan Diizinkan Anda saat ini, AWS rekomendasikan pendekatan berikut:

   - Gunakan yang terpisah Akun AWS: Buat akun tanpa akses ke sumber daya penting bisnis Anda. Pastikan AMIs pengaturan Diizinkan tidak diaktifkan di akun ini, atau yang ingin AMIs Anda uji diizinkan secara eksplisit, sehingga Anda dapat mengujinya.
   - Uji di tempat lain AWS Region: Gunakan Wilayah tempat pihak ketiga AMIs tersedia, tetapi di mana Anda belum mengaktifkan AMIs pengaturan yang Diizinkan.

   Pendekatan ini membantu memastikan sumber daya penting bisnis Anda tetap aman saat Anda menguji yang baru. AMIs

Izin IAM yang diperlukan

Untuk menggunakan AMIs fitur Diizinkan, Anda memerlukan izin IAM berikut:

- `GetAllowedImagesSettings`
- `EnableAllowedImagesSettings`
- `DisableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`

Mengelola pengaturan untuk Diizinkan AMIs

Anda dapat mengelola pengaturan untuk Diizinkan AMIs. Pengaturan ini adalah per Wilayah per akun.

Tugas

- Aktifkan Diizinkan AMIs
- Tetapkan AMIs kriteria yang Diizinkan
- Nonaktifkan Diizinkan AMIs
- Dapatkan AMIs kriteria yang Diizinkan
- Temukan AMIs yang diizinkan
- Temukan instance yang diluncurkan dari AMIs yang tidak diizinkan

Aktifkan Diizinkan AMIs

Anda dapat mengaktifkan Diizinkan AMIs dan tentukan AMIs Kriteria yang diizinkan. Kami menyarankan Anda memulai dalam mode audit, yang menunjukkan kepada Anda mana yang AMIs akan terpengaruh oleh kriteria tanpa benar-benar membatasi akses.

Console

Untuk mengaktifkan Diizinkan AMIs

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor.
3. Pada kartu Atribut akun, di bawah Pengaturan, pilih Diizinkan AMIs.
4. Pada AMIs tab Diizinkan, pilih Kelola.
5. Untuk AMIs Pengaturan yang Diizinkan, pilih Mode audit atau Diaktifkan. Kami menyarankan Anda memulai dalam mode audit, menguji kriteria, dan kemudian kembali ke langkah ini untuk mengaktifkan Diizinkan AMIs.
6. (Opsional) Untuk kriteria AMI, masukkan kriteria dalam format JSON.
7. Pilih Perbarui.

AWS CLI

Untuk mengaktifkan Diizinkan AMIs

Gunakan perintah enable-allowed-images-settings.

```
aws ec2 enable-allowed-images-settings --allowed-images-settings-state enabled
```

Untuk mengaktifkan mode audit sebagai gantinya, tentukan `audit-mode` sebagai gantinya`enabled`.

```
aws ec2 enable-allowed-images-settings --allowed-images-settings-state audit-mode
```

PowerShell

Untuk mengaktifkan Diizinkan AMIs

Gunakan Enable-EC2AllowedImagesSettingcmdlet.

```
Enable-EC2AllowedImagesSetting -AllowedImagesSettingsState enabled
```

Untuk mengaktifkan mode audit sebagai gantinya, tentukan `audit-mode` sebagai gantinya`enabled`.

```
Enable-EC2AllowedImagesSetting -AllowedImagesSettingsState audit-mode
```

Tetapkan AMIs kriteria yang Diizinkan

Setelah mengaktifkan Diizinkan AMIs, Anda dapat mengatur atau mengganti AMIs kriteria yang Diizinkan.

Untuk konfigurasi yang benar dan nilai yang valid, lihat AMIs Konfigurasi yang diizinkan danAMIs Parameter yang diizinkan.

Console

Untuk menetapkan AMIs kriteria yang Diizinkan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor.
3. Pada kartu Atribut akun, di bawah Pengaturan, pilih Diizinkan AMIs.
4. Pada AMIs tab Diizinkan, pilih Kelola.

5. Untuk kriteria AMI, masukkan kriteria dalam format JSON.
6. Pilih Perbarui.

AWS CLI

Untuk menetapkan AMIs kriteria yang Diizinkan

Gunakan allowed-images-settings perintah replace-image-criteria-in- dan tentukan file JSON yang berisi AMIs kriteria Diizinkan.

```
aws ec2 replace-image-criteria-in-allowed-images-settings --cli-input-json
 file://file_name.json
```

PowerShell

Untuk menetapkan AMIs kriteria yang Diizinkan

Gunakan Set-EC2ImageCriteriaInAllowedImagesSettingcmdlet dan tentukan file JSON yang berisi kriteria Diizinkan. AMIs

```
$imageCriteria = Get-Content -Path .\file_name.json | ConvertFrom-Json
Set-EC2ImageCriteriaInAllowedImagesSetting -ImageCriterion $imageCriteria
```

Nonaktifkan Diizinkan AMIs

Anda dapat menonaktifkan Diizinkan AMIs sebagai berikut.

Console

Untuk menonaktifkan Diizinkan AMIs

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor.
3. Pada kartu Atribut akun, di bawah Pengaturan, pilih Diizinkan AMIs.
4. Pada AMIs tab Diizinkan, pilih Kelola.
5. Untuk AMIs Pengaturan yang Diizinkan, pilih Dinonaktifkan.
6. Pilih Perbarui.

AWS CLI

Untuk menonaktifkan Diizinkan AMIs

Gunakan perintah disable-allowed-images-settings.

```
aws ec2 disable-allowed-images-settings
```

PowerShell

Untuk menonaktifkan Diizinkan AMIs

Gunakan Disable-EC2AllowedImagesSettingcmdlet.

```
Disable-EC2AllowedImagesSetting
```

Dapatkan AMIs kriteria yang Diizinkan

Anda bisa mendapatkan status saat ini dari AMIs pengaturan Diizinkan dan AMIs kriteria Diizinkan.

Console

Untuk mendapatkan AMIs status dan kriteria yang Diizinkan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor.
3. Pada kartu Atribut akun, di bawah Pengaturan, pilih Diizinkan AMIs.
4. Pada AMIs tab Diizinkan, AMIs Pengaturan yang diizinkan diatur ke mode Diaktifkan, Dinonaktifkan, atau Audit.
5. Jika status Diizinkan AMIs adalah mode Diaktifkan atau Audit, kriteria AMI, menampilkan kriteria AMI dalam format JSON.

AWS CLI

Untuk mendapatkan AMIs status dan kriteria yang Diizinkan

Gunakan perintah get-allowed-images-settings.

```
aws ec2 get-allowed-images-settings
```

Dalam contoh output berikut, keadaan `audit-mode` dan kriteria gambar ditetapkan dalam akun.

```
{
    "State": "audit-mode",
    "ImageCriteria": [
        {
            "MarketplaceProductCodes": [
                "abcdefg1234567890"
            ]
        },
        {
            "ImageProviders": [
                "123456789012",
                "123456789013"
            ],
            "CreationDateCondition": {
                "MaximumDaysSinceCreated": 300
            }
        },
        {
            "ImageProviders": [
                "123456789014"
            ],
            "ImageNames": [
                "golden-ami-*"
            ]
        },
        {
            "ImageProviders": [
                "amazon"
            ],
            "DeprecationTimeCondition": {
                "MaximumDaysSinceDeprecated": 0
            }
        }
    ],
    "ManagedBy": "account"
}
```

PowerShell

Untuk mendapatkan AMIs status dan kriteria yang Diizinkan

Gunakan Get-EC2AllowedImagesSettingcmdlet.

```
Get-EC2AllowedImagesSetting | Select-Object `
    State, `
    ManagedBy, `
    @{Name='ImageProviders'; Expression={($_.ImageCriteria.ImageProviders)}}, `
    @{Name='MarketplaceProductCodes';
 Expression={($_.ImageCriteria.MarketplaceProductCodes)}}, `
    @{Name='ImageNames'; Expression={($_.ImageCriteria.ImageNames)}}, `
    @{Name='MaximumDaysSinceCreated';
 Expression={($_.ImageCriteria.CreationDateCondition.MaximumDaysSinceCreated)}}, `
    @{Name='MaximumDaysSinceDeprecated';
 Expression={($_.ImageCriteria.DeprecationTimeCondition.MaximumDaysSinceDeprecated)}}
```

Dalam contoh output berikut, keadaan `audit-mode` dan kriteria gambar ditetapkan dalam akun.

```
State      : audit-mode
ManagedBy  : account
ImageProviders            : {123456789012, 123456789013, 123456789014, amazon}
MarketplaceProductCodes   : {abcdefg1234567890}
ImageNames                : {golden-ami-*}
MaximumDaysSinceCreated   : 300
MaximumDaysSinceDeprecated: 0
```

Temukan AMIs yang diizinkan

Anda dapat menemukan AMIs yang diizinkan atau tidak diizinkan oleh AMIs kriteria Diizinkan saat ini.

> **Note**
>
> Diizinkan AMIs harus dalam mode audit.

Console

Untuk memeriksa apakah AMI memenuhi AMIs kriteria yang Diizinkan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI.

4. Pada tab Detail (jika Anda memilih kotak centang) atau di area ringkasan (jika Anda memilih ID AMI), cari bidang Gambar yang Diizinkan.

   - Ya - AMI memenuhi AMIs kriteria yang Diizinkan. AMI ini akan tersedia untuk pengguna di akun Anda setelah Anda mengaktifkan DiizinkanAMIs.
   - Tidak - AMI tidak memenuhi AMIs kriteria yang Diizinkan.

5. Di panel navigasi, pilih Katalog AMI.

   AMI bertanda Tidak diizinkan menunjukkan AMI yang tidak memenuhi AMIs kriteria yang Diizinkan. AMI ini tidak akan terlihat atau tersedia bagi pengguna di akun Anda saat Diizinkan AMIs diaktifkan.

AWS CLI

Untuk memeriksa apakah AMI memenuhi AMIs kriteria yang Diizinkan

Gunakan perintah describe-images.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[].ImageAllowed \
    --output text
```

Berikut ini adalah output contoh.

```
True
```

Untuk menemukan AMIs yang memenuhi AMIs kriteria yang Diizinkan

Gunakan perintah describe-images.

```
aws ec2 describe-images \
    --filters "Name=image-allowed,Values=true" \
    --max-items 10 \
    --query Images[].ImageId
```

Berikut ini adalah output contoh.

```
ami-000eaaa8be2fd162a
ami-000f82db25e50de8e
```

```
ami-000fc21eb34c7a9a6
ami-0010b876f1287d7be
ami-0010b929226fe8eba
ami-0010957836340aead
ami-00112c992a47ba871
ami-00111759e194abcc1
ami-001112565ffcafa5e
ami-0011e45aaee9fba88
```

PowerShell

Untuk memeriksa apakah AMI memenuhi AMIs kriteria yang Diizinkan

Gunakan Get-EC2Imagecmdlet.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).ImageAllowed
```

Berikut ini adalah output contoh.

```
True
```

Untuk menemukan AMIs yang memenuhi AMIs kriteria yang Diizinkan

Gunakan Get-EC2Imagecmdlet.

```
Get-EC2Image `
    -Filter @{Name="image-allows";Values="true"} `
    -MaxResult 10 | `
    Select ImageId
```

Berikut ini adalah output contoh.

```
ami-000eaaa8be2fd162a
ami-000f82db25e50de8e
ami-000fc21eb34c7a9a6
ami-0010b876f1287d7be
ami-0010b929226fe8eba
ami-0010957836340aead
ami-00112c992a47ba871
ami-00111759e194abcc1
ami-001112565ffcafa5e
ami-0011e45aaee9fba88
```

Temukan instance yang diluncurkan dari AMIs yang tidak diizinkan

Anda dapat mengidentifikasi instans yang diluncurkan menggunakan AMI yang tidak memenuhi AMIs kriteria Diizinkan.

Console

Untuk memeriksa apakah instance diluncurkan menggunakan AMI yang tidak diizinkan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pada tab Detail, di bawah Detail instans, temukan gambar yang Diizinkan.
   - Ya - AMI memenuhi AMIs kriteria yang Diizinkan.
   - Tidak - AMI tidak memenuhi AMIs kriteria yang Diizinkan.

AWS CLI

Untuk menemukan instance yang diluncurkan menggunakan AMIs yang tidak diizinkan

Gunakan describe-instance-image-metadataperintah dengan `image-allowed` filter.

```
aws ec2 describe-instance-image-metadata \
    --filters "Name=image-allowed,Values=false" \
    --query "InstanceImageMetadata[*].[InstanceId,ImageMetadata.ImageId]" \
    --output table
```

Berikut ini adalah output contoh.

```
-------------------------------------------------
|          DescribeInstanceImageMetadata         |
+----------------------+-------------------------+
|  i-08fd74f3f1595fdbd |  ami-09245d5773578a1d6  |
|  i-0b1bf24fd4f297ab9 |  ami-07cccf2bd80ed467f  |
|  i-026a2eb590b4f7234 |  ami-0c0ec0a3a3a4c34c0  |
|  i-006a6a4e8870c828f |  ami-0a70b9d193ae8a799  |
|  i-0781e91cfeca3179d |  ami-00c257e12d6828491  |
|  i-02b631e2a6ae7c2d9 |  ami-0bfddf4206f1fa7b9  |
+----------------------+-------------------------+
```

PowerShell

Untuk menemukan instance yang diluncurkan menggunakan AMIs yang tidak diizinkan

Gunakan Get-EC2InstanceImageMetadatacmdlet.

```
Get-EC2InstanceImageMetadata `
    -Filter @{Name="image-allowed";Values="false"} | `
    Select InstanceId, @{Name='ImageId'; Expression={($_.ImageMetadata.ImageId)}}
```

Berikut ini adalah output contoh.

```
InstanceId          ImageId
----------          -------
i-08fd74f3f1595fdbd ami-09245d5773578a1d6
i-0b1bf24fd4f297ab9 ami-07cccf2bd80ed467f
i-026a2eb590b4f7234 ami-0c0ec0a3a3a4c34c0
i-006a6a4e8870c828f ami-0a70b9d193ae8a799
i-0781e91cfeca3179d ami-00c257e12d6828491
i-02b631e2a6ae7c2d9 ami-0bfddf4206f1fa7b9
```

AWS Config

Anda dapat menambahkan AWS Config aturan ec2- instance-launched-with-allowed -ami, mengonfigurasinya untuk kebutuhan Anda, dan kemudian menggunakannya untuk mengevaluasi instance Anda.

Untuk informasi selengkapnya, lihat Menambahkan AWS Config aturan dan ec2- instance-launched-with-allowed -ami di Panduan AWS Config Pengembang.

Jadikan AMI Anda tersedia untuk umum untuk digunakan di Amazon EC2

Anda dapat membuat AMI Anda tersedia untuk umum dengan membagikannya kepada semua Akun AWS.

Jika Anda ingin mencegah berbagi publik AMIs, Anda dapat mengaktifkan blokir akses publik untuk AMIs. Hal ini memblokir setiap upaya untuk membuat AMI publik, membantu mencegah akses tidak sah dan potensi penyalahgunaan data AMI. Perhatikan bahwa mengaktifkan blokir akses publik tidak memengaruhi akses Anda AMIs yang sudah tersedia untuk umum; mereka tetap tersedia untuk umum. Untuk informasi selengkapnya, lihat Memahami memblokir akses publik untuk AMIs.

Untuk mengizinkan hanya akun tertentu yang menggunakan AMI Anda untuk meluncurkan instans, lihat Bagikan AMI dengan AWS akun tertentu.

Daftar Isi

- Pertimbangan-pertimbangan
- Bagikan AMI dengan semua AWS akun (bagikan secara publik)

Pertimbangan-pertimbangan

Pertimbangkan hal berikut sebelum menjadikan AMI publik.

- Kepemilikan — Untuk membuat AMI publik, Anda Akun AWS harus memiliki AMI.
- Wilayah — AMIs adalah sumber daya Regional. Saat Anda membagikan AMI, AMI hanya tersedia di Wilayah tempat Anda membagikannya. Agar AMI tersedia di Wilayah yang berbeda, salin AMI ke Wilayah, lalu bagikan. Untuk informasi selengkapnya, lihat Salin Amazon EC2 AMI.
- Blokir akses publik — Untuk berbagi AMI secara publik, blokir akses publik untuk AMIs harus dinonaktifkan di setiap Wilayah di mana AMI akan dibagikan secara publik. Setelah membagikan AMI secara publik, Anda dapat mengaktifkan kembali blokir akses publik AMIs untuk mencegah pembagian publik lebih lanjut dari AMI Anda. AMIs
- Beberapa tidak AMIs dapat dipublikasikan - Jika AMI Anda menyertakan salah satu komponen berikut, Anda tidak dapat mempublikasikannya (tetapi Anda dapat membagikan AMI dengan spesifik Akun AWS):
  - Volume terenkripsi
  - Snapshot volume terenkripsi
  - Kode produk
- Hindari pemaparan data sensitif – Untuk menghindari pemaparan data sensitif saat Anda membagikan AMI, baca pertimbangan keamanan di Rekomendasi untuk membuat Linux bersama AMIs dan ikuti tindakan yang direkomendasikan.
- Penggunaan – Saat Anda membagikan AMI, pengguna hanya dapat meluncurkan instans dari AMI tersebut. Mereka tidak dapat menghapus, berbagi, atau memodifikasinya. Namun, setelah mereka meluncurkan instans menggunakan AMI Anda, mereka dapat membuat AMI dari instans yang mereka luncurkan.
- Pengakhiran otomatis — Secara default, tanggal penghentian semua publik AMIs diatur ke dua tahun dari tanggal pembuatan AMI. Anda dapat mengatur tanggal pengusangan menjadi lebih awal dari dua tahun. Untuk membatalkan tanggal penghentian, atau untuk memindahkan penghentian

ke tanggal berikutnya, Anda harus menjadikan AMI pribadi dengan hanya membagikannya dengan spesifik. Akun AWS

- Hapus usang AMIs — Setelah AMI publik mencapai tanggal penghentian, jika tidak ada instans baru yang diluncurkan dari AMI selama enam bulan atau lebih, AWS akhirnya menghapus properti berbagi publik sehingga usang AMIs tidak muncul di daftar AMI publik.
- Penagihan — Anda tidak ditagih ketika AMI Anda digunakan oleh orang lain Akun AWS untuk meluncurkan instans. Akun yang meluncurkan instans menggunakan AMI akan dikenai biaya untuk instans yang diluncurkan.

Bagikan AMI dengan semua AWS akun (bagikan secara publik)

Setelah Anda membuat AMI publik, AMI tersedia di Komunitas AMIs di konsol, yang dapat Anda akses dari Katalog AMI di navigator kiri di konsol EC2 atau saat meluncurkan instance menggunakan konsol. Harap diperhatikan bahwa diperlukan waktu hingga AMI muncul di AMIs Komunitas setelah Anda membuatnya publik.

Console

Untuk menjadikan AMI publik

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI Anda dari daftar, lalu pilih Tindakan, Ubah izin AMI.
4. Di bawah Ketersediaan AMI, pilih Publik.
5. Pilih Simpan perubahan.

AWS CLI

Setiap AMI memiliki `launchPermission` properti yang mengontrol yang Akun AWS, selain pemilik, diizinkan untuk menggunakan AMI itu untuk meluncurkan instance. Dengan memodifikasi `launchPermission` properti AMI, Anda dapat membuat AMI menjadi publik (yang memberikan izin peluncuran ke semua Akun AWS), atau membagikannya hanya dengan Akun AWS yang Anda tentukan.

Anda dapat menambah atau menghapus akun IDs dari daftar akun yang memiliki izin peluncuran untuk AMI. Untuk menjadikan AMI publik, tentukan kelompok `all`. Anda dapat menentukan izin peluncuran publik dan eksplisit.

Untuk menjadikan AMI publik

1. Gunakan perintah modify-image-attribute sebagai berikut untuk menambahkan grup `all` ke daftar `launchPermission` untuk AMI tertentu.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. Untuk memverifikasi izin peluncuran AMI, gunakan perintah describe-image-attribute.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. (Opsional) Untuk menjadikan AMI kembali privat, hapus grup `all` dari izin peluncurannya. Perhatikan bahwa pemilik AMI selalu memiliki izin peluncuran sehingga tidak terpengaruh oleh perintah ini.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Setiap AMI memiliki `launchPermission` properti yang mengontrol yang Akun AWS, selain pemilik, diizinkan untuk menggunakan AMI itu untuk meluncurkan instance. Dengan memodifikasi `launchPermission` properti AMI, Anda dapat membuat AMI menjadi publik (yang memberikan izin peluncuran ke semua Akun AWS), atau membagikannya hanya dengan Akun AWS yang Anda tentukan.

Anda dapat menambah atau menghapus akun IDs dari daftar akun yang memiliki izin peluncuran untuk AMI. Untuk menjadikan AMI publik, tentukan kelompok `all`. Anda dapat menentukan izin peluncuran publik dan eksplisit.

Untuk menjadikan AMI publik

1. Gunakan perintah Edit-EC2ImageAttribute sebagai berikut untuk menambahkan grup `all` ke daftar `launchPermission` untuk AMI tertentu.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -UserGroup all
```

2. Untuk memverifikasi izin peluncuran AMI, gunakan perintah Get-EC2ImageAttribute berikut.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

3. (Opsional) Untuk menjadikan AMI kembali privat, hapus grup `all` dari izin peluncurannya. Perhatikan bahwa pemilik AMI selalu memiliki izin peluncuran sehingga tidak terpengaruh oleh perintah ini.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -UserGroup all
```

Memahami memblokir akses publik untuk AMIs

Untuk mencegah berbagi publik Anda AMIs, Anda dapat mengaktifkan blokir akses publik AMIs di tingkat akun.

Ketika mengaktifkan memblokir akses publik, setiap upaya untuk menjadikan AMI publik secara otomatis diblokir. Namun, jika Anda sudah memiliki publik AMIs, mereka tetap tersedia untuk umum.

Untuk berbagi secara publik AMIs, Anda harus menonaktifkan blokir akses publik. Setelah selesai berbagi, praktik terbaik adalah mengaktifkan kembali blokir akses publik untuk mencegah berbagi publik yang tidak diinginkan dari Anda. AMIs

> **Note**
>
> Pengaturan ini dikonfigurasi di tingkat akun, baik secara langsung di akun atau dengan menggunakan kebijakan deklaratif. Itu harus dikonfigurasi di setiap AWS Region tempat Anda ingin mencegah berbagi publik Anda AMIs. Menggunakan kebijakan deklaratif

memungkinkan Anda menerapkan pengaturan di beberapa Wilayah secara bersamaan, serta di beberapa akun secara bersamaan. Saat kebijakan deklaratif sedang digunakan, Anda tidak dapat mengubah setelan secara langsung di dalam akun. Topik ini menjelaskan cara mengonfigurasi pengaturan secara langsung di dalam akun. Untuk informasi tentang penggunaan kebijakan deklaratif, lihat Kebijakan deklaratif di AWS Organizations Panduan Pengguna.

Anda dapat membatasi izin IAM untuk pengguna administrator sehingga hanya mereka yang dapat mengaktifkan atau menonaktifkan blokir akses publik. AMIs

Topik

- Pengaturan default
- Mengelola setelan blokir akses publik untuk AMIs

Pengaturan default

Blokir akses publik untuk AMIs pengaturan diaktifkan atau dinonaktifkan secara default tergantung pada apakah akun Anda baru atau sudah ada, dan apakah Anda memiliki publik AMIs. Tabel berikut menjelaskan pengaturan default:

AWS akun	Memblokir akses publik untuk pengaturan AMIs default
Akun baru	Diaktifkan
Akun yang ada tanpa publik AMIs [1]	Diaktifkan
Akun yang ada dengan satu atau lebih publik AMIs	Nonaktif

[1] Jika akun Anda memiliki satu atau lebih publik AMIs pada atau setelah 15 Juli 2023, Blokir akses publik untuk AMIs dinonaktifkan secara default untuk akun Anda, bahkan jika Anda kemudian membuat semua AMIs pribadi.

Mengelola setelan blokir akses publik untuk AMIs

Anda dapat mengelola pengaturan blokir akses publik untuk AMI Anda untuk mengontrol apakah mereka dapat dibagikan secara publik. Anda dapat mengaktifkan, menonaktifkan, atau melihat status akses publik blokir saat ini untuk AMI Anda menggunakan konsol Amazon EC2 atau. AWS CLI

Lihat status blokir akses publik untuk AMIs

Untuk melihat apakah pembagian publik Anda AMIs diblokir di akun Anda, Anda dapat melihat status untuk memblokir akses publik AMIs. Anda harus melihat status AWS Region di masing-masing tempat Anda ingin melihat apakah berbagi publik Anda AMIs diblokir.

Izin yang diperlukan

Untuk mendapatkan pengaturan akses publik blok saat ini AMIs, Anda harus memiliki izin `GetImageBlockPublicAccessState` IAM.

Console

Untuk melihat status blokir akses publik AMIs di Wilayah yang ditentukan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari bilah navigasi (di bagian atas layar), pilih Wilayah tempat untuk melihat status akses publik blok AMIs.
3. Di panel navigasi, pilih Dasbor.
4. Pada kartu Atribut akun, di bawah Pengaturan, pilih Perlindungan dan keamanan data.
5. Di bawah Blokir akses publik untuk AMIs, periksa bidang Akses publik. Nilainya adalah Berbagi publik baru diblokir atau Berbagi publik baru diizinkan.

AWS CLI

Untuk mendapatkan status akses publik blok untuk AMIs

Gunakan perintah get-image-block-public-access-state. Nilainya adalah `block-new-sharing` atau `unblocked`.

Contoh: Untuk Wilayah tertentu

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

`ManagedBy`Bidang menunjukkan entitas yang mengkonfigurasi pengaturan. Dalam contoh ini, `account` menunjukkan bahwa pengaturan dikonfigurasi langsung di akun. Nilai `declarative-policy` berarti pengaturan dikonfigurasi oleh kebijakan deklaratif. Untuk informasi selengkapnya, lihat Kebijakan deklaratif di Panduan AWS Organizations Pengguna.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing",
    "ManagedBy": "account"
}
```

Contoh: Untuk semua Wilayah di akun Anda

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-image-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Berikut ini adalah output contoh.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       unblocked
eu-west-3        block-new-sharing
...
```

PowerShell

Untuk mendapatkan status akses publik blok untuk AMIs

Gunakan Get-EC2ImageBlockPublicAccessStatecmdlet. Nilainya adalah `block-new-sharing` atau `unblocked`.

Contoh: Untuk Wilayah tertentu

```
Get-EC2ImageBlockPublicAccessState -Region us-east-1
```

Berikut ini adalah output contoh.

```
block-new-sharing
```

Contoh: Untuk semua Wilayah di akun Anda

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
        [PSCustomObject]@{
            Region   = $_
            PublicAccessState = (Get-EC2ImageBlockPublicAccessState -Region $_)
        }
} | `
Format-Table -AutoSize
```

Berikut ini adalah output contoh.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Aktifkan blokir akses publik untuk AMIs

Untuk mencegah pembagian publik Anda AMIs, aktifkan blokir akses publik AMIs di tingkat akun. Anda harus mengaktifkan blokir akses publik untuk masing-masing AMIs AWS Region di mana Anda ingin mencegah berbagi publik Anda AMIs. Jika Anda sudah memiliki publik AMIs, mereka akan tetap tersedia untuk umum.

Izin yang diperlukan

Untuk mengaktifkan pengaturan blokir akses publik AMIs, Anda harus memiliki izin `EnableImageBlockPublicAccess` IAM.

Pertimbangan-pertimbangan

- Diperlukan waktu hingga 10 menit untuk mengonfigurasi pengaturan ini. Selama waktu ini, jika Anda menggambarkan status akses publik, responsnya adalah`unblocked`. Ketika konfigurasi selesai, responsnya adalah`block-new-sharing`.

Console

Untuk mengaktifkan blokir akses publik AMIs di Wilayah yang ditentukan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari bilah navigasi (di bagian atas layar), pilih Wilayah tempat mengaktifkan blokir akses publik AMIs.
3. Di panel navigasi, pilih Dasbor.
4. Pada kartu Atribut akun, di bawah Pengaturan, pilih Perlindungan dan keamanan data.
5. Di bawah Blokir akses publik untuk AMIs, pilih Kelola.
6. Pilih kotak centang Blokir berbagi publik baru, lalu pilih Perbarui.

AWS CLI

Untuk mengaktifkan blokir akses publik untuk AMIs

Gunakan perintah enable-image-block-public-access.

Contoh: Untuk Wilayah tertentu

```
aws ec2 enable-image-block-public-access \
--region us-east-1 \
--image-block-public-access-state block-new-sharing
```

Berikut ini adalah output contoh.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
```

```
}
```

Contoh: Untuk semua Wilayah di akun Anda

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 enable-image-block-public-access \
            --region $region \
            --image-block-public-access-state block-new-sharing \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Berikut ini adalah output contoh.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
...
```

PowerShell

Untuk mengaktifkan blokir akses publik untuk AMIs

Gunakan perintah Enable-EC2ImageBlockPublicAccess.

Contoh: Untuk Wilayah tertentu

```
Enable-EC2ImageBlockPublicAccess `
    -Region us-east-1 `
    -ImageBlockPublicAccessState block-new-sharing
```

Berikut ini adalah output contoh.

```
Value
-----
block-new-sharing
```

Contoh: Untuk semua Wilayah di akun Anda

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (
        Enable-EC2ImageBlockPublicAccess `
         -Region $_ `
         -ImageBlockPublicAccessState block-new-sharing)
    }
} | `
Format-Table -AutoSize
```

Berikut ini adalah output contoh.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Nonaktifkan blokir akses publik untuk AMIs

Untuk memungkinkan pengguna di akun Anda berbagi secara publik AMIs, nonaktifkan blokir akses publik di tingkat akun. Anda harus menonaktifkan blokir akses publik untuk masing-masing AMIs AWS Region di mana Anda ingin mengizinkan berbagi publik AndaAMIs.

Izin yang diperlukan

Untuk menonaktifkan pengaturan blokir akses publik AMIs, Anda harus memiliki izin `DisableImageBlockPublicAccess` IAM.

Pertimbangan-pertimbangan

- Diperlukan waktu hingga 10 menit untuk mengonfigurasi pengaturan ini. Selama waktu ini, jika Anda menggambarkan status akses publik, responsnya adalah`block-new-sharing`. Ketika konfigurasi selesai, responsnya adalah`unblocked`.

Console

Untuk menonaktifkan blokir akses publik untuk AMIs di Wilayah yang ditentukan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari bilah navigasi (di bagian atas layar), pilih Wilayah tempat menonaktifkan blokir akses publik AMIs.
3. Di panel navigasi, pilih Dasbor.
4. Pada kartu Atribut akun, di bawah Pengaturan, pilih Perlindungan dan keamanan data.
5. Di bawah Blokir akses publik untuk AMIs, pilih Kelola.
6. Kosongkan kotak centang Blokir berbagi publik baru, lalu pilih Perbarui.
7. Masukkan **`confirm`** saat diminta konfirmasi, lalu pilih Izinkan berbagi publik.

AWS CLI

Untuk menonaktifkan blokir akses publik untuk AMIs

Gunakan perintah disable-image-block-public-access.

Contoh: Untuk Wilayah tertentu

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Berikut ini adalah output contoh.

```
{
   "ImageBlockPublicAccessState": "unblocked"
}
```

Contoh: Untuk semua Wilayah di akun Anda

```
echo -e "Region   \t Public Access State" ; \
```

```
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-image-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Berikut ini adalah output contoh.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

PowerShell

Untuk menonaktifkan blokir akses publik untuk AMIs

Gunakan Disable-EC2ImageBlockPublicAccesscmdlet.

Contoh: Untuk Wilayah tertentu

```
Disable-EC2ImageBlockPublicAccess -Region us-east-1
```

Berikut ini adalah output contoh.

```
Value
-----
unblocked
```

Contoh: Untuk semua Wilayah di akun Anda

```
(Get-EC2Region).RegionName | `
```

```
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Disable-EC2ImageBlockPublicAccess -Region $_)
    }
} | `
Format-Table -AutoSize
```

Berikut ini adalah output contoh.

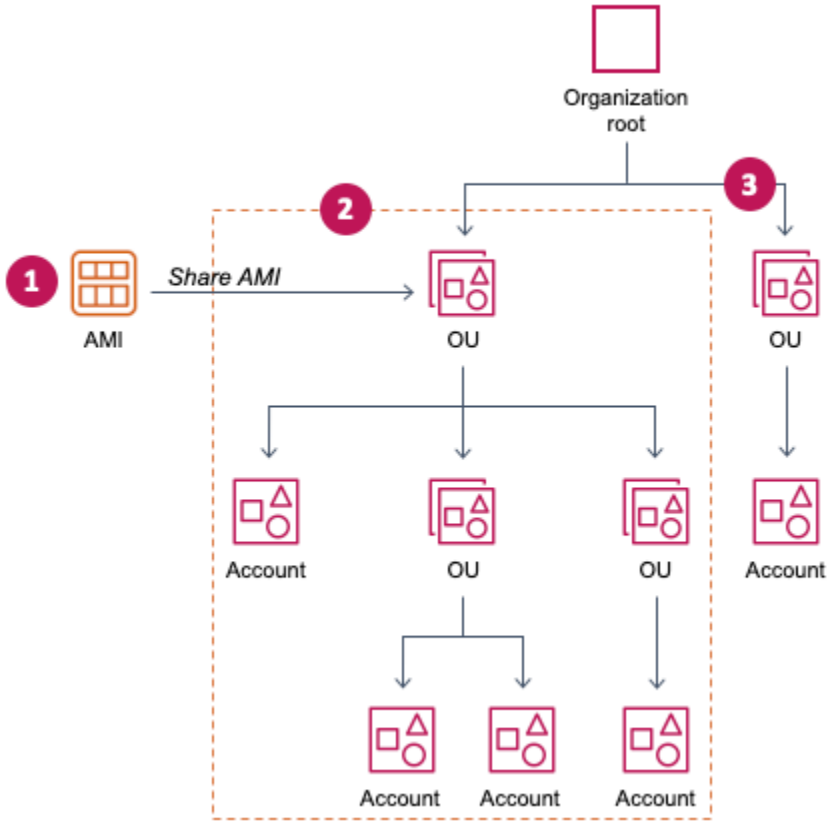
```
Region         PublicAccessState
------         -----------------
ap-south-1     unblocked
eu-north-1     unblocked
eu-west-3      unblocked
...
```

Bagikan AMI dengan organisasi dan unit organisasi

AWS Organizationsadalah layanan manajemen akun yang memungkinkan Anda untuk mengkonsolidasikan beberapa Akun AWS ke dalam organisasi yang Anda buat dan kelola secara terpusat. Anda dapat berbagi AMI dengan organisasi atau unit organisasi (OU) yang telah Anda buat, selain membagikannya dengan akun tertentu.

Organisasi adalah entitas yang Anda buat untuk mengkonsolidasikan dan mengelola Akun AWS Anda secara terpusat. Anda dapat mengorganisasi akun dalam struktur hierarkis seperti pohon, dengan root di bagian atas dan unit-unit organisasi bersarang di bawah root organisasi. Setiap akun dapat ditambahkan langsung ke root, atau ditempatkan di salah satu OUs dalam hierarki. Untuk informasi selengkapnya, lihat Terminologi dan konsep organisasi AWS di Panduan Pengguna AWS Organizations .

Saat Anda berbagi AMI dengan organisasi atau OU, semua akun turunan mendapatkan akses ke AMI. Misalnya, dalam diagram berikut, AMI dibagikan dengan OU tingkat atas (ditunjukkan oleh panah pada angka 1). Semua OUs dan akun yang bersarang di bawah OU tingkat atas itu (ditunjukkan oleh garis putus-putus di nomor 2) juga memiliki akses ke AMI. Akun di organisasi dan OU di luar garis putus-putus (ditunjukkan oleh angka 3) tidak memiliki akses ke AMI karena mereka bukan turunan dari OU yang dibagikan AMI.



Topik

- Pertimbangan-pertimbangan
- Dapatkan ARN dari organisasi atau unit organisasi
- Izinkan organisasi dan OUs menggunakan kunci KMS
- Kelola berbagi AMI dengan organisasi atau OU

Pertimbangan-pertimbangan

Pertimbangkan hal berikut saat berbagi AMIs dengan organisasi atau unit organisasi tertentu.

- Kepemilikan – Untuk berbagi AMI, Akun AWS Anda harus merupakan pemilik AMI.
- Batas berbagi — Pemilik AMI dapat berbagi AMI dengan organisasi atau OU mana pun, termasuk organisasi dan OUs bahwa mereka bukan anggotanya.

  Untuk jumlah maksimum entitas yang dapat dibagikan AMI dalam satu Wilayah, lihat Kuota layanan Amazon EC2.

- Tag – Anda tidak dapat membagikan tag buatan pengguna (tag yang Anda lampirkan ke AMI). Saat Anda membagikan AMI, tag yang ditentukan pengguna tidak tersedia untuk organisasi atau OU mana pun Akun AWS yang dengannya AMI dibagikan.
- Format ARN – Saat Anda menentukan organisasi atau OU dalam sebuah perintah, pastikan menggunakan format ARN yang benar. Anda akan mendapatkan kesalahan jika Anda hanya menentukan ID, misalnya, jika Anda hanya menentukan `o-123example` atau `ou-1234-5example`.

  Format ARN yang benar:

  - ARN Organisasi: `arn:aws:organizations::`*`111122223333`*`:organization/`*`organization-id`*
  - ARN OU: `arn:aws:organizations::`*`111122223333`*`:ou/`*`organization-id`*`/`*`ou-id`*

  Di mana:

  - *`111122223333`*adalah contoh ID akun 12 digit untuk akun manajemen. Jika Anda tidak tahu nomor akun manajemen, Anda dapat menjelaskan organisasi atau unit organisasi untuk mendapatkan ARN, yang mencakup nomor akun manajemen. Untuk informasi selengkapnya, lihat Dapatkan ARN dari organisasi atau unit organisasi.
  - *`organization-id`* adalah ID organisasi, misalnya, `o-123example`.
  - *`ou-id`* adalah ID unit organisasi, misalnya, `ou-1234-5example`.

  Untuk informasi selengkapnya tentang format ARNs, lihat Amazon Resource Names (ARNs) di Panduan Pengguna IAM.
- Enkripsi dan kunci — Anda dapat berbagi AMIs yang didukung oleh snapshot yang tidak terenkripsi dan terenkripsi.
  - Snapshot terenkripsi harus dienkripsi dengan kunci yang dikelola pelanggan. Anda tidak dapat berbagi AMIs yang didukung oleh snapshot yang dienkripsi dengan kunci terkelola default AWS .
  - Jika Anda membagikan AMI yang didukung oleh snapshot terenkripsi, Anda harus mengizinkan organisasi atau OUs menggunakan kunci terkelola pelanggan yang digunakan untuk mengenkripsi snapshot. Untuk informasi selengkapnya, lihat Izinkan organisasi dan OUs menggunakan kunci KMS.
- Wilayah — AMIs adalah sumber daya Regional. Saat Anda membagikan AMI, AMI hanya tersedia di Wilayah tempat Anda membagikannya. Agar AMI tersedia di Wilayah yang berbeda, salin AMI ke Wilayah, lalu bagikan. Untuk informasi selengkapnya, lihat Salin Amazon EC2 AMI.

- Penggunaan – Saat Anda membagikan AMI, pengguna hanya dapat meluncurkan instans dari AMI tersebut. Mereka tidak dapat menghapus, berbagi, atau memodifikasinya. Namun, setelah mereka meluncurkan instans menggunakan AMI Anda, mereka dapat membuat AMI dari instans yang mereka luncurkan.
- Penagihan — Anda tidak ditagih ketika AMI Anda digunakan oleh orang lain Akun AWS untuk meluncurkan instans. Akun yang meluncurkan instans menggunakan AMI akan dikenai biaya untuk instans yang diluncurkan.

Dapatkan ARN dari organisasi atau unit organisasi

Organisasi dan unit organisasi ARNs berisi nomor akun manajemen 12 digit. Jika Anda tidak tahu nomor akun manajemen, Anda dapat menjelaskan organisasi atau unit organisasi untuk mendapatkan ARN untuk keduanya. Dalam contoh berikut, `123456789012` adalah ID akun dari akun manajemen.

Izin yang diperlukan

Sebelum Anda bisa mendapatkan ARNs, Anda harus memiliki izin untuk menggambarkan organisasi dan unit organisasi. Kebijakan berikut ini memberikan izin yang diperlukan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS CLI

Untuk mendapatkan ARN suatu organisasi

Gunakan perintah describe-organization. Tambahkan `--query` opsi untuk mengembalikan hanya ARN organisasi.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Berikut ini adalah output contoh.

```
"arn:aws:organizations::123456789012:organization/o-1234567abc"
```

Untuk mendapatkan ARN unit organisasi

Gunakan perintah describe-organizational-unit. Gunakan `--query` parameter untuk mengembalikan hanya unit organisasi ARN.

```
aws organizations describe-organizational-unit \
    --organizational-unit-id ou-a123-b4567890 \
    --query 'OrganizationalUnit.Arn'
```

Berikut ini adalah output contoh.

```
"arn:aws:organizations::123456789012:ou/o-1234567abc/ou-a123-b4567890"
```

PowerShell

Untuk mendapatkan ARN suatu organisasi

Gunakan Get- ORGOrganization cmdlet.

```
(Get-ORGOrganization).Arn
```

Berikut ini adalah output contoh.

```
arn:aws:organizations::123456789012:organization/o-1234567abc
```

Untuk mendapatkan ARN unit organisasi

Gunakan cmdlet Get- ORGOrganizational Unit.

```
(Get-ORGOrganizationalUnit -OrganizationalUnitId "ou-a123-b4567890").Arn
```

Berikut ini adalah output contoh.

```
arn:aws:organizations::123456789012:ou/o-1234567abc/ou-a123-b4567890
```

Izinkan organisasi dan OUs menggunakan kunci KMS

Jika Anda berbagi AMI yang didukung oleh snapshot terenkripsi, Anda juga harus mengizinkan organisasi atau unit organisasi (OUs) untuk menggunakan kunci KMS yang digunakan untuk mengenkripsi snapshot.

> **Note**
>
> Snapshot terenkripsi harus dienkripsi dengan kunci yang dikelola pelanggan. Anda tidak dapat berbagi AMIs yang didukung oleh snapshot yang dienkripsi dengan kunci terkelola default AWS .

Untuk mengontrol akses ke kunci KMS, dalam kebijakan kunci Anda dapat menggunakan kunci `aws:PrincipalOrgID`dan `aws:PrincipalOrgPaths`kondisi untuk mengizinkan hanya izin prinsipal tertentu untuk tindakan yang ditentukan. Prinsipal dapat berupa pengguna, peran IAM, pengguna federasi, atau pengguna Akun AWS root.

Kunci kondisi digunakan sebagai berikut:

- `aws:PrincipalOrgID`— Memungkinkan setiap prinsipal milik organisasi yang diwakili oleh ID yang ditentukan.
- `aws:PrincipalOrgPaths`— Memungkinkan setiap prinsipal milik yang OUs diwakili oleh jalur yang ditentukan.

Untuk memberikan izin kepada organisasi (termasuk OUs dan akun miliknya) untuk menggunakan kunci KMS, tambahkan pernyataan berikut ke kebijakan kunci.

```
{
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "kms:Describe*",
```

```
        "kms:List*",
        "kms:Get*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Untuk memberikan izin khusus OUs (dan akun miliknya) untuk menggunakan kunci KMS, Anda dapat menggunakan kebijakan yang mirip dengan contoh berikut.

```
{
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms:CreateGrant"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
```

```
            }
        }
}
```

Untuk contoh pernyataan kondisi lainnya, lihat aws:PrincipalOrgID dan aws:PrincipalOrgPaths di Panduan Pengguna IAM.

Untuk informasi tentang akses lintas akun, lihat Mengizinkan pengguna di akun lain menggunakan kunci KMS di Panduan AWS Key Management Service Pengembang.

Kelola berbagi AMI dengan organisasi atau OU

Anda dapat mengelola berbagi AMI dengan organisasi dan unit organisasi (OU) untuk mengontrol apakah mereka dapat meluncurkan instans Amazon EC2.

Lihat organisasi dan OUs dengan mana AMI dibagikan

Anda dapat menemukan organisasi dan OUs dengan mana Anda telah berbagi AMI Anda.

Console

Untuk memeriksa dengan organisasi mana dan OUs Anda telah membagikan AMI Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI Anda dalam daftar, pilih tab Izin, dan gulir ke bawah ke Organisasi OUs bersama/.

   Untuk menemukan AMIs yang dibagikan dengan Anda, lihatTemukan AMI bersama untuk digunakan untuk instans Amazon EC2.

AWS CLI

Untuk memeriksa dengan organisasi mana dan OUs Anda telah membagikan AMI Anda

Gunakan describe-image-attributeperintah dengan `launchPermission` atribut.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Berikut ini adalah contoh respons.

```
{
    "ImageId": "ami-0abcdef1234567890",
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

PowerShell

Untuk memeriksa dengan organisasi mana dan OUs Anda telah membagikan AMI Anda

Gunakan Get-EC2ImageAttributecmdlet.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Berbagi AMI dengan organisasi atau OU

Anda dapat berbagi AMI dengan organisasi atau OU.

> **Note**
>
> Anda tidak perlu membagikan snapshot Amazon EBS yang dirujuk oleh AMI untuk membagikan AMI. Hanya AMI itu sendiri yang perlu dibagikan, dan sistem secara otomatis menyediakan instance dengan akses ke snapshot EBS yang direferensikan untuk peluncuran. Namun, Anda perlu berbagi kunci KMS yang digunakan untuk mengenkripsi snapshot yang ditunjuk oleh AMI. Untuk informasi selengkapnya, lihat Izinkan organisasi dan OUs menggunakan kunci KMS.

Console

Untuk berbagi AMI dengan organisasi atau OU

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.

3. Pilih AMI Anda dalam daftar, lalu pilih Tindakan, Ubah izin AMI.
4. Di bawah Ketersediaan AMI, pilih Privat.
5. Di samping Organisasi bersama/OUs, pilih Tambahkan ARN. organization/OU
6. Untuk ARN Organisasi/OU, masukkan ARN organisasi atau ARN OU di mana Anda ingin berbagi AMI, lalu pilih Bagikan AMI. Perhatikan bahwa Anda harus menentukan ARN lengkap, bukan hanya ID-nya.

   Untuk berbagi AMI ini dengan beberapa organisasi atau OUs, ulangi langkah ini sampai Anda telah menambahkan semua organisasi yang diperlukan atau OUs.
7. Setelah selesai, pilih Simpan perubahan.
8. (Opsional) Untuk melihat organisasi atau OUs yang telah Anda bagikan AMI, pilih AMI dalam daftar, pilih tab Izin, dan gulir ke bawah ke Organisasi OUs bersama/. Untuk menemukan AMIs yang dibagikan dengan Anda, lihatTemukan AMI bersama untuk digunakan untuk instans Amazon EC2.

AWS CLI

Untuk berbagi AMI dengan organisasi

Gunakan modify-image-attributeperintah untuk memberikan izin peluncuran untuk AMI yang ditentukan ke organisasi yang ditentukan.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Untuk berbagi AMI dengan OU

modify-image-attributePerintah memberikan izin peluncuran untuk AMI yang ditentukan ke OU yang ditentukan. Perhatikan bahwa Anda harus menentukan ARN lengkap, bukan hanya ID-nya.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

PowerShell

Gunakan Edit-EC2ImageAttributeperintah (Alat untuk Windows PowerShell) untuk berbagi AMI seperti yang ditunjukkan pada contoh berikut.

Untuk berbagi AMI dengan organisasi atau OU

Perintah berikut memberikan izin peluncuran untuk AMI yang ditentukan ke organisasi tertentu.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Untuk berhenti berbagi AMI dengan organisasi atau OU

Perintah berikut menghapus izin peluncuran untuk AMI yang ditentukan dari organisasi tertentu:

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Untuk berhenti berbagi AMI dengan semua organisasi, OUs, dan Akun AWS

Perintah berikut ini menghapus semua izin peluncuran publik dan eksplisit dari AMI yang ditentukan. Perhatikan bahwa pemilik AMI selalu memiliki izin peluncuran sehingga tidak terpengaruh oleh perintah ini.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Berhenti berbagi AMI dengan organisasi atau OU

Anda dapat berhenti berbagi AMI dengan organisasi atau OU.

> **Note**
>
> Anda tidak dapat berhenti berbagi AMI dengan akun tertentu jika akun tersebut berada di organisasi atau OU yang dengannya AMI dibagikan. Jika Anda mencoba untuk berhenti berbagi AMI dengan menghapus izin peluncuran untuk akun tersebut, Amazon EC2 akan menampilkan pesan sukses. Namun, AMI terus dibagikan dengan akun tersebut.

Console

Untuk berhenti berbagi AMI dengan organisasi atau OU

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI Anda dalam daftar, lalu pilih Tindakan, Ubah izin AMI.
4. Di bawah Organisasi bersama/ OUs, pilih organisasi atau OUs yang ingin Anda hentikan berbagi AMI, lalu pilih Hapus yang dipilih.
5. Setelah selesai, pilih Simpan perubahan.
6. (Opsional) Untuk mengonfirmasi bahwa Anda telah berhenti membagikan AMI dengan organisasi atauOUs, pilih AMI dalam daftar, pilih tab Izin, dan gulir ke bawah ke Organisasi OUs bersama/.

AWS CLI

Untuk berhenti berbagi AMI dengan organisasi atau OU

Gunakan perintah modify-image-attribute. Contoh ini menghapus izin peluncuran untuk AMI yang ditentukan dari organisasi yang ditentukan.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Untuk berhenti berbagi AMI dengan semua organisasi, OUs, dan Akun AWS

Gunakan perintah reset-image-attribute. Contoh ini menghapus semua izin peluncuran publik dan eksplisit dari AMI yang ditentukan. Perhatikan bahwa pemilik AMI selalu memiliki izin peluncuran sehingga tidak terpengaruh oleh perintah ini.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

PowerShell

Untuk berhenti berbagi AMI dengan organisasi atau OU

Gunakan Edit-EC2ImageAttributecmdlet. Contoh ini menghapus izin peluncuran untuk AMI yang ditentukan dari organisasi yang ditentukan.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Untuk berhenti berbagi AMI dengan semua organisasi, OUs, dan Akun AWS

Gunakan Reset-EC2ImageAttributecmdlet. Contoh ini menghapus semua izin peluncuran publik dan eksplisit dari AMI yang ditentukan. Perhatikan bahwa pemilik AMI selalu memiliki izin peluncuran sehingga tidak terpengaruh oleh perintah ini.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute LaunchPermission
```

Bagikan AMI dengan AWS akun tertentu

Anda dapat berbagi AMI dengan spesifik Akun AWS tanpa membuat AMI publik. Yang Anda butuhkan adalah Akun AWS IDs.

Akun AWS ID adalah angka 12 digit, seperti`012345678901`, yang secara unik mengidentifikasi sebuah. Akun AWS Untuk informasi selengkapnya, lihat Melihat Akun AWS pengenal di Panduan AWS Account Management Referensi.

Pertimbangan-pertimbangan

Pertimbangkan hal berikut saat berbagi AMIs dengan spesifik Akun AWS.

- Kepemilikan – Untuk berbagi AMI, Akun AWS Anda harus merupakan pemilik AMI.
- Batas berbagi – Untuk jumlah maksimum entitas yang dapat digunakan bersama AMI dalam suatu Wilayah, lihat kuota layanan Amazon EC2.
- Tag – Anda tidak dapat membagikan tag buatan pengguna (tag yang Anda lampirkan ke AMI). Saat Anda membagikan AMI, tag yang ditentukan pengguna tidak tersedia untuk semua Akun AWS yang digunakan bersama AMI.
- Snapshots — Anda tidak perlu membagikan snapshot Amazon EBS yang direferensikan AMI untuk membagikan AMI. Anda hanya dapat membagikan AMI itu sendiri; sistem menyediakan akses instans ke snapshot EBS yang direferensikan untuk peluncuran. Namun, Anda harus membagikan kunci KMS apa pun yang digunakan untuk mengenkripsi snapshot yang direferensikan AMI. Untuk informasi selengkapnya, lihat Membagikan snapshot Amazon EBS di Panduan Pengguna Amazon EBS.
- Enkripsi dan kunci — Anda dapat berbagi AMIs yang didukung oleh snapshot yang tidak terenkripsi dan terenkripsi.
  - Snapshot terenkripsi harus dienkripsi dengan kunci KMS. Anda tidak dapat berbagi AMIs yang didukung oleh snapshot yang dienkripsi dengan kunci terkelola default AWS .
  - Jika Anda berbagi AMI yang didukung oleh snapshot terenkripsi, Anda harus mengizinkan Akun AWS untuk menggunakan kunci KMS yang digunakan untuk mengenkripsi snapshot. Untuk informasi selengkapnya, lihat Izinkan organisasi dan OUs menggunakan kunci KMS. Untuk menyiapkan kebijakan utama yang Anda perlukan untuk meluncurkan instans Auto Scaling saat menggunakan kunci terkelola pelanggan untuk enkripsi, lihat AWS KMS key Kebijakan yang diperlukan untuk digunakan dengan volume terenkripsi di Panduan Pengguna Amazon EC2 Auto Scaling.
- Wilayah — AMIs adalah sumber daya Regional. Saat Anda membagikan AMI, AMI hanya tersedia di Wilayah tersebut. Agar AMI tersedia di Wilayah yang berbeda, salin AMI ke Wilayah, lalu bagikan. Untuk informasi selengkapnya, lihat Salin Amazon EC2 AMI.
- Penggunaan – Saat Anda membagikan AMI, pengguna hanya dapat meluncurkan instans dari AMI tersebut. Mereka tidak dapat menghapus, berbagi, atau memodifikasinya. Namun, setelah mereka meluncurkan instans menggunakan AMI Anda, mereka akan dapat membuat AMI dari instans mereka.

- Menyalin bersama AMIs — Jika pengguna di akun lain ingin menyalin AMI bersama, Anda harus memberi mereka izin baca untuk penyimpanan yang mendukung AMI. Untuk informasi selengkapnya, lihat Penyalinan lintas akun.
- Penagihan — Anda tidak ditagih ketika AMI Anda digunakan oleh orang lain Akun AWS untuk meluncurkan instans. Akun yang meluncurkan instans menggunakan AMI akan dikenai biaya untuk instans yang diluncurkan.

Console

Untuk memberikan izin peluncuran eksplisit

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI Anda dalam daftar, lalu pilih Tindakan, Ubah izin AMI.
4. Pilih Privat.
5. Di bawah Akun bersama, pilih Tambahkan ID akun.
6. Untuk Akun AWS ID, masukkan Akun AWS ID yang ingin Anda bagikan AMI, lalu pilih Bagikan AMI.

   Untuk membagikan AMI ini dengan beberapa akun, ulangi Langkah 5 dan 6 hingga Anda telah menambahkan semua akun yang diperlukan IDs.
7. Setelah selesai, pilih Simpan perubahan.
8. (Opsional) Untuk melihat AMI yang telah Anda bagikan, pilih AMI dalam daftar, dan pilih tab Izin. Akun AWS IDs Untuk menemukan AMIs yang dibagikan dengan Anda, lihatTemukan AMI bersama untuk digunakan untuk instans Amazon EC2.

AWS CLI

Gunakan modify-image-attributeperintah untuk berbagi AMI seperti yang ditunjukkan pada contoh berikut.

Untuk memberikan izin peluncuran eksplisit

Contoh berikut memberikan izin peluncuran untuk AMI yang ditentukan ke yang ditentukan. Akun AWS

```
aws ec2 modify-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=123456789012}]"
```

Untuk menghapus izin peluncuran bagi sebuah akun

Contoh berikut menghapus izin peluncuran untuk AMI yang ditentukan dari yang ditentukan Akun AWS.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=123456789012}]"
```

Untuk menghapus semua izin peluncuran

Contoh berikut menghapus semua izin peluncuran publik dan eksplisit dari AMI yang ditentukan. Perhatikan bahwa pemilik AMI selalu memiliki izin peluncuran sehingga tidak terpengaruh oleh perintah ini.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

PowerShell

Gunakan Edit-EC2ImageAttributeperintah (Alat untuk Windows PowerShell) untuk berbagi AMI seperti yang ditunjukkan pada contoh berikut.

Untuk memberikan izin peluncuran eksplisit

Contoh berikut memberikan izin peluncuran untuk AMI yang ditentukan ke yang ditentukan. Akun AWS

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -UserId "123456789012"
```

Untuk menghapus izin peluncuran bagi sebuah akun

Contoh berikut menghapus izin peluncuran untuk AMI yang ditentukan dari yang ditentukan Akun AWS.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission -OperationType remove `
    -UserId "123456789012"
```

Untuk menghapus semua izin peluncuran

Exaple berikut menghapus semua izin peluncuran publik dan eksplisit dari AMI yang ditentukan. Perhatikan bahwa pemilik AMI selalu memiliki izin peluncuran sehingga tidak terpengaruh oleh perintah ini.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Batalkan memiliki AMI yang dibagikan dengan Anda Akun AWS

Amazon Machine Image (AMI) dapat dibagikan dengan Akun AWS spesifik dengan menambahkan akun ke izin peluncuran AMI. Jika AMI telah dibagikan dengan Anda Akun AWS dan Anda tidak ingin lagi dibagikan dengan akun Anda, Anda dapat menghapus akun Anda dari izin peluncuran AMI. Anda melakukan ini dengan menjalankan `cancel-image-launch-permission` AWS CLI perintah. Saat menjalankan perintah ini, Anda akan Akun AWS dihapus dari izin peluncuran untuk AMI yang ditentukan. Untuk menemukan AMIs yang dibagikan dengan Anda Akun AWS, lihatTemukan AMI bersama untuk digunakan untuk instans Amazon EC2.

Anda dapat membatalkan AMI dibagikan dengan akun Anda, misalnya, untuk mengurangi kemungkinan peluncuran instans dengan AMI yang tidak digunakan atau sudah usang yang dibagikan kepada Anda. Saat Anda membatalkan AMI yang dibagikan dengan akun Anda, AMI tidak lagi muncul di daftar AMI apa pun di konsol EC2 atau output describe-images.

Topik

- Batasan
- Membatalkan berbagi AMI dengan akun Anda

Batasan

- Anda dapat menghapus akun Anda dari izin peluncuran AMI yang dibagikan Akun AWS hanya dengan Anda. Anda tidak dapat menggunakan `cancel-image-launch-permission` untuk menghapus akun Anda dari izin peluncuran AMI yang dibagikan dengan organisasi atau unit organisasi (OU) atau untuk menghapus akses ke publik AMIs.
- Anda tidak dapat menghapus akun secara permanen dari izin peluncuran AMI. Pemilik AMI dapat membagikan AMI kepada akun Anda lagi.
- AMIs adalah sumber daya regional. Saat menjalankan `cancel-image-launch-permission`, Anda harus menentukan Wilayah tempat AMI berada. Entah menentukan Region dalam perintah, atau menggunakan variabel AWS_DEFAULT_REGION lingkungan.
- Hanya SDK AWS CLI dan SDK yang mendukung penghapusan akun Anda dari izin peluncuran AMI. Konsol EC2 sekarang tidak mendukung tindakan ini.

Membatalkan berbagi AMI dengan akun Anda

> **Note**
>
> Setelah membatalkan AMI yang dibagikan dengan akun Anda, Anda tidak dapat mengembalikannya. Untuk mendapatkan kembali akses ke AMI, pemilik AMI harus membagikannya dengan akun Anda.

AWS CLI

Untuk membatalkan AMI yang dibagikan dengan akun Anda

Gunakan perintah cancel-image-launch-permission.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0abcdef1234567890 \
    --region us-east-1
```

PowerShell

Untuk membatalkan AMI yang dibagikan dengan akun Anda

Gunakan Stop-EC2ImageLaunchPermissioncmdlet.

```
Stop-EC2ImageLaunchPermission `
    -ImageId ami-0abcdef1234567890 `
    -Region us-east-1
```

Rekomendasi untuk membuat Linux bersama AMIs

Gunakan panduan berikut untuk mengurangi permukaan serangan dan meningkatkan keandalan yang AMIs Anda buat.

> **Important**
>
> Tidak ada daftar pedoman keamanan yang lengkap. Bangun AMIs bersama Anda dengan cermat dan luangkan waktu untuk mempertimbangkan di mana Anda data sensitif Anda terekspos.

Daftar Isi

- Nonaktifkan login jarak jauh berbasis kata sandi untuk pengguna root
- Nonaktifkan akses root lokal
- Hapus pasangan kunci host SSH
- Instal kredensial kunci publik
- Nonaktifkan pemeriksaan DNS sshd (opsional)
- Hapus data sensitif

Jika Anda membangun AMIs AWS Marketplace, lihat Praktik terbaik untuk membangun AMIs di Panduan AWS Marketplace Penjual untuk pedoman, kebijakan, dan praktik terbaik.

Nonaktifkan login jarak jauh berbasis kata sandi untuk pengguna root

Menggunakan kata sandi root tetap untuk AMI publik adalah risiko keamanan yang segera diketahui. Bahkan mengandalkan pengguna untuk mengubah kata sandi setelah masuk pertama membuka jendela kesempatan kecil potensi penyalahgunaan.

Untuk mengatasi masalah ini, nonaktifkan masuk jarak jauh berbasis kata sandi untuk pengguna root.

Untuk menonaktifkan login jarak jauh berbasis kata sandi untuk pengguna root

1. Buka file `/etc/ssh/sshd_config` dengan teks editor dan temukan baris berikut:

   ```
   #PermitRootLogin yes
   ```

2. Ubah baris menjadi:

   ```
   PermitRootLogin without-password
   ```

   Lokasi file konfigurasi ini mungkin berbeda untuk distribusi Anda, atau jika Anda tidak menjalankan OpenSSH. Jika demikian, berkonsultasilah dengan dokumentasi yang relevan.

Nonaktifkan akses root lokal

Saat Anda bekerja dengan shared AMIs, praktik terbaik adalah menonaktifkan login root langsung. Caranya, masuk ke instans yang sedang berjalan dan keluarkan perintah berikut:

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Perintah ini tidak memengaruhi penggunaan `sudo`.

Hapus pasangan kunci host SSH

Jika Anda berencana untuk berbagi AMI yang berasal dari AMI publik, hapus pasangan kunci host SSH yang ada terletak di `/etc/ssh`. Ini memaksa SSH untuk menghasilkan pasangan kunci SSH unik baru ketika seseorang meluncurkan instance menggunakan AMI Anda, meningkatkan keamanan dan mengurangi kemungkinan "" man-in-the-middle serangan.

Hapus semua file kunci berikut yang ada di sistem Anda.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub

- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

Anda dapat menghapus semua file ini dengan aman dengan perintah berikut.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

Warning

Utilitas penghapusan aman seperti shred mungkin tidak menghapus semua salinan file dari media penyimpanan Anda. Salinan file tersembunyi dapat dibuat dengan penjurnalan sistem file (termasuk Amazon Linux default ext4), snapshot, pencadangan, RAID, dan cache sementara. Untuk informasi lebih lanjut, lihat dokumentasi yang rusak.

Important

Jika Anda lupa menghapus pasangan kunci host SSH yang ada dari AMI publik, proses audit rutin kami memberi tahu Anda dan semua pelanggan yang menjalankan instans AMI Anda tentang potensi risiko keamanan. Setelah masa tenggang singkat, kami menandai AMI sebagai privat.

Instal kredensial kunci publik

Setelah mengonfigurasi AMI untuk mencegah masuk menggunakan kata sandi, Anda harus memastikan pengguna dapat masuk menggunakan mekanisme lain.

Amazon EC2 memungkinkan pengguna untuk menentukan nama pasangan kunci publik-privat saat meluncurkan sebuah instans. Saat nama pasangan kunci yang valid diberikan ke panggilan API `RunInstances` (atau melalui alat API baris perintah), kunci publik (bagian dari pasangan kunci yang

dimiliki Amazon EC2 di server setelah panggilan `CreateKeyPair` atau `ImportKeyPair`) tersedia untuk instans melalui kueri HTTP terhadap metadata instans.

Untuk masuk melalui SSH, AMI Anda harus mengambil nilai kunci saat boot dan menambahkannya ke `/root/.ssh/authorized_keys` (atau setara untuk akun pengguna lain di AMI). Pengguna dapat meluncurkan instans AMI Anda dengan pasangan kunci dan masuk tanpa yang memerlukan kata sandi root.

Banyak distribusi, termasuk Amazon Linux dan Ubuntu, menggunakan paket `cloud-init` untuk menginjeksikan kredensial kunci publik untuk pengguna yang telah dikonfigurasi. Jika distribusi Anda tidak mendukung `cloud-init`, Anda dapat menambahkan kode berikut ke skrip penyalaan sistem (seperti `/etc/rc.local`) untuk menarik kunci publik yang Anda tentukan pada saat peluncuran untuk pengguna root.

> **Note**
>
> Dalam contoh berikut, alamat IP http://169.254.169.254/ adalah alamat tautan lokal dan hanya valid dari instans.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
```

```
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Hal ini dapat diterapkan ke pengguna; Anda tidak perlu membatasinya ke pengguna `root`.

> **Note**
>
> Pemaketan ulang instans berdasarkan AMI ini mencakup kunci yang digunakan untuk meluncurkan. Untuk mencegah inklusi kunci, Anda harus membersihkan (atau menghapus) file `authorized_keys` atau mengecualikan file ini dari pemaketan ulang.

Nonaktifkan pemeriksaan DNS sshd (opsional)

Menonaktifkan pemeriksaan DNS sshd akan sedikit melemahkan keamanan sshd. Namun, jika resolusi DNS gagal, login SSH masih berfungsi. Jika Anda tidak menonaktifkan pemeriksaan sshd, kegagalan resolusi DNS akan mencegah semua login.

Untuk menonaktifkan pemeriksaan DNS sshd

1. Buka file `/etc/ssh/sshd_config` dengan editor teks dan cari baris berikut:

   ```
   #UseDNS yes
   ```

2. Ubah baris menjadi:

   ```
   UseDNS no
   ```

> **Note**
>
> Lokasi file konfigurasi ini mungkin berbeda untuk distribusi Anda, atau jika Anda tidak menjalankan OpenSSH. Jika demikian, berkonsultasilah dengan dokumentasi yang relevan.

Hapus data sensitif

Kami tidak sarankan Anda menyimpan data atau perangkat lunak sensitif di AMI apa pun yang Anda bagikan. Pengguna yang meluncurkan AMI bersama mungkin dapat memaketkannya kembali dan mendaftarkannya sebagai milik mereka sendiri. Ikuti panduan ini untuk membantu Anda menghindari beberapa risiko keamanan yang mudah diabaikan:

- Kami menyarankan penggunaan opsi `--exclude` *`directory`* pada `ec2-bundle-vol` untuk melewati direktori dan subdirektori yang berisi informasi rahasia yang tidak ingin Anda sertakan dalam paketan Anda. Secara khusus, kecualikan semua pasangan public/private kunci SSH milik pengguna dan `authorized_keys` file SSH saat menggabungkan gambar. Publik Amazon AMIs menyimpan ini `/root/.ssh` untuk pengguna root, dan `/home/`*`user_name`*`/.ssh/` untuk pengguna biasa. Untuk informasi selengkapnya, lihat ec2-bundle-vol.
- Selalu hapus riwayat shell sebelum pembuatan paketan. Jika Anda mencoba lebih dari satu unggahan paketan di AMI yang sama, riwayat shell berisi kunci akses Anda. Contoh berikut harus menjadi perintah terakhir yang Anda jalankan sebelum memaketkan dari dalam instans.

```
[ec2-user ~]$ shred -u ~/.*history
```

> **Warning**
>
> Batasan shred yang dijelaskan dalam peringatan di atas berlaku juga di sini.
> Perhatikan bahwa bash mencatat riwayat sesi saat ini ke disk saat keluar. Jika Anda keluar dari instans setelah menghapus `~/.bash_history`, lalu masuk kembali, Anda akan menemukan `~/.bash_history` telah dibuat ulang dan berisi semua perintah yang dijalankan selama sesi Anda sebelumnya.
> Program lain selain bash juga menulis riwayat ke disk, berhati-hatilah dan hapus atau kecualikan dot-file dan dot-directories yang tidak perlu.

- Membuat paketan dari instans berjalan memerlukan kunci privat dan sertifikat X.509 Anda. Simpan kredensial ini dan kredensial lainnya di lokasi yang tidak dipaketkan (misalnya penyimpanan instans).

Pantau peristiwa AMI menggunakan Amazon EventBridge

Ketika status Amazon Machine Image (AMI) berubah, Amazon EC2 menghasilkan peristiwa yang dikirim ke Amazon EventBridge (sebelumnya dikenal sebagai Amazon CloudWatch Events). Acara dikirim ke bus EventBridge acara default dalam format JSON. Anda dapat menggunakan Amazon EventBridge untuk mendeteksi dan bereaksi terhadap peristiwa ini. Anda melakukan ini dengan membuat aturan EventBridge yang memicu tindakan sebagai respons terhadap suatu peristiwa. Misalnya, Anda dapat membuat EventBridge aturan yang mendeteksi kapan proses pembuatan AMI telah selesai dan kemudian memanggil topik Amazon SNS untuk mengirim pemberitahuan email kepada Anda.

Amazon EC2 menghasilkan `EC2 AMI State Change` peristiwa ketika AMI memasuki salah satu status berikut:

- `available`
- `failed`
- `deregistered`
- `disabled`

Peristiwa dihasilkan atas dasar upaya terbaik.

Tabel berikut ini mencantumkan operasi dan status AMI yang dapat dimasuki oleh AMI. Dalam tabel, Ya menunjukkan status yang dapat dimasuki AMI ketika operasi yang sesuai berjalan.

Operasi AMI	available	failed	deregistered	disabled
CopyImage	Ya	Ya		
CreateImage	Ya	Ya		
CreateRestoreImageTask	Ya	Ya		

Operasi AMI	available	failed	deregistered	disabled
DeregisterImage			Ya	
DisableImage				Ya
EnableImage	Ya			
RegisterImage	Ya	Ya		

Peristiwa EC2 AMI State Change

- Detail peristiwa
- Peristiwa available
- Peristiwa failed
- Peristiwa deregistered
- Peristiwa disabled

Detail peristiwa

Anda dapat menggunakan bidang berikut dalam acara untuk membuat aturan yang memicu tindakan:

`"source": "aws.ec2"`

Mengidentifikasi bahwa acara tersebut berasal dari Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Mengidentifikasi nama peristiwa.

`"detail": { "ImageId": "ami-0abcdef1234567890", "State": "available", }`

Menyediakan ID AMI dan status AMI (`available`,`failed`,`deregistered`, atau`disabled`).

Untuk informasi selengkapnya, lihat berikut ini di Panduan EventBridge Pengguna Amazon:

- EventBridge Acara Amazon
- Pola EventBridge acara Amazon

- EventBridge Aturan Amazon

Untuk tutorial tentang cara membuat fungsi Lambda dan EventBridge aturan yang menjalankan fungsi Lambda, lihat Tutorial: Log status EC2 instance Amazon menggunakan EventBridge dalam Panduan Pengembang.AWS Lambda

Peristiwa available

Berikut ini adalah contoh peristiwa yang EC2 dihasilkan Amazon ketika AMI memasuki `available` status setelah berhasil`CreateImage`,,`CopyImage`, `RegisterImage``CreateRestoreImageTask`, atau `EnableImage` operasi.

`"State": "available"` menunjukkan bahwa operasi berhasil.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

Peristiwa failed

Berikut ini adalah contoh peristiwa yang EC2 dihasilkan Amazon saat AMI memasuki `failed` status setelah gagal`CreateImage`, `CopyImage``RegisterImage`, atau `CreateRestoreImageTask` operasi.

Bidang berikut memberikan informasi terkait:

- `"State": "failed"` – Menunjukkan bahwa operasi gagal.
- `"ErrorMessage": ""` – Memberikan alasan kegagalan operasi.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "failed",
        "ErrorMessage": "Description of failure"
    }
}
```

Peristiwa deregistered

Berikut ini adalah contoh peristiwa yang EC2 dihasilkan Amazon ketika AMI memasuki `deregistered` status setelah `DeregisterImage` operasi berhasil. Jika operasi gagal, tidak ada peristiwa yang dihasilkan. Kegagalan diketahui segera karena `DeregisterImage` merupakan operasi tersinkron.

`"State": "deregistered"` menunjukkan bahwa operasi `DeregisterImage` berhasil.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

Peristiwa disabled

Berikut ini adalah contoh peristiwa yang EC2 dihasilkan Amazon ketika AMI memasuki `disabled` status setelah `DisableImage` operasi berhasil. Jika operasi gagal, tidak ada peristiwa yang dihasilkan. Kegagalan diketahui segera karena `DisableImage` merupakan operasi tersinkron.

`"State": "disabled"` menunjukkan bahwa operasi `DisableImage` berhasil.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "disabled",
        "ErrorMessage": ""
    }
}
```

Memahami informasi penagihan AMI

Ada banyak Amazon Machine Images (AMIs) untuk dipilih saat meluncurkan instans Anda, dan mereka mendukung berbagai platform dan fitur sistem operasi. Untuk memahami bagaimana AMI yang Anda pilih saat meluncurkan instans memengaruhi garis bawah AWS tagihan Anda, Anda dapat meneliti platform sistem operasi terkait dan informasi penagihan. Lakukan ini sebelum Anda meluncurkan instans On-Demand atau Instans Spot, atau membeli Instans Cadangan.

Berikut adalah dua contoh bagaimana meneliti AMI Anda sebelumnya dapat membantu Anda memilih AMI yang paling sesuai dengan kebutuhan Anda:

- Untuk Instans Spot, Anda dapat menggunakan Detail platform AMI untuk mengonfirmasi bahwa AMI didukung untuk Instans Spot.
- Saat membeli Instans Cadangan, Anda dapat memastikan bahwa, Anda memilih platform sistem operasi (Platform), yang memetakan Detail platform pada AMI.

Untuk informasi selengkapnya tentang harga instans, lihat EC2 harga Amazon.

Daftar Isi

- Bidang informasi penagihan AMI
- Mencari detail penagihan dan penggunaan AMI
- Memverifikasi biaya AMI pada tagihan Anda

Bidang informasi penagihan AMI

Bidang berikut menyediakan informasi penagihan yang terkait dengan AMI:

Detail platform AMI

Detail platform yang terkait akan dengan kode penagihan AMI. Sebagai contoh, `Red Hat Enterprise Linux`.

Operasi penggunaan

Pengoperasian EC2 instans Amazon dan kode penagihan yang terkait dengan AMI. Misalnya, `RunInstances:0010`. Operasi penggunaan sesuai dengan kolom LineItem/Operation pada Laporan AWS Biaya dan Penggunaan (CUR) Anda dan di API Daftar Harga.AWS

Anda dapat melihat bidang ini di Instans atau AMIshalaman di EC2 konsol Amazon, atau dalam respons yang ditampilkan oleh gambar-deskripsi atau perintah. Get-EC2Image

Contoh data: operasi penggunaan berdasarkan platform

Tabel berikut mencantumkan beberapa detail platform dan nilai operasi penggunaan yang dapat ditampilkan di Instans atau AMIshalaman di EC2 konsol Amazon, atau dalam respons yang ditampilkan oleh gambar-gambar atau perintah. Get-EC2Image

Detail platform	Operasi penggunaan [2]
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0[3]

Detail platform	Operasi penggunaan [2]
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise[1]	RunInstances:0102

Detail platform	Operasi penggunaan [2]
Windows with SQL Server Standard[1]	RunInstances:0006
Windows with SQL Server Web[1]	RunInstances:0202

[1] Jika dua lisensi perangkat lunak dikaitkan dengan AMI, bidang detail Platform menunjukkan keduanya.

[2] Jika Anda menjalankan Instans Spot, lineitem/Operationpada Laporan AWS Biaya dan Penggunaan Anda mungkin berbeda dari nilai operasi Penggunaan yang tercantum di sini. Misalnya, jika `lineitem/Operation` ditampilkan`RunInstances:0010:SV006`, itu berarti Amazon EC2 menjalankan Red Hat Enterprise Linux Spot Instance-hour di US East (Virginia N.) di Zona 6.

[3] Ini muncul seperti RunInstances (Linux/UNIX) dalam laporan penggunaan Anda.

Mencari detail penagihan dan penggunaan AMI

Properti berikut dapat membantu Anda memverifikasi biaya AMI pada tagihan Anda:

- Detail platform
- Operasi penggunaan
- ID AMI

Console

Untuk menemukan informasi penagihan AMI untuk AMI

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI.
4. Pada tab Detail, temukan Detail platform dan operasi Penggunaan.

Untuk menemukan informasi penagihan AMI untuk sebuah instans

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.

2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pada tab Detail, perluas detail Instans dan temukan detail Platform dan operasi Penggunaan.

AWS CLI

Untuk menemukan informasi penagihan AMI untuk AMI

Gunakan perintah describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query "Images[].
{PlatformDetails:PlatformDetails,UsageOperation:UsageOperation}"
```

Berikut ini adalah contoh output untuk AMI Linux.

```
[
    {
        "PlatformDetails": "Linux/UNIX",
        "UsageOperation": "RunInstances"
    }
]
```

Untuk menemukan informasi penagihan AMI untuk sebuah instans

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].
{PlatformDetails:PlatformDetails,UsageOperation:UsageOperation}"
```

Berikut ini adalah contoh output untuk instance Windows.

```
[
    {
        "PlatformDetails": "Windows",
        "UsageOperation": "RunInstances:0002"
    }
```

```
]
```

PowerShell

Untuk menemukan informasi penagihan AMI untuk AMI

Gunakan Get-EC2Imagecmdlet.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Format-List PlatformDetails, UsageOperation
```

Berikut ini adalah contoh output untuk AMI Linux.

```
PlatformDetails : Linux/UNIX
UsageOperation  : RunInstances
```

Untuk menemukan informasi penagihan AMI untuk sebuah instans

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances | `
    Format-List PlatformDetails, UsageOperation
```

Berikut ini adalah contoh output untuk instance Windows.

```
PlatformDetails : Windows
UsageOperation  : RunInstances:0002
```

Memverifikasi biaya AMI pada tagihan Anda

Untuk memastikan bahwa Anda tidak menimbulkan biaya yang tidak direncanakan, Anda dapat memverifikasi bahwa informasi penagihan untuk instans dalam Laporan AWS Biaya dan Penggunaan (CUR) cocok dengan informasi penagihan yang terkait dengan AMI yang Anda gunakan untuk meluncurkan instans.

Untuk memverifikasi informasi penagihan, temukan ID instans di CUR Anda dan periksa nilai yang sesuai di kolom `lineitem/Operation`. Nilai harus sesuai dengan nilai untuk Operasi penggunaan yang berkaitan dengan AMI.

Sebagai contoh, `ami-0123456789EXAMPLE` AMI memiliki informasi penagihan berikut:

- Detail platform = `Red Hat Enterprise Linux`
- Operasi penggunaan = `RunInstances:0010`

Jika Anda meluncurkan instans menggunakan AMI ini, Anda dapat mencari ID instans di CUR dan memeriksa nilai yang sesuai di kolom `lineitem/Operation`. Dalam contoh ini, nilainya harus berupa `RunInstances:0010`.

Kuota AMI di Amazon EC2

Kuota berikut berlaku untuk membuat dan berbagi AMIs. Kuota berlaku per AWS Region.

Nama kuota	Deskripsi	Kuota default per Wilayah
AMIs	Jumlah maksimum publik dan swasta yang AMIs diizinkan per Wilayah. Ini termasuk tersedia, tertunda, dan dinonaktifkan AMIs, dan AMIs di Recycle Bin.	50.000
Publik AMIs	Jumlah maksimum publik AMIs, termasuk publik AMIs di Recycle Bin, diperbolehkan per Wilayah.	5
Berbagi AMI	Jumlah maksimum entitas (organisasi, unit organisasi (OUs), dan akun) yang dapat dibagikan AMI di Wilayah. Perhatikan bahwa jika Anda berbagi AMI dengan organisasi atau OU, jumlah akun dalam organisasi atau OU tidak dihitung dalam kuota.	1.000

Jika Anda melebihi kuota dan ingin membuat atau berbagi lebih banyak AMIs, Anda dapat melakukan hal berikut:

- Jika Anda melebihi total AMIs atau AMIs kuota publik, pertimbangkan untuk membatalkan pendaftaran gambar yang tidak digunakan.
- Jika Anda melebihi AMIs kuota publik Anda, pertimbangkan untuk membuat satu atau lebih publik AMIs pribadi.
- Jika Anda melebihi kuota berbagi AMI, pertimbangkan untuk berbagi AMIs dengan organisasi atau OU, bukan akun terpisah.
- Minta kenaikan kuota untuk AMIs.

Minta kenaikan kuota untuk AMIs

Jika Anda membutuhkan lebih dari kuota default AMIs, Anda dapat meminta kenaikan kuota.

Untuk meminta kenaikan kuota untuk AMIs

1. Buka konsol Service Quotas di https://console.aws.amazon.com/servicequotas/.
2. Di panel navigasi, pilih Layanan AWS .
3. Pilih Amazon Elastic Compute Cloud (Amazon EC2) dari daftar, atau ketik nama layanan di kotak pencarian.
4. Pilih kuota AMI untuk meminta kenaikan. Kuota AMI yang dapat Anda pilih adalah:
   - AMIs
   - Publik AMIs
   - Berbagi AMI
5. Pilih Ajukan peningkatan kuota.
6. Untuk Mengubah nilai kuota, masukkan nilai kuota yang baru, lalu pilih Ajukan.

Untuk melihat permintaan yang tertunda atau baru diselesaikan, pilih Dasbor dari panel navigasi. Untuk permintaan yang tertunda, pilih status permintaan untuk membuka penerimaan permintaan. Status awal dari permintaan adalah Tertunda. Setelah status berubah menjadi Kuota yang diminta, Anda akan melihat nomor kasus di bagian Nomor kasus Pusat Dukungan. Pilih nomor kasus untuk membuka tiket untuk permintaan Anda.

Setelah permintaan diselesaikan, Nilai kuota yang diterapkan untuk kuota tersebut diatur ke nilai baru.

Untuk informasi lebih lanjut, lihat Panduan Pengguna Kuota Layanan.

Instans Amazon EC2

Instans Amazon EC2 adalah server virtual di lingkungan AWS cloud. Anda memiliki kontrol penuh atas instans Anda, dari saat Anda pertama kali memulainya (disebut sebagai meluncurkan instance) hingga Anda menghapusnya (disebut sebagai mengakhiri instance). Anda dapat memilih dari berbagai sistem operasi saat meluncurkan instans Anda. Anda dapat terhubung ke instans Anda dan menyesuaikannya untuk memenuhi kebutuhan Anda. Misalnya, Anda dapat mengonfigurasi sistem operasi, menginstal pembaruan sistem operasi, dan menginstal aplikasi pada instans Anda.

Amazon EC2 menyediakan berbagai jenis instans. Anda dapat memilih jenis instans yang menyediakan sumber daya komputasi, memori, penyimpanan, dan kinerja jaringan yang Anda perlukan untuk menjalankan aplikasi Anda.

Dengan Amazon EC2, Anda hanya membayar untuk apa yang Anda gunakan. Penagihan untuk instans Anda dimulai saat Anda meluncurkan instans Anda dan transisi ke status berjalan. Penagihan berhenti ketika Anda menghentikan instans Anda dan dilanjutkan ketika Anda memulai instans Anda. Saat Anda menghentikan instans, penagihan berhenti saat transisi ke status mematikan.

Amazon EC2 menyediakan fitur yang dapat Anda gunakan untuk mengoptimalkan kinerja dan biaya instans Anda. Misalnya, Anda dapat menggunakan Amazon EC2 Fleet atau Amazon EC2 Auto Scaling untuk meningkatkan atau menurunkan kapasitas saat penggunaan instans Anda berubah. Anda dapat mengurangi biaya untuk instans Anda menggunakan Instans Spot atau Savings Plans.

Instans terkelola dikelola oleh penyedia layanan, seperti Amazon EKS Auto Mode. Anda tidak dapat langsung mengubah pengaturan instans terkelola. Instans terkelola diidentifikasi oleh nilai sebenarnya di bidang Dikelola. Untuk informasi selengkapnya, lihat Instans terkelola Amazon EC2.

Fitur dan tugas

- Tipe instans Amazon EC2
- Instans terkelola Amazon EC2
- Gunakan virtualisasi bersarang untuk menjalankan hypervisor di instans Amazon EC2
- Opsi penagihan dan pembelian Amazon EC2
- Simpan parameter peluncuran instans di templat peluncuran Amazon EC2
- Luncurkan instans Amazon EC2
- Connect ke instans EC2
- Perubahan status EC2 instans Amazon

- Pemulihan instans otomatis
- Gunakan metadata instans untuk mengelola instans EC2
- Mendeteksi apakah host adalah sebuah EC2 instance
- Dokumen identitas instans untuk EC2 instans Amazon
- Kepatuhan STIG untuk instans Anda EC2
- Jam presisi dan sinkronisasi waktu pada instans EC2 Anda
- Manajer Kapasitas EC2
- Mengelola driver perangkat untuk instans EC2 Anda
- Konfigurasikan instans Windows Amazon EC2 Anda
- Tingkatkan instans EC2 Windows ke versi Windows Server yang lebih baru
- Tutorial: Hubungkan instans Amazon EC2 ke basis data Amazon RDS

Tipe instans Amazon EC2

Saat meluncurkan sebuah instans, tipe instans yang Anda pilih menentukan perangkat keras komputer host yang digunakan untuk instans Anda. Setiap tipe instans menawarkan kemampuan komputasi, memori, dan penyimpanan yang berbeda, serta dikelompokkan dalam sebuah keluarga instans berdasarkan kemampuan tersebut. Pilih tipe instans berdasarkan persyaratan aplikasi atau perangkat lunak yang rencananya akan Anda jalankan pada instans Anda. Untuk informasi selengkapnya tentang fitur dan kasus penggunaan, lihat Jenis Instans Amazon EC2.

Amazon EC2 mengkhususkan beberapa sumber daya komputer host, seperti CPU, memori, dan penyimpanan instans, untuk instans tertentu. Amazon EC2 berbagi sumber daya lain dari komputer host, seperti jaringan dan subsistem disk, antarinstans. Jika setiap instans pada komputer host mencoba menggunakan sebanyak mungkin salah satu sumber daya bersama ini, masing-masing menerima bagian yang sama dari sumber daya tersebut. Namun, jika sumber daya kurang digunakan, sebuah instans dapat menggunakan bagian yang lebih tinggi dari sumber daya tersebut selama tersedia.

Setiap tipe instans memberikan performa minimum yang lebih tinggi atau lebih rendah dari sumber daya bersama. Misalnya, tipe instance dengan I/O kinerja tinggi memiliki alokasi sumber daya bersama yang lebih besar. Mengalokasikan bagian yang lebih besar dari sumber daya bersama juga mengurangi varians kinerja. I/O Untuk sebagian besar aplikasi, I/O kinerja moderat lebih dari cukup. Namun, untuk aplikasi yang membutuhkan I/O kinerja yang lebih besar atau lebih konsisten, pertimbangkan jenis instance dengan I/O kinerja yang lebih tinggi.

Daftar Isi

- Tipe instans yang tersedia
- Spesifikasi perangkat keras
- Jenis hypervisor
- Tipe virtualisasi AMI
- Prosesor
- Temukan jenis EC2 instans Amazon
- Dapatkan rekomendasi dari pencari tipe instans EC2
- Dapatkan rekomendasi EC2 instans dari Compute Optimizer
- Perubahan jenis instans Amazon EC2
- Instance performa yang dapat melonjak
- Akselerasi kinerja dengan instans GPU
- Instans Mac Amazon EC2
- Jenis instans Amazon EBS yang dioptimalkan
- Opsi CPU untuk instans Amazon EC2
- AMD SEV-SNP untuk instans Amazon EC2
- Kontrol status prosesor untuk instans Amazon EC2 Linux

Tipe instans yang tersedia

Amazon EC2 menyediakan berbagai pilihan tipe instans yang dioptimalkan agar sesuai dengan berbagai kasus penggunaan. Tipe instans terdiri dari berbagai kombinasi CPU, memori, penyimpanan, dan kapasitas jaringan, serta memberi Anda fleksibilitas untuk memilih campuran sumber daya yang sesuai untuk aplikasi Anda. Setiap tipe instans menyertakan satu atau beberapa ukuran instans, memungkinkan Anda untuk menskalakan sumber daya sesuai dengan persyaratan beban kerja target Anda.

Konvensi penamaan tipe instans

Nama didasarkan pada keluarga instance, generasi, keluarga prosesor, kemampuan, dan ukuran. Untuk informasi selengkapnya, lihat Konvensi penamaan di Panduan Jenis Instans Amazon EC2.

Menemukan tipe instans

Untuk menentukan jenis instans mana yang memenuhi persyaratan Anda, seperti Wilayah yang didukung, sumber daya komputasi, atau sumber daya penyimpanan, lihat Temukan jenis EC2 instans Amazon serta spesifikasi jenis instans Amazon EC2 di Panduan Jenis Instans Amazon EC2.

Spesifikasi perangkat keras

Untuk spesifikasi tipe instans yang mendetail, lihat Spesifikasi di Panduan Jenis Instans Amazon EC2. Untuk informasi harga, lihat Harga Sesuai Permintaan Amazon EC2.

Untuk menentukan tipe instans yang paling sesuai dengan kebutuhan Anda, kami menyarankan Anda meluncurkan sebuah instans dan menggunakan aplikasi tolok ukur Anda sendiri. Karena Anda membayar dengan basis per detik instans, akan lebih mudah dan murah untuk menguji banyak tipe instans sebelum membuat keputusan. Jika kebutuhan berubah, bahkan setelah membuat keputusan, Anda dapat mengubah tipe instans nanti. Untuk informasi selengkapnya, lihat Perubahan jenis instans Amazon EC2.

Jenis hypervisor

Amazon EC2 mendukung hypervisor berikut: Xen dan Nitro.

Contoh berbasis nitro

- Tujuan umum: M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6iD | M6idn | M6in | M7a | M7g | M7gd | M7i | M7i-flex | M8a | M8AZn | M8g | m8gb | m8gd | m8gn | m8i | m8id | M8i-flex | T3 | T3a | T4G
- Komputasi dioptimalkan: C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gD | C6gN | C6i | C6iD | C6in | C7a | C7g | C7gD | C7gN | C7i | C7i-flex | C8a | C8g | C8gB | C8gB | C8gB | C8gB d | C8gN | C8i | C8id | C8i-Flex
- Memori dioptimalkan: R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6iD | R6idn | R6in | R7a | R7g | R7gd | R7i | R7iZ | R8a | R8g | R8gb | R8gd | R8gn | R8i | R8iD | R8i-flex | U-3tb1 | U-6TB1 | U-9tb1 | U-12tb1 | U-18tb1 | U-24tb1 | U7i-6tb | U7i-8tb | U7i-12tb | U7in-16tb | U7in-24tb | U7in-32tb | U7inh-32tb | U7inh-32tb | U7inh-32tb tB | x2gd | x2idn | x2iEDN | x2IEZN | x8g | x8AEDZ | x8i | z1d
- Penyimpanan dioptimalkan: D3 | D3en | i3en | i4G | i4i | i7i | i7ie | i8g | i8GE | iM4GN | IS4gen
- Komputasi dipercepat: DL1 | DL2q | F2 | G4ad | G4dn | G5 | G5g | G6 | G6e | G6f | Gr6 | GR6f | G7e | Inf1 | Inf2 | P4d | P4de | P5 | P5e | P5en | P6-B200 | P6-B300 | P6e- | Trn1 | Trn1n | Trn2 | Trn2u | GB200 VT1
- Komputasi kinerja tinggi: HPC6a | hPC6id | hPC7a | hPC7g | hPC8a

- Generasi sebelumnya: A1 | P3dn

Untuk informasi selengkapnya tentang versi Nitro hypervisor yang didukung, lihat Dukungan fitur jaringan di Panduan Jenis Instans Amazon EC2.

Contoh berbasis Xen

- Tujuan umum: M1 | M2 | M3 | M4 | T1 | T2
- Komputasi dioptimalkan: C1 | C3 | C4
- Memori dioptimalkan: R3 | R4 | X1 | X1e
- Penyimpanan dioptimalkan: D2 | H1 | I2 | I3
- Komputasi yang dipercepat: F1 | G3 | P2 | P3

Tipe virtualisasi AMI

Tipe virtualisasi instans Anda ditentukan oleh AMI yang Anda gunakan untuk meluncurkannya. Tipe instans generasi saat ini hanya mendukung mesin virtual perangkat keras (HVM). Beberapa jenis instans generasi sebelumnya mendukung paravirtual (PV) dan beberapa AWS Wilayah mendukung instance PV. Untuk informasi selengkapnya, lihat Tipe virtualisasi.

Untuk mendapatkan performa terbaik, kami menyarankan Anda menggunakan AMI HVM. Selain itu, HVM AMIs diperlukan untuk memanfaatkan jaringan yang disempurnakan. Virtualisasi HVM menggunakan teknologi hardware-assist yang disediakan oleh platform. AWS Dengan virtualisasi HVM, VM tamu berjalan seolah-olah berada di platform perangkat keras native, hanya saja VM tersebut masih menggunakan jaringan PV dan driver penyimpanan untuk meningkatkan performanya.

Prosesor

Instans EC2 mendukung berbagai prosesor.

Prosesor

- Prosesor Intel
- Prosesor AMD
- AWS Prosesor Graviton
- AWS Trainium

- AWS Inferensia

Prosesor Intel

Instans Amazon EC2 yang berjalan pada prosesor Intel mungkin menyertakan fitur prosesor berikut. Tidak semua instance yang berjalan pada prosesor Intel mendukung semua fitur prosesor ini. Untuk informasi tentang fitur yang tersedia untuk setiap jenis instans, lihat Jenis Instans Amazon EC2.

- Instruksi Baru Intel AES (AES-NI) — Kumpulan instruksi enkripsi Intel AES-NI melakukan peningkatan berdasarkan algoritma Advanced Encryption Standard (AES) asli untuk memberikan perlindungan data yang lebih cepat dan keamanan yang lebih kuat. Semua instans EC2 generasi saat ini mendukung fitur prosesor ini.
- Intel Advanced Vector Extensions (Intel AVX, Intel AVX2, dan Intel AVX-512) — Intel AVX dan Intel berukuran 256-bit, dan Intel AVX-512 AVX2 adalah ekstensi set instruksi 512-bit yang dirancang untuk aplikasi yang intensif Floating Point (FP). Instruksi Intel AVX meningkatkan kinerja untuk aplikasi seperti gambar dan audio/video pemrosesan, simulasi ilmiah, analitik keuangan, serta pemodelan dan analisis 3D. Fitur-fitur ini hanya tersedia pada instans yang diluncurkan dengan AMIs HVM.
- Teknologi Intel Turbo Boost — Prosesor Intel Turbo Boost Technology secara otomatis menjalankan inti lebih cepat dari frekuensi operasi dasar.
- Intel Deep Learning Boost (Intel DL Boost) — Mempercepat kasus penggunaan AI deep learning. Prosesor Intel Xeon Scalable Generasi ke-2 memperluas Intel AVX-512 dengan Instruksi Jaringan Neural Vektor baru (VNNI/INT8) that significantly increases deep learning inference performance over previous generation Intel Xeon Scalable processors (with FP32) for image recognition/segmentation, deteksi objek, pengenalan suara, terjemahan bahasa, sistem rekomendasi, pembelajaran penguatan, dan banyak lagi. VNNI mungkin tidak kompatibel dengan semua distribusi Linux.

  Instans berikut mendukung VNNI: `M5n`, `R5n`, `M5dn`, `M5zn`, `R5b`, `R5dn`, `D3`, `D3en`, dan `C6i`. Instans `C5` dan `C5d` mendukung VNNI hanya untuk instans `12xlarge`, `24xlarge`, dan `metal`.

Kebingungan dapat dihasilkan dari konvensi penamaan industri untuk 64-bit. CPUs Produsen chip Advanced Micro Devices (AMD) memperkenalkan arsitektur 64-bit pertama yang sukses secara komersial berbasis set instruksi Intel x86. Akibatnya, arsitektur secara luas disebut sebagai AMD64 terlepas dari produsen chip. Windows dan beberapa distribusi Linux mengikuti praktik ini. Ini menjelaskan mengapa informasi sistem internal pada instance yang menjalankan Ubuntu atau

Windows menampilkan arsitektur CPU seolah-olah instance berjalan pada perangkat keras Intel. AMD64

Prosesor AMD

Instans Amazon EC2 yang berjalan pada prosesor AMD EPYC dapat membantu Anda mengoptimalkan biaya dan kinerja untuk beban kerja Anda. Contoh ini mungkin mendukung fitur prosesor berikut. Tidak semua instance yang berjalan pada prosesor AMD mendukung semua fitur prosesor ini. Untuk informasi tentang fitur yang tersedia untuk setiap jenis instans, lihat Jenis Instans Amazon EC2.

- Enkripsi Memori Aman AMD (UKM)
- Enkripsi Memori Kunci Tunggal Transparan AMD (TSME)
- Ekstensi Vektor Tingkat Lanjut AMD (AVX)
- AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP)
- Instruksi Jaringan Saraf Vektor (VNNI)
- BFloat16

AWS Prosesor Graviton

AWS Graviton adalah rangkaian prosesor yang dirancang untuk memberikan kinerja harga terbaik untuk beban kerja Anda yang berjalan di instans Amazon EC2.

Untuk informasi lebih lanjut, lihat Memulai dengan Graviton.

AWS Trainium

Instans yang didukung oleh AWS Trainium dibuat khusus untuk pelatihan pembelajaran mendalam yang berkinerja tinggi dan hemat biaya. Anda dapat menggunakan contoh ini untuk melatih pemrosesan bahasa alami, visi komputer, dan model pemberi rekomendasi yang digunakan di serangkaian aplikasi yang luas, seperti pengenalan suara, rekomendasi, deteksi penipuan, dan klasifikasi gambar dan video. Gunakan alur kerja Anda yang ada dalam kerangka kerja ML populer, seperti PyTorch dan. TensorFlow

AWS Inferensia

Instans yang didukung oleh AWS Inferentia dirancang untuk mempercepat pembelajaran mesin. Mereka memberikan inferensi pembelajaran mesin berkinerja tinggi dan latensi rendah. Instans ini

dioptimalkan untuk menerapkan model deep learning (DL) untuk aplikasi, seperti pemrosesan bahasa alami, deteksi dan klasifikasi objek, personalisasi dan pemfilteran konten, dan pengenalan ucapan.

Ada berbagai cara untuk memulai:

- Gunakan SageMaker AI, layanan yang dikelola sepenuhnya yang merupakan cara termudah untuk memulai dengan model pembelajaran mesin. Untuk informasi selengkapnya, lihat SageMaker Memulai AI di Panduan Pengembang Amazon SageMaker AI.
- Luncurkan instans Inf1 atau Inf2 menggunakan AMI Deep Learning. Untuk informasi selengkapnya, lihat AWS Inferentia dengan DLAMI di Panduan Developer AWS Deep Learning AMIs .
- Luncurkan instans Inf1 atau Inf2 menggunakan AMI Anda sendiri dan instal AWS Neuron SDK, yang memungkinkan Anda untuk mengompilasi, menjalankan, dan membuat profil model deep learning untuk AWS Inferentia.
- Luncurkan instans kontainer menggunakan instans Inf1 atau Inf2 dan AMI yang dioptimalkan Amazon ECS. Untuk informasi selengkapnya, lihat Amazon Linux 2 (Inferentia) AMIs di Panduan Pengembang Layanan Amazon Elastic Container.
- Buat klaster Amazon EKS dengan simpul yang menjalankan instans Inf1. Untuk informasi selengkapnya, lihat dukungan Inferentia di Panduan Pengguna Amazon EKS.

Temukan jenis EC2 instans Amazon

Sebelum dapat meluncurkan sebuah instans, Anda harus memilih tipe instans yang akan digunakan. Tipe instans yang Anda pilih mungkin bergantung pada sumber daya yang dibutuhkan oleh beban kerja Anda, seperti sumber daya komputasi, memori, atau penyimpanan. Akan bermanfaat untuk mengidentifikasi beberapa tipe instans yang mungkin sesuai dengan beban kerja Anda dan mengevaluasi kinerjanya di lingkungan pengujian. Tidak ada pengganti untuk mengukur performa aplikasi Anda di bawah beban.

Anda bisa mendapatkan saran dan panduan untuk jenis EC2 instance menggunakan pencari tipe EC2 instance. Untuk informasi selengkapnya, lihat the section called “Pencari jenis instans EC2”.

Jika Anda sudah menjalankan EC2 instans, Anda dapat menggunakan AWS Compute Optimizer untuk mendapatkan rekomendasi tentang jenis instans yang harus Anda gunakan untuk meningkatkan kinerja, menghemat uang, atau keduanya. Untuk informasi selengkapnya, lihat the section called “Rekomendasi Compute Optimizer”.

Tugas

- Untuk menemukan tipe instans menggunakan konsol
- Jelaskan jenis instance menggunakan AWS CLI
- Temukan jenis instance menggunakan AWS CLI
- Temukan jenis instance menggunakan Alat untuk PowerShell

Untuk menemukan tipe instans menggunakan konsol

Anda dapat menemukan jenis instans yang memenuhi kebutuhan Anda menggunakan EC2 konsol Amazon.

Untuk menemukan tipe instans menggunakan konsol

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Dari bilah navigasi, pilih Wilayah untuk meluncurkan instans Anda. Anda dapat memilih Wilayah yang tersedia untuk Anda, terlepas dari lokasi Anda.
3. Pada panel navigasi, pilih Tipe Instans.
4. (Opsional) Pilih ikon preferensi (roda gigi) untuk memilih atribut tipe instans yang akan ditampilkan, seperti harga Linux Sesuai Permintaan, lalu pilih Konfirmasi. Atau, pilih nama tipe instans untuk membuka halaman detailnya dan melihat semua atribut yang tersedia melalui konsol. Konsol tidak menampilkan semua atribut yang tersedia melalui API atau baris perintah.
5. Gunakan atribut tipe instans untuk memfilter daftar tipe instans yang ditampilkan ke hanya tipe instans yang memenuhi kebutuhan Anda. Misalnya, Anda dapat memfilter atribut berikut:
   - Zona ketersediaan — Nama Zona Ketersediaan, Local Zone, atau Wavelength Zone. Untuk informasi selengkapnya, lihat the section called “Wilayah dan Zona”.
   - v CPUs atau Cores — Jumlah v CPUs atau core.
   - Memori (GiB) — Ukuran memori, dalam GiB.
   - Performa jaringan – Performa jaringan, dalam Gigabits.
   - Penyimpanan instans lokal – Menunjukkan apakah tipe instans memiliki penyimpanan instans lokal (`true` | `false`).
6. (Opsional) Untuk melihat side-by-side perbandingan, pilih kotak centang untuk beberapa jenis instance. Perbandingan ditampilkan di bagian bawah layar.
7. (Opsional) Untuk menyimpan daftar tipe instans ke file nilai dipisahkan koma (.csv) untuk peninjauan lebih lanjut, pilih Tindakan, Unduh CSV daftar. File tersebut mencakup semua tipe instans yang cocok dengan filter yang Anda atur.

8. (Opsional) Untuk meluncurkan instans menggunakan tipe instans yang sesuai dengan kebutuhan Anda, pilih kotak centang untuk tipe instans dan pilih Tindakan, Luncurkan instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

Jelaskan jenis instance menggunakan AWS CLI

Anda dapat menggunakan describe-instance-typesperintah untuk menggambarkan jenis instance tertentu.

Untuk sepenuhnya menggambarkan jenis instance

Perintah berikut menampilkan semua rincian yang tersedia untuk jenis instance tertentu. Outputnya panjang, jadi dihilangkan di sini.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2
```

Menggambarkan jenis instance dan menyaring output

Perintah berikut menampilkan rincian jaringan untuk jenis instance tertentu.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].NetworkInfo"
```

Berikut ini adalah output contoh.

```
[
    {
        "NetworkPerformance": "Low to Moderate",
        "MaximumNetworkInterfaces": 2,
        "MaximumNetworkCards": 1,
        "DefaultNetworkCardIndex": 0,
        "NetworkCards": [
            {
                "NetworkCardIndex": 0,
                "NetworkPerformance": "Low to Moderate",
```

```
                "MaximumNetworkInterfaces": 2,
                "BaselineBandwidthInGbps": 0.064,
                "PeakBandwidthInGbps": 1.024
            }
        ],
        "Ipv4AddressesPerInterface": 2,
        "Ipv6AddressesPerInterface": 2,
        "Ipv6Supported": true,
        "EnaSupport": "unsupported",
        "EfaSupported": false,
        "EncryptionInTransitSupported": false,
        "EnaSrdSupported": false
    }
]
```

Perintah berikut menampilkan memori yang tersedia untuk jenis instance tertentu.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].MemoryInfo"
```

Berikut ini adalah output contoh.

```
[
    {
        "SizeInMiB": 1024
    }
]
```

Temukan jenis instance menggunakan AWS CLI

Anda dapat menggunakan describe-instance-type-offeringsperintah describe-instance-typesand untuk menemukan jenis instance yang memenuhi kebutuhan Anda.

Contoh

- Contoh 1: Temukan jenis instance berdasarkan Availability Zone
- Contoh 2: Temukan jenis instance berdasarkan ukuran memori yang tersedia
- Contoh 3: Temukan jenis instance berdasarkan penyimpanan instance yang tersedia
- Contoh 4: Temukan jenis instance yang mendukung hibernasi

Contoh 1: Temukan jenis instance berdasarkan Availability Zone

Contoh berikut hanya menampilkan jenis instance yang ditawarkan di Availability Zone yang ditentukan.

```
aws ec2 describe-instance-type-offerings \
    --location-type "availability-zone" \
    --filters "Name=location,Values=us-east-2a" \
    --region us-east-2 \
    --query "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

Outputnya adalah daftar jenis instance, diurutkan menurut abjad. Berikut ini adalah awal dari output saja.

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c4.2xlarge
   ...
```

Contoh 2: Temukan jenis instance berdasarkan ukuran memori yang tersedia

Contoh berikut hanya menampilkan jenis instance generasi saat ini dengan 64 GiB (65536 MiB) memori.

```
aws ec2 describe-instance-types \
    --filters "Name=current-generation,Values=true" "Name=memory-info.size-in-
mib,Values=65536" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Outputnya adalah daftar jenis instance, diurutkan menurut abjad. Berikut ini adalah awal dari output saja.

```
c5a.8xlarge
c5ad.8xlarge
c6a.8xlarge
c6g.8xlarge
```

```
c6gd.8xlarge
c6gn.8xlarge
c6i.8xlarge
c6id.8xlarge
c6in.8xlarge
   ...
```

Contoh 3: Temukan jenis instance berdasarkan penyimpanan instance yang tersedia

Contoh berikut menampilkan ukuran total penyimpanan instans untuk semua instance R7 dengan volume penyimpanan instance.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r7*" "Name=instance-storage-
supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Berikut ini adalah output contoh.

```
---------------------------
|  DescribeInstanceTypes  |
+----------------+--------+
|  r7gd.xlarge   |  237   |
|  r7gd.8xlarge  |  1900  |
|  r7gd.16xlarge |  3800  |
|  r7gd.medium   |  59    |
|  r7gd.4xlarge  |  950   |
|  r7gd.2xlarge  |  474   |
|  r7gd.metal    |  3800  |
|  r7gd.large    |  118   |
|  r7gd.12xlarge |  2850  |
+----------------+--------+
```

Contoh 4: Temukan jenis instance yang mendukung hibernasi

Contoh berikut menampilkan jenis instance yang mendukung hibernasi.

```
aws ec2 describe-instance-types \
    --filters "Name=hibernation-supported,Values=true" \
    --region us-east-2 \
```

```
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Outputnya adalah daftar jenis instance, diurutkan menurut abjad. Berikut ini adalah awal dari output saja.

```
c4.2xlarge
c4.4xlarge
c4.8xlarge
c4.large
c4.xlarge
c5.12xlarge
c5.18xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
...
```

Temukan jenis instance menggunakan Alat untuk PowerShell

Anda dapat menggunakan Get-EC2InstanceTypedan Get-EC2InstanceTypeOfferingcmdlet untuk menemukan jenis instance yang memenuhi kebutuhan Anda.

Contoh

- Temukan jenis instance berdasarkan Availability Zone
- Temukan jenis instance berdasarkan ukuran memori yang tersedia
- Temukan jenis instans berdasarkan penyimpanan instans yang tersedia
- Temukan jenis instance yang mendukung hibernasi

Temukan jenis instance berdasarkan Availability Zone

Contoh berikut hanya menampilkan jenis instance yang ditawarkan di Availability Zone yang ditentukan.

```
(Get-EC2InstanceTypeOffering `
    -LocationType "availability-zone" `
    -Region us-east-2 `
    -Filter @{Name="location"; Values="us-east-2a"}).InstanceType | Sort-Object `
```

Temukan jenis instance berdasarkan ukuran memori yang tersedia

Contoh berikut hanya menampilkan jenis instance generasi saat ini dengan 64 GiB (65536 MiB) memori.

```
(Get-EC2InstanceType `
    -Filter @{Name="current-generation"; Values="true"},
            @{Name="memory-info.size-in-mib"; Values="65536"}).InstanceType | Sort-
Object
```

Temukan jenis instans berdasarkan penyimpanan instans yang tersedia

Contoh berikut menampilkan ukuran total penyimpanan instans untuk semua instance R7 dengan volume penyimpanan instance.

```
Get-EC2InstanceType `
    -Filter @{Name="instance-type"; Values="r7*"},
            @{Name="instance-storage-supported"; Values="true"} | `
     Select InstanceType, @{Name="TotalSizeInGB";
 Expression={($_.InstanceStorageInfo.TotalSizeInGB)}}
```

Berikut ini adalah output contoh.

```
InstanceType  TotalSizeInGB
------------  -------------
r7gd.8xlarge           1900
r7gd.16xlarge          3800
r7gd.xlarge             237
r7gd.4xlarge            950
r7gd.medium              59
r7gd.2xlarge            474
r7gd.large              118
r7gd.metal             3800
r7gd.12xlarge          2850
```

Temukan jenis instance yang mendukung hibernasi

Contoh berikut menampilkan jenis instance yang mendukung hibernasi.

```
(Get-EC2InstanceType `
    -Filter @{Name="hibernation-supported"; Values="true"}).InstanceType | Sort-Object
```

Dapatkan rekomendasi dari pencari tipe instans EC2

Pencari tipe instans EC2 mempertimbangkan kasus penggunaan, jenis beban kerja, preferensi produsen CPU, dan cara Anda memprioritaskan harga dan kinerja, serta parameter tambahan yang dapat Anda tentukan. Kemudian menggunakan data ini untuk memberikan saran dan panduan untuk jenis instans Amazon EC2 yang paling sesuai dengan beban kerja baru Anda.

Dengan begitu banyak jenis instans yang tersedia, menemukan jenis instans yang tepat untuk beban kerja Anda dapat memakan waktu dan kompleks. Dengan menggunakan pencari tipe instans EC2, Anda dapat tetap up to date dengan jenis instans terbaru dan mencapai kinerja harga terbaik untuk beban kerja Anda.

Anda bisa mendapatkan saran dan panduan untuk jenis instans EC2 menggunakan konsol Amazon EC2. Anda juga dapat pergi langsung ke Amazon Q untuk meminta saran tipe instans. Untuk informasi selengkapnya, lihat Panduan Pengguna Pengembang Amazon Q.

Jika Anda mencari rekomendasi tipe instans untuk beban kerja yang ada, gunakan AWS Compute Optimizer. Untuk informasi selengkapnya, lihat Dapatkan rekomendasi EC2 instans dari Compute Optimizer.

Gunakan pencari tipe instans EC2

Di konsol Amazon EC2, Anda bisa mendapatkan saran jenis instans dari pencari jenis instans EC2 di wizard instance peluncuran, saat membuat template peluncuran, atau di halaman Jenis instans.

Gunakan petunjuk berikut untuk mendapatkan saran dan panduan untuk jenis instans EC2 menggunakan pencari jenis instans EC2 di konsol Amazon EC2. Untuk melihat animasi langkah-langkahnya, lihatLihat animasi: Dapatkan saran tipe instans menggunakan pencari tipe instans EC2.

Untuk mendapatkan saran tipe instans menggunakan pencari tipe instans EC2

1. Mulai proses Anda menggunakan salah satu dari berikut ini:
   - Ikuti prosedur untuk meluncurkan instans. Di samping Tipe instans, pilih tautan Dapatkan saran.
   - Ikuti prosedur untuk membuat template peluncuran. Di samping Tipe instans, pilih tautan Dapatkan saran.
   - Di panel navigasi, pilih Jenis Instance, lalu pilih tombol Instance type finder.
2. Di layar Dapatkan saran tentang pemilihan jenis instance, lakukan hal berikut:

a. Tentukan persyaratan jenis instans Anda dengan memilih opsi untuk jenis Beban Kerja, Kasus penggunaan, Prioritas, dan produsen CPU.

b. (Opsional) Untuk menentukan persyaratan yang lebih rinci untuk beban kerja Anda, lakukan hal berikut:

   i. Perluas Parameter lanjutan.

   ii. Untuk menambahkan parameter, pilih parameter, pilih Tambah, dan tentukan nilai untuk parameter. Ulangi untuk setiap parameter tambahan yang ingin Anda tambahkan. Untuk menunjukkan tidak ada nilai minimum atau maksimum, biarkan bidang kosong.

   iii. Untuk menghapus parameter setelah menambahkannya, pilih X di sebelah parameter.

c. Pilih Dapatkan saran tipe instans.

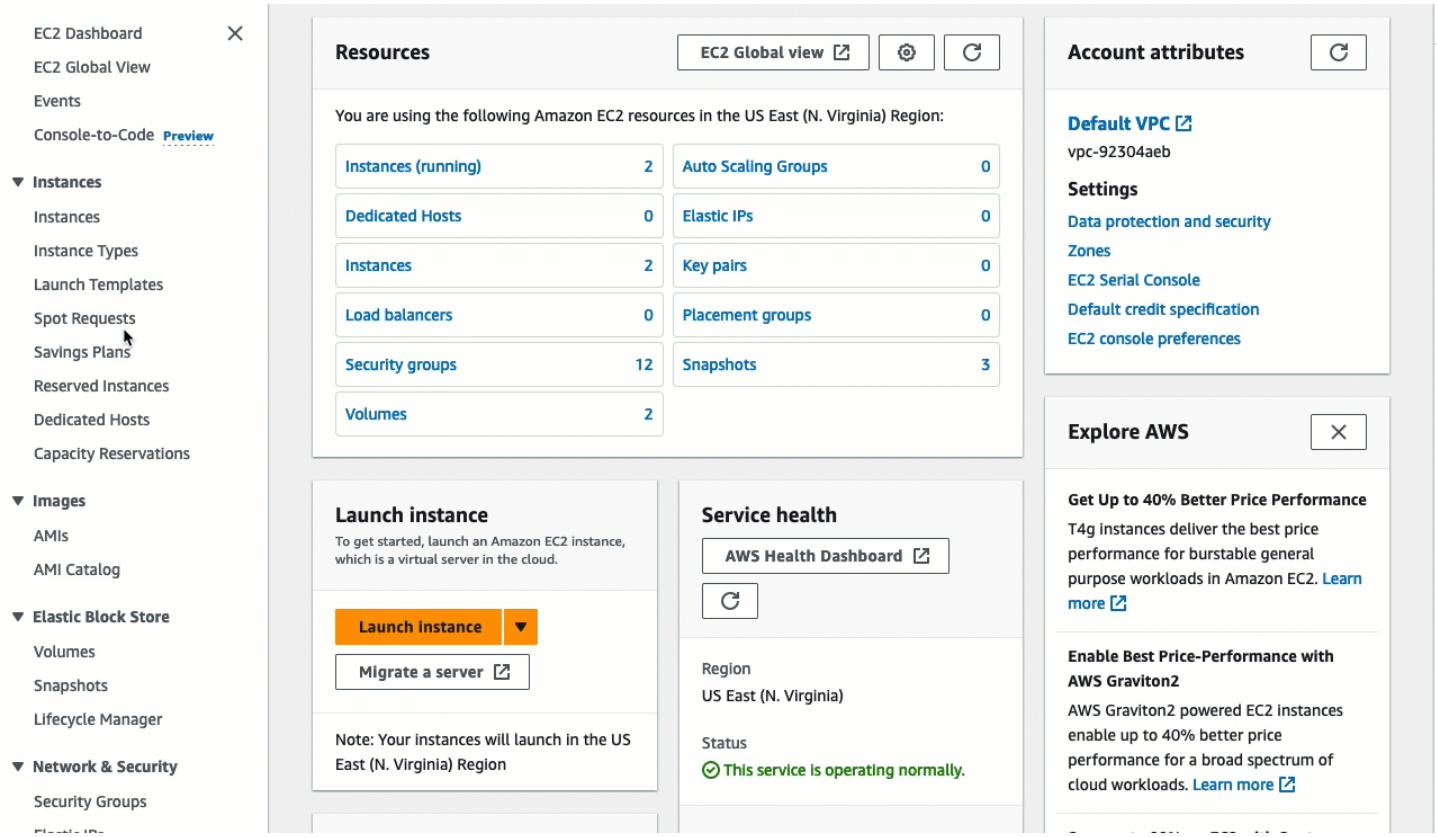
   Amazon EC2 memberi Anda saran untuk keluarga misalnya yang cocok dengan persyaratan yang Anda tentukan.

3. Untuk melihat detail setiap jenis instans dalam keluarga instans yang disarankan, pilih Lihat detail keluarga instans yang direkomendasikan.

4. Pilih jenis instans yang memenuhi persyaratan Anda, lalu pilih Actions, Launch instance atau Actions, Create launch template.

   Atau, jika Anda memulai proses di wizard instance peluncuran atau halaman template peluncuran, dan Anda lebih suka kembali ke alur asli Anda, catat jenis instance yang ingin Anda gunakan. Kemudian, di wizard instance peluncuran atau template peluncuran, untuk jenis Instance, pilih jenis instance, dan selesaikan prosedur untuk meluncurkan instance atau membuat template peluncuran.

Lihat animasi: Dapatkan saran tipe instans menggunakan pencari tipe instans EC2



Dapatkan rekomendasi EC2 instans dari Compute Optimizer

AWS Compute Optimizer memberikan EC2 rekomendasi Amazon untuk membantu Anda meningkatkan kinerja, menghemat uang, atau keduanya. Anda dapat menggunakan rekomendasi ini untuk memutuskan apakah akan mengubah ke jenis instans baru.

Untuk membuat rekomendasi, Compute Optimizer menganalisis spesifikasi instans dan metrik pemanfaatan yang ada. Data yang dikompilasi kemudian digunakan untuk merekomendasikan jenis EC2 instans Amazon mana yang paling mampu menangani beban kerja yang ada. Rekomendasi ditampilkan bersama dengan harga instans per jam. Untuk informasi selengkapnya, lihat metrik EC2 instans Amazon di Panduan AWS Compute Optimizer Pengguna.

Daftar Isi

- Persyaratan
- Klasifikasi temuan
- Melihat rekomendasi
- Pertimbangan untuk mengevaluasi rekomendasi

Persyaratan

Untuk mendapatkan rekomendasi dari Compute Optimizer, Anda harus terlebih dahulu memilih Compute Optimizer. Untuk informasi selengkapnya, lihat Memulai dengan AWS Compute Optimizer dalam Panduan Pengguna AWS Compute Optimizer .

Compute Optimizer menghasilkan rekomendasi untuk beberapa tipe instans, tetapi tidak semua tipe instance. Jika Anda menggunakan jenis instans yang tidak didukung, Compute Optimizer tidak akan menghasilkan rekomendasi. Untuk daftar jenis instans yang didukung, lihat persyaratan EC2 instans Amazon di Panduan AWS Compute Optimizer Pengguna.

Klasifikasi temuan

Compute Optimizer mengklasifikasikan EC2 temuannya untuk instance sebagai berikut:

- Under-provisioned — EC2 Instance dianggap kurang disediakan ketika setidaknya satu spesifikasi instans Anda, seperti CPU, memori, atau jaringan, tidak memenuhi persyaratan kinerja beban kerja Anda. EC2 Instance yang kurang disediakan dapat menyebabkan kinerja aplikasi yang buruk.
- Over-provisioned — EC2 Instance dianggap terlalu disediakan ketika setidaknya satu spesifikasi instans Anda, seperti CPU, memori, atau jaringan, dapat diperkecil sementara masih memenuhi persyaratan kinerja beban kerja Anda, dan ketika tidak ada spesifikasi yang kurang disediakan. EC2 Instans yang disediakan secara berlebihan dapat menyebabkan biaya infrastruktur yang tidak perlu.
- Dioptimalkan — EC2 Instans dianggap dioptimalkan ketika semua spesifikasi instans Anda, seperti CPU, memori, dan jaringan, memenuhi persyaratan kinerja beban kerja Anda, dan instans tidak disediakan secara berlebihan. EC2 Instans yang dioptimalkan menjalankan beban kerja Anda dengan kinerja dan biaya infrastruktur yang optimal. Untuk instans yang dioptimalkan, Compute Optimizer dapat sewaktu-waktu merekomendasikan tipe instans generasi baru.
- Tidak ada – Tidak ada rekomendasi untuk instans ini. Hal ini mungkin terjadi jika Anda memilih Compute Optimizer selama kurang dari 12 jam, atau ketika instans berjalan kurang dari 30 jam, atau saat tipe instans tidak didukung oleh Compute Optimizer.

Melihat rekomendasi

Setelah memilih Compute Optimizer, Anda dapat melihat temuan yang dihasilkan Compute Optimizer untuk instans Anda di konsol Amazon. EC2 EC2 Anda kemudian dapat mengakses konsol Compute Optimizer untuk melihat rekomendasi. Jika Anda baru-baru ini ikut serta, temuan mungkin tidak tercermin di EC2 konsol hingga 12 jam.

Untuk melihat rekomendasi untuk instans menggunakan EC2 konsol Amazon

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih ID instance untuk membuka halaman detail instance.
4. Pada halaman detail instance, di bagian ringkasan atas, temukan AWS Compute Optimizer temuan. Jika ada temuan, kami menampilkan klasifikasi temuan dan tautan untuk melihat detailnya. Jika tidak, kami menampilkan Tidak ada rekomendasi yang tersedia untuk contoh ini.
5. Jika ada temuan, pilih Lihat detail. Ini membuka halaman Rekomendasi untuk EC2 instans di konsol Compute Optimizer. Jenis instance saat ini diberi label Current. Ada juga hingga tiga rekomendasi tipe instans, berlabel Opsi 1, Opsi 2, dan Opsi 3. Halaman ini juga menampilkan data CloudWatch metrik terbaru untuk contoh tersebut.

Untuk melihat rekomendasi untuk semua instans di semua Wilayah

Anda dapat melihat rekomendasi untuk semua EC2 instans Amazon di semua Wilayah menggunakan konsol Compute Optimizer. Untuk informasi selengkapnya, lihat Melihat rekomendasi EC2 instans dan Melihat detail EC2 instans di Panduan AWS Compute Optimizer Pengguna.

Pertimbangan untuk mengevaluasi rekomendasi

Ketika Anda menerima rekomendasi, Anda harus memutuskan apakah akan menindaklanjutinya. Sebelum mengubah tipe instans, pertimbangkan hal berikut:

- Rekomendasi tidak memprakirakan penggunaan Anda. Rekomendasi didasarkan pada penggunaan historis Anda selama periode waktu 14 hari terakhir. Pastikan untuk memilih tipe instans yang diperkirakan memenuhi kebutuhan sumber daya Anda di masa mendatang.
- Fokus pada metrik grafik untuk menentukan apakah penggunaan aktual lebih rendah daripada kapasitas instans. Anda juga dapat melihat data metrik (rata-rata, puncak, persentil) CloudWatch untuk mengevaluasi lebih lanjut rekomendasi EC2 instans Anda. Misalnya, perhatikan cara metrik persentase CPU berubah sepanjang hari dan apakah ada puncak yang perlu diakomodasi. Untuk informasi selengkapnya, lihat Melihat Metrik yang Tersedia di Panduan CloudWatch Pengguna Amazon.
- Compute Optimizer mungkin menyediakan rekomendasi untuk instans performa yang dapat melonjak, yaitu instans T3, T3a, dan T2. Jika Anda secara berkala meledak di atas garis dasar, pastikan Anda dapat terus melakukannya berdasarkan v dari CPUs jenis instance baru. Untuk informasi selengkapnya, lihat Konsep kunci untuk instance kinerja yang dapat meledak.

- Jika Anda telah membeli Instans Terpesan, Instans Sesuai Permintaan Anda mungkin ditagih sebagai Instans Terpesan. Sebelum Anda mengubah tipe instans saat ini, pertama-tama evaluasi dampaknya terhadap penggunaan dan cakupan Instans Terpesan.
- Pertimbangkan konversi ke instans generasi yang lebih baru, jika memungkinkan.
- Saat bermigrasi ke keluarga instans yang berbeda, pastikan tipe instans saat ini dan tipe instans yang baru kompatibel. Misalnya, dalam hal virtualisasi, arsitektur, atau tipe jaringan. Untuk informasi selengkapnya, lihat Kompatibilitas untuk mengubah tipe instans.
- Terakhir, pertimbangkan penilaian risiko performa yang diberikan untuk setiap rekomendasi. Risiko kinerja menunjukkan jumlah upaya yang mungkin perlu Anda keluarkan untuk memvalidasi apakah tipe instans yang direkomendasikan memenuhi persyaratan kinerja beban kerja Anda. Kami juga menyarankan pengujian beban dan performa yang ketat sebelum dan setelah membuat perubahan apa pun.

Perubahan jenis instans Amazon EC2

Saat kebutuhan Anda berubah, Anda mungkin menemukan bahwa instans Anda digunakan secara berlebihan (tipe instans terlalu kecil) atau kurang termanfaatkan (tipe instans terlalu besar). Jika demikian, Anda dapat mengubah ukuran instans Anda dengan mengubah tipe instans-nya. Misalnya, jika instans `t2.micro` Anda terlalu kecil untuk beban kerjanya, Anda dapat meningkatkan ukurannya dengan mengubahnya ke tipe instans T2 yang lebih besar, seperti `t2.large`. Atau Anda dapat mengubahnya ke tipe instans lain, seperti `m5.large`. Anda mungkin juga ingin mengubah dari generasi sebelumnya ke jenis instans generasi saat ini untuk memanfaatkan beberapa fitur, seperti dukungan untuk IPv6.

Jika Anda menginginkan rekomendasi tipe instans yang paling mampu menangani beban kerja yang ada, Anda dapat menggunakan AWS Compute Optimizer. Untuk informasi selengkapnya, lihat Dapatkan rekomendasi EC2 instans dari Compute Optimizer.

Saat mengubah tipe instans, Anda akan mulai membayar tarif tipe instans yang baru. Untuk tarif sesuai permintaan semua tipe instans, lihat: Harga Sesuai Permintaan Amazon EC2.

Untuk menambahkan penyimpanan tambahan ke instans Anda tanpa mengubah jenis instans, tambahkan volume EBS ke instance. Untuk informasi selengkapnya, lihat Melampirkan volume Amazon EBS ke instans di Panduan Pengguna Amazon EBS.

Instruksi mana yang harus diikuti?

Ada instruksi yang berbeda untuk mengubah tipe instans. Instruksi yang akan digunakan bergantung pada volume root instans, dan apakah tipe instans itu kompatibel dengan konfigurasi instans saat ini. Untuk informasi tentang bagaimana kompatibilitas ditentukan, lihat Kompatibilitas untuk mengubah tipe instans.

Gunakan tabel berikut untuk menentukan instruksi mana yang harus diikuti.

Volume akar	Kompatibilitas	Gunakan petunjuk ini
EBS	Kompatibel	Ubah tipe instans
EBS	Tidak kompatibel	Migrasi ke tipe instans baru
Penyimpanan instans	Tidak berlaku	Migrasi ke tipe instans baru

Kompatibilitas untuk mengubah tipe instans

Anda dapat mengubah tipe instans hanya jika konfigurasi instans saat ini kompatibel dengan tipe instans yang Anda inginkan. Jika tipe instans yang Anda inginkan tidak kompatibel dengan konfigurasi instans saat ini, Anda harus meluncurkan instans baru dengan konfigurasi yang kompatibel dengan tipe instans tersebut, lalu memigrasikan aplikasi Anda ke instans baru.

Kompatibilitas ditentukan melalui hal-hal berikut:

Tipe virtualisasi

Linux AMIs menggunakan salah satu dari dua jenis virtualisasi: paravirtual (PV) atau hardware virtual machine (HVM). Jika instans diluncurkan dari PV AMI, Anda tidak dapat mengubah tipe instans yang hanya HVM. Untuk informasi selengkapnya, lihat Tipe virtualisasi. Untuk memeriksa tipe virtualisasi instans Anda, periksa nilai Virtualisasi di panel detail layar Instans di konsol Amazon EC2.

Arsitektur

AMIs khusus untuk arsitektur prosesor, jadi Anda harus memilih jenis instance dengan arsitektur prosesor yang sama dengan jenis instance saat ini. Contoh:

- Jika tipe instans saat ini memiliki prosesor berdasarkan arsitektur Arm, Anda dibatasi pada tipe instans yang mendukung prosesor berdasarkan arsitektur Arm, seperti C6g dan M6g.

- Jenis instance berikut adalah satu-satunya tipe instance yang mendukung 32-bit AMIs:`t2.nano`,,`t2.micro`,`t2.small`,`t2.medium`,`c3.large`,`t1.micro`, `m1.small`m1.medium, danc1.medium. Jika Anda mengubah tipe instans dari instans 32-bit, Anda dibatasi untuk tipe instans ini.

Adaptor jaringan

Jika Anda beralih dari driver untuk satu adaptor jaringan ke yang lain, pengaturan adaptor jaringan diatur ulang saat sistem operasi membuat adaptor baru. Untuk mengonfigurasi ulang pengaturan, Anda mungkin memerlukan akses ke akun lokal dengan izin administrator. Berikut ini adalah contoh perpindahan dari satu adaptor jaringan ke yang lain:

- AWS PV (instans T2) ke Intel 82599 VF (instans M4)
- Intel 82599 VF (sebagian besar instans M4) ke ENA (instans M5)
- ENA (instans M5) ke ENA bandwidth tinggi (instans M5n)

Jaringan yang ditingkatkan

Tipe instans yang mendukung jaringan yang ditingkatkan memerlukan instalasi driver yang diperlukan. Misalnya, instans berbasis NITRO memerlukan EBS yang didukung AMIs dengan driver Elastic Network Adapter (ENA) yang diinstal. Untuk mengubah tipe instans yang tidak mendukung peningkatan jaringan menjadi tipe instans yang mendukung peningkatan jaringan, Anda harus menginstal driver ENA atau driver ixgbevf pada instans tersebut, yang sesuai.

> **Note**
>
> Saat Anda mengubah ukuran instans yang mengaktifkan ENA Ekspres diaktifkan, tipe instans baru juga harus mendukung ENA Ekspres. Untuk daftar tipe instans yang mendukung ENA Ekspres, lihat Tipe instans yang didukung untuk ENA Ekspres. Untuk mengubah tipe instans yang mendukung ENA Ekspres ke tipe instans yang tidak mendukungnya, pastikan ENA Ekspres saat ini tidak diaktifkan sebelum Anda mengubah ukuran instans.

NVMe

Volume EBS diekspos sebagai perangkat NVMe blok pada instans berbasis Nitro. Jika Anda mengubah dari jenis instans yang tidak mendukung NVMe ke jenis instans yang mendukung NVMe, Anda harus terlebih dahulu menginstal NVMe driver pada instance Anda. Selain itu, nama

perangkat untuk perangkat yang Anda tentukan dalam pemetaan perangkat blok diganti namanya menggunakan nama NVMe perangkat ()`/dev/nvme[0-26]n1`.

[Instance Linux] Oleh karena itu, untuk me-mount sistem file saat boot menggunakan`/etc/fstab`, Anda harus menggunakan UUID/Label alih-alih nama perangkat.

Batas Volume

Jumlah maksimum volume Amazon EBS yang dapat dilampirkan ke instans bergantung pada tipe instans dan ukuran instans. Untuk informasi selengkapnya, lihat Batas volume Amazon EBS untuk instans Amazon EC2.

Anda hanya dapat mengubah ke tipe instans atau ukuran instans yang mendukung jumlah volume yang sama atau yang lebih besar daripada yang saat ini dilampirkan ke instans. Jika Anda mengubah ke tipe instans atau ukuran instans yang tidak mendukung jumlah volume yang saat ini dilampirkan, permintaan akan gagal. Misalnya, jika Anda mengubah dari instans `m7i.4xlarge` dengan 32 volume terlampir ke `m6i.4xlarge`, yang mendukung maksimum 27 volume, permintaan akan gagal.

NitroTPM

Jika Anda meluncurkan instance menggunakan AMI dengan NitRotPM diaktifkan dan jenis instans yang mendukung NitroTPM, instance akan diluncurkan dengan nitRotPM diaktifkan. Anda hanya dapat mengubah ke jenis instance yang juga mendukung NitRotPM.

Mengubah jenis instans untuk instans Amazon EC2

Gunakan petunjuk berikut untuk mengubah jenis instans instans yang didukung Amazon EBS jika jenis instans yang Anda butuhkan kompatibel dengan konfigurasi instans Anda saat ini. Untuk informasi selengkapnya, lihat the section called “Kompatibilitas”.

Pertimbangan

- Anda harus menghentikan instans Anda sebelum dapat mengubah jenis instance-nya. Pastikan Anda merencanakan waktu henti saat instans dihentikan. Menghentikan instans dan mengubah tipe instansnya mungkin memerlukan waktu beberapa menit, lalu memulai ulang instans Anda mungkin memerlukan waktu yang bervariasi, tergantung skrip pemulaian aplikasi Anda. Untuk informasi selengkapnya, lihat Hentikan dan mulai instans Amazon EC2.
- Saat Anda berhenti dan memulai sebuah instans, kami memindahkan instans tersebut ke perangkat keras baru. Jika instans Anda memiliki IPv4 alamat publik, yang bukan IP Elastis,

kami merilis alamat dan memberikan contoh Anda IPv4 alamat publik baru. Untuk informasi selengkapnya tentang perilaku alamat IP sepanjang siklus hidup instance, lihat. Perbedaan antara status instance

- Anda tidak dapat mengubah tipe instans dari Instans Spot.
- [Instans Windows] Kami menyarankan Anda memperbarui paket driver AWS PV sebelum mengubah jenis instans. Untuk informasi selengkapnya, lihat the section called “Mutakhirkan driver PV”.
- Jika instans Anda berada dalam grup Auto Scaling, layanan Amazon EC2 Auto Scaling menandai instans yang dihentikan sebagai tidak sehat, dan dapat menghentikannya serta meluncurkan instance pengganti. Untuk mencegahnya, Anda dapat menangguhkan proses penskalaan untuk grup saat Anda mengubah tipe instans. Untuk informasi selengkapnya, lihat Menangguhkan dan melanjutkan proses grup Auto Scaling dalam Panduan Pengguna Amazon EC2 Auto Scaling.
- Saat Anda mengubah jenis instance instance dengan volume penyimpanan NVMe instans, instance yang diperbarui mungkin memiliki volume penyimpanan instans tambahan, karena semua volume penyimpanan NVMe instans tersedia meskipun tidak ditentukan dalam pemetaan perangkat blok AMI atau instans. Jika tidak, instans yang diperbarui memiliki jumlah volume penyimpanan instans yang sama dengan yang Anda tentukan saat meluncurkan instans asli.
- Jumlah maksimum volume Amazon EBS yang dapat dilampirkan ke instans bergantung pada tipe instans dan ukuran instans. Anda tidak dapat mengubah ke tipe instans atau ukuran instans yang tidak mendukung jumlah volume yang sudah dilampirkan ke instans Anda. Untuk informasi selengkapnya, lihat Batas volume Amazon EBS untuk instans Amazon EC2.
- [Instance Linux] Anda dapat menggunakan `AWSSupport-MigrateXenToNitroLinux` runbook untuk memigrasikan instance Linux yang kompatibel dari jenis instance Xen ke jenis instans Nitro. Untuk informasi selengkapnya, lihat AWSSupport-MigrateXenToNitroLinux runbook di referensi buku runbook Otomatisasi AWS Systems Manager .
- [Instans Windows] Untuk panduan tambahan tentang memigrasi instance Windows yang kompatibel dari tipe instans Xen ke tipe instans Nitro, lihat Memigrasi ke jenis instans generasi terbaru.

Untuk mengubah tipe instans dari instans yang didukung Amazon EBS

1. (Opsional) Jika tipe instans yang baru memerlukan driver yang tidak diinstal pada instans yang ada, Anda harus terhubung ke instans dan menginstal driver terlebih dahulu. Untuk informasi selengkapnya, lihat Kompatibilitas untuk mengubah tipe instans.

2. [Instans Windows] Jika Anda mengonfigurasi instance Windows Anda untuk menggunakan pengalamatan IP statis dan Anda mengubah dari jenis instans yang tidak mendukung jaringan yang ditingkatkan ke jenis instans yang mendukung jaringan yang ditingkatkan, Anda mungkin mendapatkan peringatan tentang potensi konflik alamat IP saat Anda mengkonfigurasi ulang pengalamatan IP statis. Untuk mencegahnya, aktifkan DHCP pada antarmuka jaringan untuk instans Anda sebelum Anda mengubah tipe instans. Dari instans Anda, buka Network and Sharing Center, buka Internet Protocol Version 4 (TCP/IPv4) Properties untuk antarmuka jaringan, dan pilih Dapatkan alamat IP secara otomatis. Ubah tipe instans dan konfigurasikan kembali pengalamatan IP statis pada antarmuka jaringan.
3. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
4. Di panel navigasi, pilih Instans.
5. Pilih instans dan pilih Status instans, Hentikan instans. Ketika diminta konfirmasi, pilih Berhenti. Hal ini dapat memerlukan waktu beberapa menit sampai instans berhenti.
6. Dengan instans yang masih dipilih, klik Tindakan, Pengaturan instans, Ubah tipe instans. Opsi ini berwarna abu-abu jika status instans tidak `stopped`.
7. Pada halaman Ubah tipe instans, lakukan hal berikut:

   a. Untuk Tipe instans, pilih tipe instans yang Anda inginkan.

      Jika tipe instans tidak ada dalam daftar, maka instans itu tidak kompatibel dengan konfigurasi instans Anda. Sebagai gantinya, gunakan instruksi berikut: Migrasi ke jenis instans baru dengan meluncurkan instans EC2 baru.

   b. (Opsional) Jika tipe instans yang Anda pilih mendukung pengoptimalan EBS, pilih EBS dioptimalkan untuk mengaktifkan pengoptimalan EBS, atau batalkan pilihan EBS dioptimalkan untuk menonaktifkan pengoptimalan EBS.

      Jika tipe instans yang Anda pilih adalah EBS – dioptimalkan secara default, EBS-dioptimalkan dipilih dan Anda tidak dapat membatalkan pilihannya.

   c. (Opsional) Konfigurasikan opsi vCPU pada jenis instance baru.

      Saat Anda mengubah jenis instans dari instans yang ada, Amazon EC2 menerapkan pengaturan opsi CPU dari instans yang ada ke instans baru, jika memungkinkan. Jika jenis instans baru tidak mendukung pengaturan tersebut, opsi CPU disetel ulang ke None. Opsi ini menggunakan nomor default v CPUs untuk jenis instance baru.

      Jika jenis instans yang Anda pilih mendukung konfigurasi vCPU, pilih Tentukan opsi CPU di panel Detail lanjutan untuk mengonfigurasi v CPUs untuk jenis instans baru Anda.

d. Pilih Ubah untuk menerima pengaturan baru.

8. Untuk memulai instans, pilih instans dan pilih Status instans, Mulai instans. Hal ini diperlukan waktu beberapa menit hingga instans memasuki status `running`. Jika instans Anda tidak akan dimulai, lihat Pemecahan masalah dalam mengubah tipe instans.
9. [Instans Windows] Jika instans Anda menjalankan Windows Server 2016 atau Windows Server 2019 dengan EC2 Launch v1, sambungkan ke instance Windows Anda dan jalankan PowerShell skrip EC2 Launch berikut untuk mengonfigurasi instance setelah jenis instans diubah.

> **Important**
>
> Kata sandi administrator akan diatur ulang ketika Anda mengaktifkan skrip EC2Launch inisialisasi instans. Anda dapat memodifikasi file konfigurasi untuk menonaktifkan pengaturan ulang kata sandi administrator dengan menentukannya di pengaturan untuk tugas inisialisasi. Untuk langkah-langkah tentang cara menonaktifkan pengaturan ulang kata sandi, lihat Mengkonfigurasi tugas inisialisasi (EC2Peluncuran) atau Ubah pengaturan (EC2Luncurkan v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Migrasi ke jenis instans baru dengan meluncurkan instans EC2 baru

Anda dapat mengubah jenis instans dari instans EC2 hanya jika itu adalah instans yang didukung EBS dengan konfigurasi yang kompatibel dengan jenis instans baru yang Anda inginkan. Jika tidak, jika konfigurasi atau instance Anda tidak kompatibel dengan jenis instans baru, atau merupakan instance berbasis penyimpanan instance, Anda harus meluncurkan instance pengganti yang kompatibel dengan jenis instance yang Anda inginkan. Untuk informasi selengkapnya tentang bagaimana kompatibilitas ditentukan, lihatKompatibilitas untuk mengubah tipe instans.

Ikhtisar proses migrasi

- Cadangkan data pada instance asli.
- Luncurkan instance baru dengan konfigurasi yang kompatibel dengan jenis instans baru yang Anda inginkan, lampirkan volume EBS apa pun yang dilampirkan ke instans asli Anda.
- Instal aplikasi Anda pada instance baru Anda.

- Pulihkan data apa pun.
- Jika instans asli memiliki alamat IP Elastis, Anda harus mengaitkannya dengan instans baru Anda untuk memastikan bahwa pengguna Anda dapat terus menggunakan aplikasi Anda tanpa gangguan.

Untuk memigrasikan instance ke instance baru

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Cadangkan data apa pun yang masih Anda butuhkan sebagai berikut:
   - Connect ke instans Anda dan salin data pada volume penyimpanan instans Anda ke penyimpanan persisten.
   - Buat snapshot volume EBS Anda sehingga Anda dapat membuat volume baru dengan data yang sama, atau lepaskan volume dari instance asli sehingga Anda dapat melampirkannya ke instance baru.
3. Di panel navigasi, pilih Instans.
4. Pilih Luncurkan Instans. Saat Anda mengonfigurasi instans, lakukan hal berikut:
   a. Pilih AMI yang mendukung jenis instans yang Anda inginkan. Misalnya, Anda harus memilih AMI yang mendukung jenis prosesor dari jenis instans baru. Juga, jenis instance generasi saat ini memerlukan AMI HVM.
   b. Pilih tipe instans baru yang Anda inginkan. Jika tipe instans yang Anda inginkan tidak tersedia, maka instans itu tidak kompatibel dengan konfigurasi AMI yang Anda pilih.
   c. Jika Anda ingin mengizinkan lalu lintas yang sama untuk mencapai instance baru, pilih VPC dan grup keamanan yang sama yang digunakan dengan instance asli.
   d. Saat Anda selesai mengonfigurasi instans baru, selesaikan langkah-langkah untuk memilih pasangan kuci dan meluncurkan instans Anda. Hal ini diperlukan waktu beberapa menit hingga instans memasuki status `running`.
5. Jika Anda mencadangkan data ke snapshot EBS, buat volume dari snapshot lalu lampirkan volume ke instance baru.

   Untuk memindahkan volume EBS dari instans asli ke instans baru, lepaskan volume dari instance asli dan kemudian lampirkan volume ke instance baru.
6. Instal aplikasi Anda dan perangkat lunak yang diperlukan pada instans baru.
7. Pulihkan data apa pun yang Anda cadangkan dari volume penyimpanan instans dari instans asli.

8. Jika instance asli memiliki alamat IP Elastis, tetapkan ke instance baru sebagai berikut:

   a. Di panel navigasi, pilih Elastic IPs.

   b. Pilih alamat IP Elastis yang terkait dengan instans asli dan pilih Tindakan, Pisahkan ke Elastis. Saat diminta konfirmasi, pilih Ya, Nonaktifkan.

   c. Dengan alamat IP Elastis masih dipilih, pilih Tndakan, Kaitkan alamat IP Elastis.

   d. Untuk tipe Resource, pilih instans.

   e. Misalnya, pilih contoh baru.

   f. (Opsional) Untuk Alamat IP privat, tentukan alamat IP privat yang akan dikaitkan dengan alamat IP Elastis.

   g. Pilih Kaitkan.

9. (Opsional) Anda dapat mengakhiri instans asli jika sudah tidak diperlukan lagi. Pilih instans, verifikasi bahwa Anda akan menghentikan instans asli dan bukan instans baru (misalnya, periksa nama atau waktu peluncuran), lalu pilih Status instans, Hentikan instans.

Pemecahan masalah dalam mengubah tipe instans

Gunakan informasi berikut untuk membantu mendiagnosis dan memperbaiki masalah yang mungkin Anda temui saat mengubah tipe instans.

Instans tidak akan dimulai setelah mengubah tipe instans

Kemungkinan penyebab: Persyaratan untuk tipe instans baru tidak terpenuhi

Jika instans Anda tidak bisa boot, kemungkinan salah satu persyaratan untuk tipe instans baru tidak terpenuhi. Untuk informasi selengkapnya, lihat Mengapa instans Linux saya tidak bisa boot setelah saya mengubah tipenya?

Kemungkinan penyebab: AMI tidak mendukung tipe instans

Jika Anda menggunakan konsol EC2 untuk mengubah tipe instans, hanya tipe instans yang didukung oleh AMI yang dipilih yang akan tersedia. Namun, jika Anda menggunakan AWS CLI untuk meluncurkan instance, Anda dapat menentukan AMI dan jenis instans yang tidak kompatibel. Jika AMI dan tipe instans tidak kompatibel, instans tidak dapat dimulai. Untuk informasi selengkapnya, lihat Kompatibilitas untuk mengubah tipe instans.

Kemungkinan penyebab: Instans dalam grup penempatan klaster

Jika instans Anda berada dalam grup penempatan klaster dan, setelah mengubah tipe instans, instans gagal dimulai, coba yang berikut ini:

1. Hentikan semua instans dalam grup penempatan klaster.
2. Mengubah tipe instans yang terpengaruh.
3. Mulai semua instans dalam grup penempatan klaster.

Aplikasi atau situs web tidak dapat dijangkau dari internet setelah mengubah tipe instans

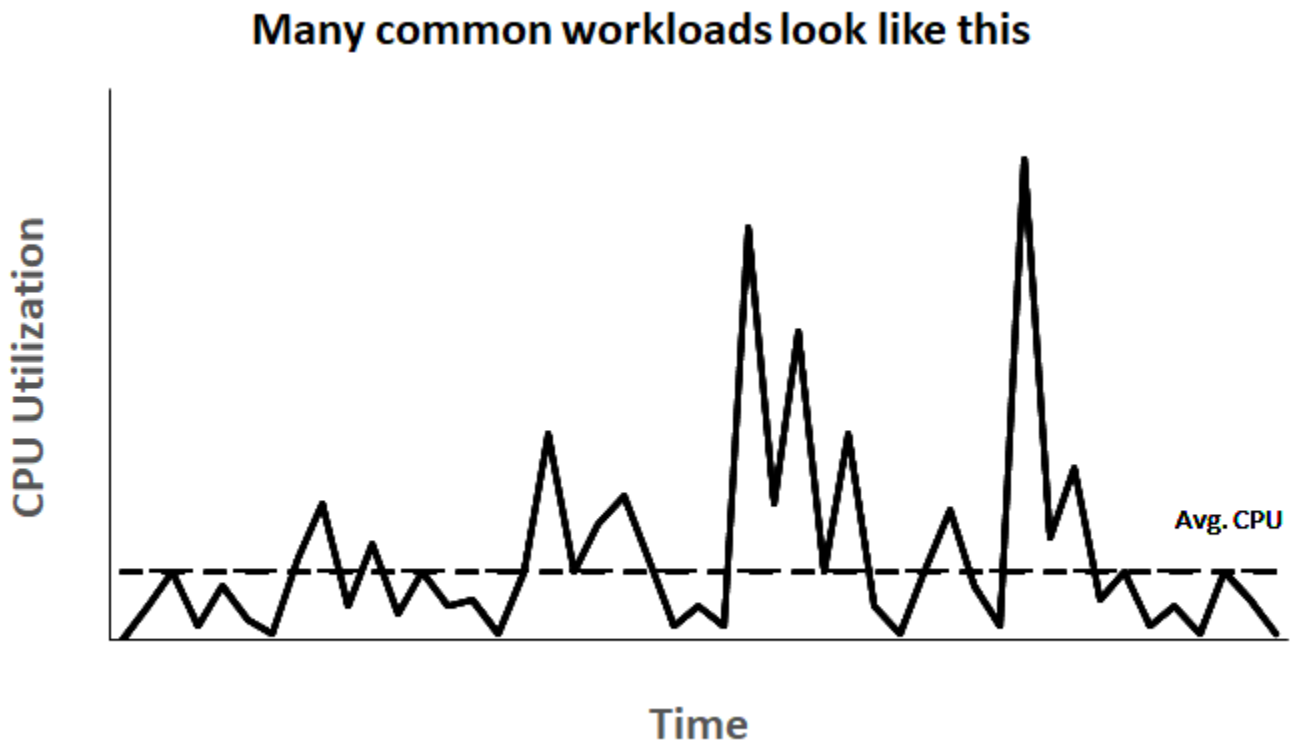
Kemungkinan penyebabnya: IPv4 Alamat publik dirilis

Saat mengubah tipe instans, Anda harus menghentikan instans tersebut terlebih dahulu. Ketika Anda menghentikan sebuah instans, kami merilis IPv4 alamat publik dan memberikan contoh Anda IPv4 alamat publik baru.

Untuk mempertahankan IPv4 alamat publik antara instans berhenti dan mulai, kami sarankan Anda menggunakan alamat IP Elastis, tanpa biaya tambahan asalkan instans Anda berjalan. Lihat informasi yang lebih lengkap di Alamat Elastic IP.

Instance performa yang dapat melonjak

Banyak beban kerja tujuan umum secara rata-rata tidak sibuk, dan tidak memerlukan performa CPU berkelanjutan tingkat tinggi. Grafik berikut menggambarkan pemanfaatan CPU untuk banyak beban kerja umum yang dijalankan pelanggan di Cloud saat AWS ini.



Beban kerja pemanfaatan low-to-moderate CPU ini menyebabkan pemborosan siklus CPU dan, akibatnya, Anda membayar lebih dari yang Anda gunakan. Untuk mengatasi hal ini, Anda dapat memanfaatkan instans tujuan umum yang dapat melonjak berbiaya rendah, yang merupakan instans T.

Keluarga instans T menyediakan kemampuan untuk melonjak di atas garis dasar bagi performa CPU dasar kapan saja selama yang diperlukan. CPU acuan ditetapkan untuk memenuhi kebutuhan sebagian besar beban kerja tujuan umum, termasuk layanan mikro skala besar, server web, basis data kecil dan menengah, logging data, repositori kode, desktop virtual, lingkungan pengembangan dan pengujian, serta aplikasi penting untuk bisnis. Instans T menawarkan keseimbangan komputasi, memori, dan sumber daya jaringan, dan memberi Anda cara yang paling hemat biaya untuk menjalankan spektrum luas aplikasi tujuan umum yang memiliki penggunaan CPU. low-to-moderate Mereka dapat menghemat biaya hingga 15% jika dibandingkan dengan instans M, dan dapat menghasilkan penghematan biaya yang lebih besar dengan ukuran instans yang lebih kecil dan lebih ekonomis, menawarkan memori serendah 2 v CPUs dan 0,5 GiB. Ukuran instans T yang lebih kecil, seperti nano, mikro, kecil, dan menengah, sangat cocok untuk beban kerja yang membutuhkan sejumlah kecil memori dan tidak mengharapkan penggunaan CPU yang tinggi.

> **Note**
>
> Topik ini menjelaskan CPU yang dapat melonjak. Untuk informasi tentang performa jaringan yang dapat melonjak, lihat Bandwidth jaringan EC2 instans Amazon.

Tipe instans yang dapat melonjak EC2

Instans burstable EC2 terdiri dari tipe instans T4G, T3a, dan T3, dan tipe instans T2 generasi sebelumnya.

Tipe instans T4g adalah instans yang dapat melonjak generasi terbaru. Tipe instans ini memberikan harga terbaik untuk performa, dan menyediakan biaya semua tipe instans EC2 yang terendah. Jenis instans T4G didukung oleh prosesor AWS Graviton2 berbasis ARM dengan dukungan ekosistem yang luas dari vendor sistem operasi, vendor perangkat lunak independen, dan layanan dan aplikasi populer. AWS

Tabel berikut merangkum perbedaan utama antara tipe-tipe instans yang dapat melonjak.

Tipe	Deskripsi	Keluarga prosesor
Generasi terbaru		
T4g	Jenis instans EC2 biaya terendah dengan biaya hingga 40% lebih tinggi price/per formance dan biaya 20% lebih rendah vs T3	AWS Prosesor Graviton2 dengan inti Arm Neoverse N1
T3a	Instans berbasis x86 paling murah dengan biaya 10% lebih rendah vs. instans T3	Prosesor EPYC generasi ke-1 dari AMD
T3	Puncak terbaik price/per formance untuk beban kerja x86 dengan hingga 30% lebih rendah dibandingkan instans price/performance T2 generasi sebelumnya	Intel Xeon Scalable (prosesor Skylake, Cascade Lake)

Tipe	Deskripsi	Keluarga prosesor
Generasi sebelumnya		
T2	Instans yang dapat melonjak generasi sebelumnya	Prosesor Intel Xeon

Untuk informasi tentang harga instans dan spesifikasi tambahan, lihat Harga Amazon EC2 dan Tipe Instans Amazon EC2. Untuk informasi tentang performa jaringan yang dapat melonjak, lihat Bandwidth jaringan EC2 instans Amazon.

Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan usianya kurang dari 12 bulan, Anda dapat menggunakan `t2.micro` instans secara gratis (atau `t3.micro` instans di Wilayah yang tidak `t2.micro` tersedia) dalam batas penggunaan tertentu. Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, Anda dapat menggunakan`t3.micro`,, `t3.small`t4g.micro, jenis `t4g.small` instans selama 6 bulan atau sampai kredit Anda habis. Untuk informasi selengkapnya, lihat AWS Tingkat Gratis.

Opsi pembelian yang didukung untuk instans T

- Instans Sesuai Permintaan
- Instans Terpesan
- Instans Khusus (khusus T3)
- Host Khusus (khusus T3, hanya dalam mode `standard`)
- Instans Spot

Untuk informasi selengkapnya, lihat Opsi penagihan dan pembelian Amazon EC2.

Daftar Isi

- Praktik terbaik
- Konsep kunci untuk instance kinerja yang dapat meledak
- Mode tidak terbatas untuk instans performa yang dapat melonjak
- Mode standar untuk instans performa yang dapat melonjak
- Konfigurasikan instance kinerja burstable
- Pantau kredit CPU untuk instans burstable

Praktik terbaik

Ikuti praktik terbaik ini untuk mendapatkan keuntungan maksimal dari instans performa yang dapat melonjak.

- Pastikan ukuran instans yang Anda pilih memenuhi persyaratan memori minimum sistem operasi dan aplikasi Anda. Sistem operasi dengan antarmuka pengguna grafis yang menggunakan banyak memori dan sumber daya CPU (misalnya, Windows) mungkin memerlukan ukuran instans `t3.micro` atau yang lebih besar untuk banyak kasus penggunaan. Seiring bertambahnya kebutuhan memori dan CPU untuk beban kerja Anda dari waktu ke waktu, Anda memiliki fleksibilitas dengan instans T untuk menskalakan ke ukuran instans yang lebih besar dengan tipe instans yang sama, atau untuk memilih tipe instans lainnya.
- Aktifkan AWS Compute Optimizer untuk akun Anda dan tinjau rekomendasi Compute Optimizer untuk beban kerja Anda. Compute Optimizer dapat membantu menilai apakah ukuran instans harus ditingkatkan untuk meningkatkan performa atau diperkecil untuk penghematan biaya. Compute Optimizer juga dapat merekomendasikan tipe instans yang berbeda berdasarkan skenario Anda. Untuk informasi selengkapnya, lihat Melihat rekomendasi instans EC2 dalam Panduan Pengguna AWS Compute Optimizer .

Konsep kunci untuk instance kinerja yang dapat meledak

Tipe instans Amazon EC2 tradisional menyediakan sumber daya CPU tetap, sementara instans performa yang dapat melonjak menyediakan tingkat pemanfaatan CPU dasar dengan kemampuan untuk melonjakkan pemanfaatan CPU di atas tingkat dasar. Hal ini memastikan Anda membayar hanya untuk CPU dasar dan lonjakan penggunaan CPU tambahan, sehingga biaya komputasi menjadi lebih rendah. Pemanfaatan dasar dan kemampuan untuk melonjak diatur oleh kredit CPU. Instans performa yang dapat melonjak adalah satu-satunya tipe instans yang menggunakan kredit untuk penggunaan CPU.

Setiap instans performa yang dapat melonjak terus-menerus mendapatkan kredit ketika tetap di bawah garis dasar CPU, dan terus-menerus menghabiskan kredit ketika melonjak di atas garis dasar. Jumlah kredit yang diperoleh atau dihabiskan tergantung pemanfaatan CPU dari instans:

- Jika pemanfaatan CPU di bawah garis dasar, maka kredit yang diperoleh lebih besar dari kredit yang dihabiskan.
- Jika pemanfaatan CPU sama dengan garis dasar, maka kredit yang diperoleh sama dengan kredit yang dihabiskan.

- Jika pemanfaatan CPU lebih tinggi dari garis dasar, maka kredit yang dihabiskan lebih tinggi dari kredit yang diperoleh.

Ketika kredit yang didapatkan lebih besar dari kredit yang dihabiskan, maka perbedaannya disebut kredit yang masih harus diperoleh, yang dapat digunakan kemudian untuk melonjak di atas pemanfaatan CPU dasar. Demikian pula, ketika kredit yang dihabiskan lebih dari kredit yang diperoleh, maka perilaku instans bergantung pada mode konfigurasi kredit—mode Standar atau mode Tak Terbatas.

Dalam mode Standar, ketika kredit yang dihabiskan lebih dari kredit yang didapatkan, maka instans akan menggunakan kredit yang masih harus diperoleh untuk melonjak di atas pemanfaatan CPU dasar. Jika kredit masih harus diperoleh sudah tidak tersisa, maka instans secara bertahap turun ke pemanfaatan CPU dasar dan tidak dapat melonjak di atas dasar sampai instans memperoleh kredit lebih.

Dalam mode Tidak Terbatas, jika instans melonjak di atas pemanfaatan CPU dasar, maka instans menggunakan kredit yang masih harus diperoleh terlebih dahulu untuk melonjak. Jika kredit yang masih harus diperoleh sudah tidak tersisa, maka instans menghabiskan kredit surplus untuk melonjak. Ketika pemanfaatan CPU-nya turun di bawah garis dasar, instans tersebut menggunakan kredit CPU yang didapatkan untuk membayar kredit surplus yang dihabiskan sebelumnya. Kemampuan untuk mendapatkan kredit CPU untuk mengurangi kredit surplus memungkinkan Amazon EC2 untuk meratakan penggunaan CPU dari sebuah instans selama periode 24 jam. Jika penggunaan CPU rata-rata selama periode 24 jam melebihi acuan, instans akan dikenai biaya untuk penggunaan tambahan dengan tarif tambahan flat per jam vCPU.

Daftar Isi

- Konsep utama dan definisi
- Mendapatkan kredit CPU
- Tingkat pendapatan kredit CPU
- Batas akrual kredit CPU
- Masa pakai kredit CPU yang masih harus diperoleh
- Pemanfaatan acuan

Konsep utama dan definisi

Konsep utama dan definisi berikut yang berlaku untuk instans performa yang dapat melonjak.

Pemanfaatan CPU

Pemanfaatan CPU adalah persentase unit komputasi EC2 yang dialokasikan yang saat ini digunakan pada instans. Metrik ini mengukur persentase siklus CPU yang dialokasikan yang sedang dimanfaatkan pada instans. CloudWatch Metrik Pemanfaatan CPU menunjukkan penggunaan CPU per instance dan bukan penggunaan CPU per inti. Spesifikasi CPU dasar dari sebuah instans juga didasarkan pada penggunaan CPU per instans. Untuk mengukur pemanfaatan CPU menggunakan Konsol Manajemen AWS atau AWS CLI, lihatMendapatkan statistik untuk instans tertentu.

Kredit CPU

Satu unit vCPU-waktu.

Contoh:

1 kredit CPU = 1 vCPU * 100% pemanfaatan * 1 menit.

1 kredit CPU = 1 vCPU * 50% pemanfaatan * 2 menit

1 kredit CPU = 2 vCPU * 25% pemanfaatan * 2 menit

Pemanfaatan acuan

Pemanfaatan acuan adalah tingkat di mana CPU dapat digunakan dengan saldo kredit bersih sebesar nol, ketika jumlah kredit CPU yang diperoleh sesuai dengan jumlah kredit CPU yang digunakan. Pemanfaatan dasar juga dikenal sebagai garis dasar. Pemanfaatan dasar dinyatakan sebagai persentase pemanfaatan vCPU, yang dihitung sebagai berikut: Pemanfaatan dasar% = (jumlah kredit v) /60 menit. earned/number CPUs

Untuk pemanfaatan dasar setiap tipe instans performa yang dapat melonjak, lihat tabel kredit.

Kredit yang diperoleh

Kredit yang diperoleh secara terus-menerus oleh sebuah instans saat sedang berjalan.

Jumlah kredit yang diperoleh per jam =% pemanfaatan baseline * jumlah v CPUs * 60 menit

Contoh:

Sebuah t3.nano dengan 2 v CPUs dan pemanfaatan dasar 5% menghasilkan 6 kredit per jam, dihitung sebagai berikut:

2 v CPUs * 5% baseline * 60 menit = 6 kredit per jam

Kredit yang dihabiskan atau digunakan

Kredit digunakan secara terus-menerus oleh sebuah instans ketika sedang berjalan.

Kredit CPU yang dihabiskan per menit = Jumlah v CPUs * Pemanfaatan CPU* 1 menit

Kredit yang masih harus diperoleh

Kredit CPU yang tidak terpakai ketika sebuah instans menggunakan kredit lebih sedikit daripada yang diperlukan untuk pemanfaatan dasar. Dengan kata lain, kredit yang masih harus diperoleh = (Kredit yang didapatkan – Kredit yang digunakan) di bawah pemanfaatan dasar.

Contoh

Jika t3.nano berjalan pada 2% pemanfaatan CPU, yang berada 5% di bawah garis dasar selama satu jam, maka kredit yang masih harus diperoleh dihitung sebagai berikut:

Kredit CPU yang masih harus dibayar = (Kredit yang diperoleh per jam - Kredit yang digunakan per jam) = 6 - 2 v CPUs * 2% pemanfaatan CPU * 60 menit = 6 - 2,4 = 3,6 kredit yang masih harus dibayar per jam

Batas akrual kredit

Tergantung ukuran instans, tetapi secara umum sama dengan jumlah kredit maksimum yang didapatkan dalam 24 jam.

Contoh

Untuk t3.nano, batas akrual kredit = 24 * 6 = 144 kredit

Kredit yang diluncurkan

Hanya berlaku untuk instans T2 yang dikonfigurasi pada mode Standar. Kredit peluncuran adalah jumlah kredit CPU terbatas yang dialokasikan untuk instans T2 baru sehingga ketika diluncurkan dalam mode Standar, dapat melonjak di atas acuan.

Kredit surplus

Kredit yang dihabiskan oleh sebuah instans setelah menghabiskan saldo kredit yang masih harus diperoleh. Kredit surplus didesain untuk instans yang dapat melonjak agar dapat mempertahankan performa tinggi dalam jangka waktu yang lama, dan hanya digunakan dalam mode Tidak Terbatas. Saldo kredit surplus digunakan untuk menentukan jumlah banyak kredit yang digunakan oleh instans untuk melonjak dalam mode Tidak Terbatas.

Mode standar

Mode konfigurasi kredit yang memungkinkan instans melonjak di atas garis dasar dengan menghabiskan kredit yang telah diperoleh dalam saldo kredit.

Mode tidak terbatas

Mode konfigurasi kredit yang memungkinkan instans untuk melonjak di atas garis dasar dengan mempertahankan pemanfaatan CPU yang tinggi untuk jangka waktu kapan pun diperlukan. Harga instans per jam secara otomatis mencakup semua fluktuasi penggunaan CPU jika penggunaan CPU rata-rata dari instans sama dengan atau di bawah acuan selama periode 24 jam yang berkelanjutan atau masa pakai instans, mana saja yang lebih pendek. Jika instans berjalan pada pemanfaatan CPU yang lebih tinggi untuk waktu yang lama, instans dapat melakukannya dengan tarif tambahan tetap per jam vCPU.

Tabel berikut merangkum perbedaan utama kredit antara tipe-tipe instans yang dapat melonjak.

Tipe	Tipe kredit CPU yang didukung	Mode konfigurasi kredit	Masa pakai kredit CPU akumulasi antara instans mulai dan berhenti
Generasi terbaru			
T4g	Kredit yang diperoleh, Kredit akrual, Kredit yang digunakan, Surplus kredit (hanya pada mode Tidak Terbatas)	Standar, Tidak Terbatas (default)	7 hari (kredit bertahan selama 7 hari setelah instans berhenti)
T3a	Kredit yang diperoleh, Kredit akrual, Kredit yang digunakan, Surplus kredit (hanya pada mode Tidak Terbatas)	Standar, Tidak Terbatas (default)	7 hari (kredit bertahan selama 7 hari setelah instans berhenti)

Tipe	Tipe kredit CPU yang didukung	Mode konfigurasi kredit	Masa pakai kredit CPU akumulasi antara instans mulai dan berhenti
T3	Kredit yang diperoleh, Kredit akrual, Kredit yang digunakan, Surplus kredit (hanya pada mode Tidak Terbatas)	Standar, Tidak Terbatas (default)	7 hari (kredit bertahan selama 7 hari setelah instans berhenti)
Generasi sebelumnya			
T2	Kredit yang diperoleh, Kredit akumulasi, Kredit yang digunakan, Kredit peluncuran (mode Standar saja), Kredit surplus (hanya ode Tak Terbatas)	Standar (default), Tidak Terbatas	0 hari (kredit hilang saat instans berhenti)

> **Note**
>
> Mode Tidak Terbatas tidak didukung untuk instans T3 yang diluncurkan pada Host Khusus.

Mendapatkan kredit CPU

Setiap instans performa yang dapat melonjak terus-menerus mendapatkan (pada resolusi tingkat milidetik) tingkat kredit CPU yang ditetapkan per jam, tergantung ukuran instans. Proses penghitungan apakah kredit bertambah atau dihabiskan juga terjadi pada resolusi tingkat milidetik, jadi Anda tidak perlu khawatir tentang pengeluaran kredit CPU yang berlebihan. Lonjakan singkat CPU menggunakan sebagian kecil kredit CPU.

Jika instans performa yang dapat melonjak menggunakan lebih sedikit sumber daya CPU daripada yang diperlukan untuk pemanfaatan dasar (seperti saat menganggur), kredit CPU yang tidak terpakai

akan ditambahkan ke saldo kredit CPU. Jika instans performa yang dapat melonjak perlu melonjak di atas tingkat pemanfaatan dasar, instans tersebut menghabiskan kredit yang masih harus diperoleh. Makin banyak kredit yang diperoleh oleh instans performa yang dapat melonjak, makin banyak waktu untuk melonjak melebihi garis dasarnya saat memerlukan lebih banyak pemanfaatan CPU.

Tabel berikut mencantumkan jenis instance kinerja burstable, tingkat di mana kredit CPU diperoleh per jam, jumlah maksimum kredit CPU yang diperoleh yang dapat diperoleh instance, jumlah v CPUs per instance, dan pemanfaatan dasar sebagai persentase dari inti penuh (menggunakan vCPU tunggal).

Tipe instans	Kredit CPU didapatkan per jam	Kredit maksimum yang diperoleh yang dapat terakumulasi*	v CPUs ***	Pemanfaatan acuan per vCPU
T2				
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**
t2.xlarge	54	1296	4	22,5% **
t2.2xlarge	81,6	1958.4	8	17%**
T3				
t3.nano	6	144	2	5%**
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**

Tipe instans	Kredit CPU didapatkan per jam	Kredit maksimum yang diperoleh yang dapat terakumulasi*	v CPUs ***	Pemanfaatan acuan per vCPU
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**
T4g				
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.2xlarge	192	4608	8	40%**

* Jumlah kredit yang dapat diperoleh setara dengan jumlah kredit yang bisa didapatkan dalam periode 24 jam.

** Pemanfaatan acuan persentase dalam tabel adalah per vCPU. Di CloudWatch , Pemakaian CPU ditampilkan per vCPU. Misalnya, pemanfaatan CPU untuk `t3.large` instance yang beroperasi pada tingkat dasar ditampilkan sebagai 30% dalam CloudWatch metrik CPU. Untuk informasi tentang cara menghitung pemanfaatan dasar, lihat Pemanfaatan acuan.

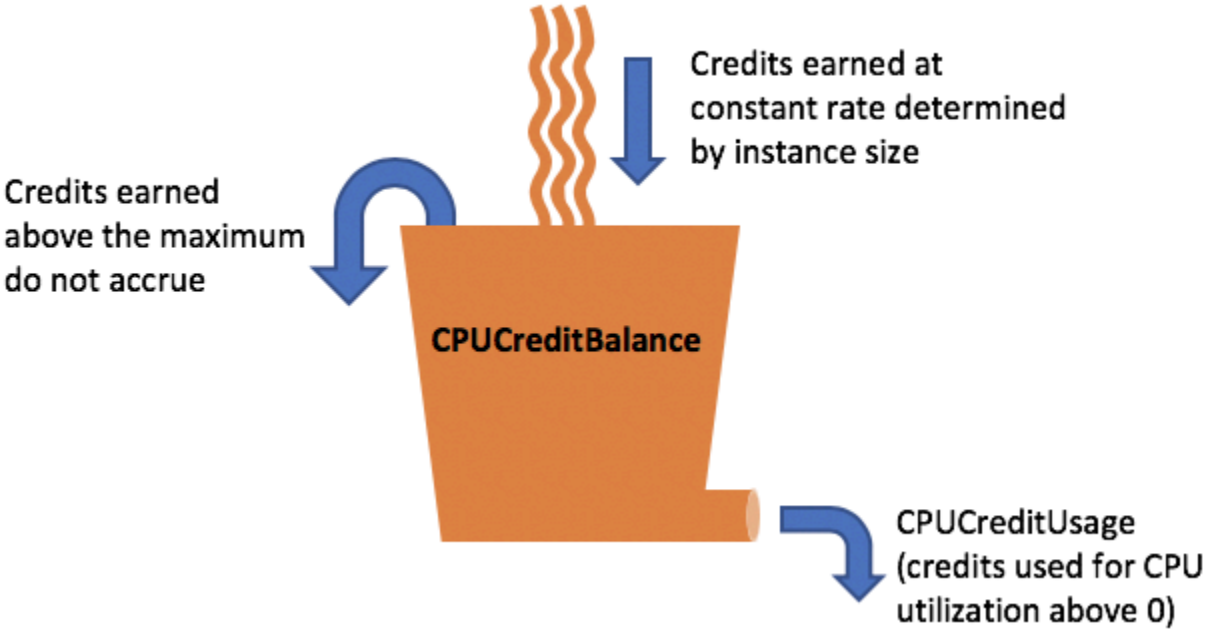
*** Tiap vCPU adalah thread dari inti Intel Xeon atau core AMD EPYC, kecuali untuk instans T2 dan T4g.

Tingkat pendapatan kredit CPU

Jumlah kredit CPU yang didapatkan per jam ditentukan oleh ukuran instans. Misalnya, `t3.nano` mendapatkan enam kredit per jam, sementara `t3.small` mendapatkan 24 kredit per jam. Tabel sebelumnya mencantumkan tingkat pendapatan kredit untuk semua instans.

Batas akrual kredit CPU

Meskipun kredit yang didapatkan tidak pernah kedaluwarsa pada instans yang berjalan, ada batasan jumlah kredit yang didapatkan yang dapat diperoleh sebuah instans. Batas tersebut ditentukan oleh batas saldo kredit CPU. Setelah batas tercapai, semua kredit baru yang didapatkan akan dibuang, seperti yang ditunjukkan pada gambar berikut. Bucket penuh menunjukkan batas saldo kredit CPU, dan spillover menunjukkan pendapatan baru kredit yang melebihi batas.



Batas saldo kredit CPU berbeda untuk setiap ukuran instans. Misalnya, instans `t3.micro` dapat memperoleh maksimum 288 kredit CPU yang didapatkan dalam saldo kredit CPU. Tabel sebelumnya mencantumkan jumlah maksimum kredit yang didapatkan yang dapat diperoleh setiap instans.

Instans T2 Standard juga mendapatkan kredit peluncuran. Kredit peluncuran tidak dihitung dalam batas saldo kredit CPU. Jika instans T2 tidak menghabiskan kredit peluncurannya, dan tetap menganggur selama 24 jam sambil memperoleh kredit yang diperoleh, saldo kredit CPU-nya akan muncul karena melebihi batas. Untuk informasi selengkapnya, lihat Kredit yang diluncurkan.

Instans T4G, T3a, dan T3 tidak mendapatkan kredit peluncuran. Instans ini diluncurkan sebagai `unlimited` secara default, sehingga dapat langsung melonjak saat memulai tanpa kredit peluncuran apa pun. Instans T3 diluncurkan pada peluncuran Host Khusus sebagai `standard` secara default; mode `unlimited` tidak didukung untuk instans T3 pada Host Khusus.

Masa pakai kredit CPU yang masih harus diperoleh

Kredit CPU pada instans yang berjalan tidak kedaluwarsa.

Untuk T2, saldo kredit CPU tidak bertahan antara instans berhenti dan mulai. Jika Anda menghentikan instans T2, instans tersebut kehilangan semua kredit yang masih harus diperoleh.

Untuk T4G, T3a, dan T3, saldo kredit CPU bertahan selama tujuh hari setelah instance berhenti dan kredit hilang setelahnya. Jika Anda memulai instans dalam tujuh hari, tidak ada kredit yang hilang.

Untuk informasi lebih lanjut, lihat`CPUCreditBalance` dalam CloudWatch tabel metrik.

Pemanfaatan acuan

Pemanfaatan acuan adalah tingkat di mana CPU dapat digunakan dengan saldo kredit bersih sebesar nol, ketika jumlah kredit CPU yang diperoleh sesuai dengan jumlah kredit CPU yang digunakan. Pemanfaatan dasar juga dikenal sebagai garis dasar.

Pemanfaatan acuan dinyatakan sebagai persentase pemanfaatan vCPU, yang dihitung sebagai berikut:

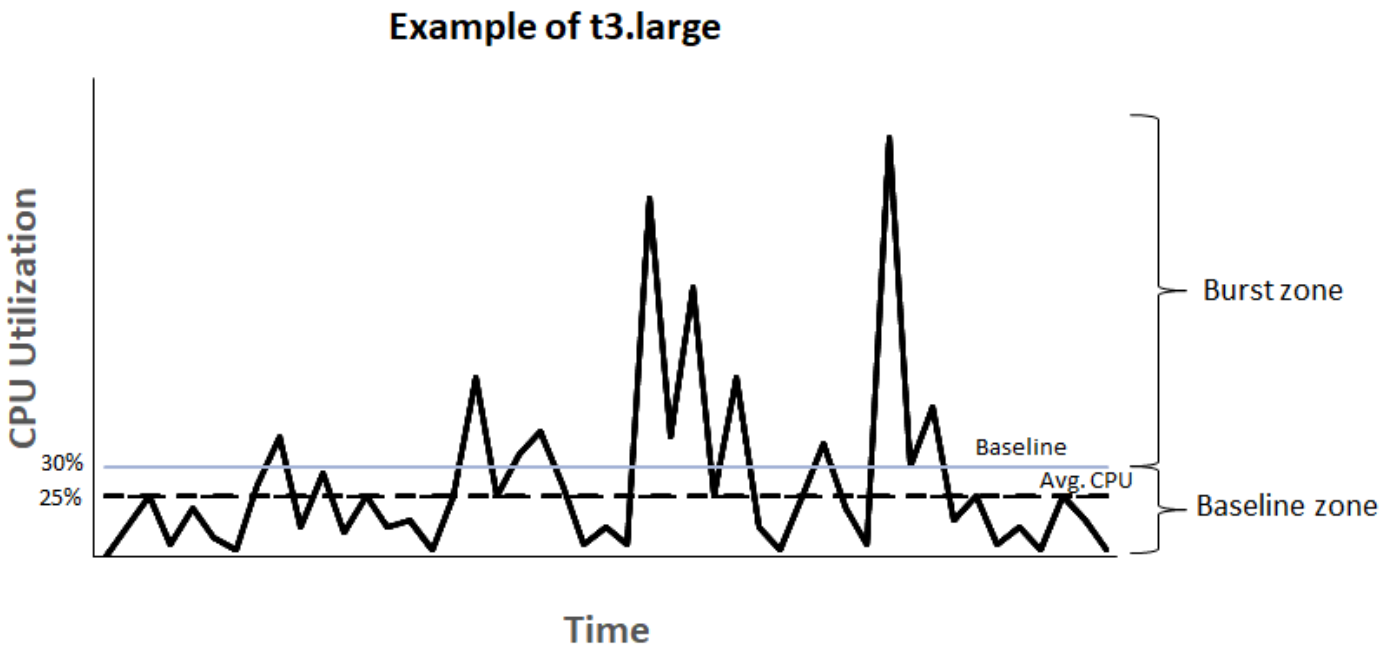
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline utilization
```

Misalnya, sebuah `t3.nano` instance, dengan 2 vCPUs, menghasilkan 6 kredit per jam, menghasilkan pemanfaatan dasar 5%, yang dihitung sebagai berikut:

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Sebuah `t3.large` contoh, dengan 2 vCPUs, menghasilkan 36 kredit per jam, menghasilkan pemanfaatan dasar 30% (). `(36/2)/60`

Grafik berikut memberikan contoh penggunaan CPU rata-rata di bawah baseline. `t3.large`



Mode tidak terbatas untuk instans performa yang dapat melonjak

Instans performa yang dapat melonjak yang dikonfigurasi sebagai `unlimited` dapat mempertahankan pemanfaatan CPU yang tinggi untuk periode waktu kapan pun saat diperlukan. Harga instans per jam secara otomatis mencakup semua fluktuasi penggunaan CPU jika penggunaan CPU rata-rata dari instans sama dengan atau di bawah acuan selama periode 24 jam yang berkelanjutan atau masa pakai instans, mana saja yang lebih pendek.

Untuk sebagian besar beban kerja tujuan umum, instans dikonfigurasi yang sebagai `unlimited` memberikan performa yang cukup tanpa biaya tambahan. Jika instans berjalan pada pemakaian CPU yang lebih tinggi untuk waktu yang lama, instans dapat melakukannya dengan tarif tambahan tetap per jam vCPU. Untuk informasi tentang harga, lihat Harga Amazon EC2 dan Harga Mode Tak Terbatas T2/T3/T4.

Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan Anda menggunakan `t3.micro` contoh `t2.micro` atau di bawah AWS Tingkat Gratispenawaran dan menggunakannya dalam `unlimited` mode, biaya mungkin berlaku jika penggunaan rata-rata Anda selama periode 24 jam bergulir melebihi penggunaan dasar instans.

Instans T4G, T3a, dan T3 diluncurkan sebagai `unlimited` default (kecuali jika Anda mengubah default). Jika rata-rata pemanfaatan CPU selama periode 24 jam melebihi garis dasar, Anda dikenai biaya untuk kredit surplus. Jika Anda meluncurkan Instans Spot `unlimited` sebagai dan berencana segera menggunakannya dan untuk durasi yang singkat, tanpa waktu menganggur untuk memperoleh kredit CPU, Anda dikenai biaya untuk kredit surplus. Kami menyarankan Anda meluncurkan Instans Spot dalam mode standar untuk menghindari pembayaran biaya yang lebih tinggi. Untuk informasi selengkapnya, lihat Kredit surplus dapat dikenakan biaya dan Luncurkan instance kinerja yang dapat meledak.

> **Note**
>
> Instans T3 diluncurkan pada peluncuran Host Khusus sebagai `standard` secara default; mode `unlimited` tidak didukung untuk instans T3 pada Host Khusus.

Daftar Isi

- Konsep mode tak terbatas untuk instance burstable
  - Cara kerja instans performa yang dapat melonjak Tidak Terbatas
  - Kapan menggunakan mode tak terbatas versus CPU tetap

- Kredit surplus dapat dikenakan biaya
- Berapa biaya kinerja burstable tanpa batas?
- Tidak ada kredit peluncuran untuk instans T2 Tidak Terbatas
- Mengaktifkan mode tidak terbatas
- Yang terjadi pada kredit saat beralih antara Tidak Terbatas dan Standar
- Memantau penggunaan kredit

- Contoh mode tak terbatas untuk instance burstable
  - Contoh 1: Menjelaskan penggunaan kredit dengan T3 Tidak Terbatas
  - Contoh 2: Menjelaskan penggunaan kredit dengan T2 Tidak Terbatas

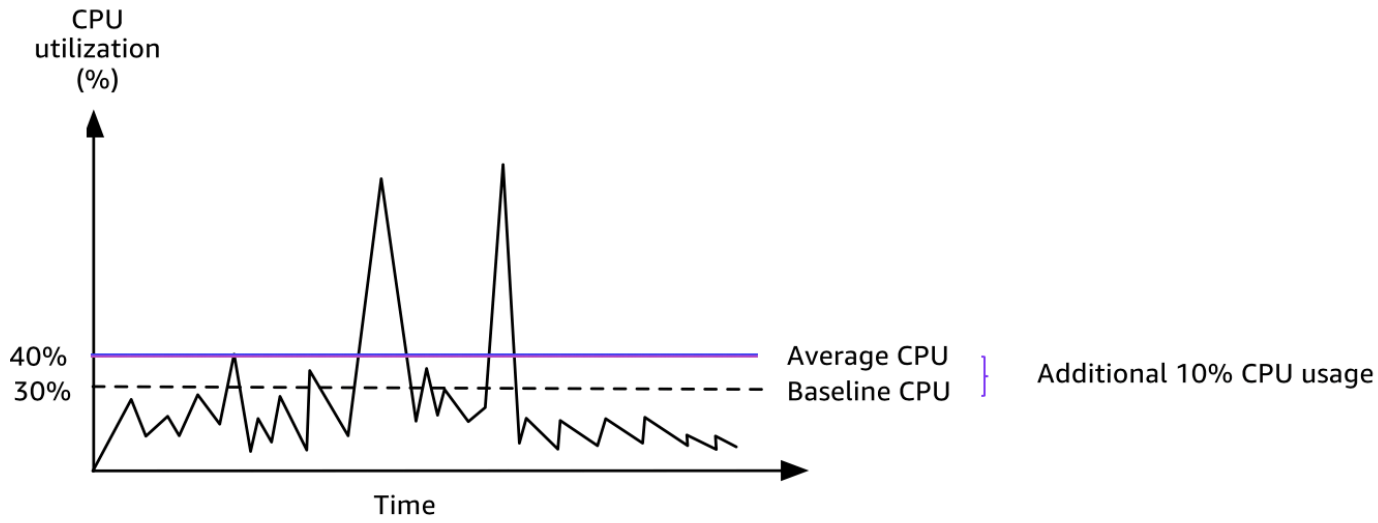
Konsep mode tak terbatas untuk instance burstable

Mode `unlimited` adalah opsi konfigurasi kredit untuk instans performa yang dapat melonjak. Mode ini dapat diaktifkan atau dinonaktifkan kapan saja untuk instans yang berjalan atau dihentikan. Anda dapat menetapkan `unlimited` sebagai opsi kredit default di tingkat akun per AWS Wilayah, per keluarga instans performa burstable, sehingga semua instance performa burstable baru di akun diluncurkan menggunakan opsi kredit default.

Cara kerja instans performa yang dapat melonjak Tidak Terbatas

Jika instans performa yang dapat melonjak yang dikonfigurasi sebagai `unlimited` menghabiskan saldo kredit CPU-nya, Instans tersebut dapat menggunakan kredit surplus untuk melampaui batas dasar. Ketika pemanfaatan CPU-nya turun di bawah garis dasar, instans tersebut menggunakan kredit CPU yang didapatkan untuk membayar kredit surplus yang dihabiskan sebelumnya. Kemampuan untuk mendapatkan kredit CPU untuk mengurangi kredit surplus memungkinkan Amazon EC2 untuk meratakan penggunaan CPU dari sebuah instans selama periode 24 jam. Jika penggunaan CPU rata-rata selama periode 24 jam melebihi acuan, instans akan dikenai biaya untuk penggunaan tambahan dengan tarif tambahan flat per jam vCPU.

Grafik berikut menunjukkan penggunaan CPU `t3.large`. Pemanfaatan CPU dasar untuk `t3.large` adalah 30%. Jika instans berjalan pada pemakaian CPU 30% atau kurang secara rata-rata selama periode 24 jam, tidak ada biaya tambahan karena biaya tersebut sudah tercakup oleh harga per jam instans. Namun, jika instans berjalan dengan rata-rata 40% pemanfaatan CPU selama 24 jam, seperti yang ditunjukkan dalam grafik, maka instans tersebut akan ditagih untuk 10% penggunaan CPU tambahan dengan tarif tambahan tetap per jam vCPU.



Untuk informasi selengkapnya tentang pemanfaatan acuan per vCPU untuk setiap tipe instans dan jumlah kredit yang didapatkan oleh setiap tipe instans, lihat tabel kredit.

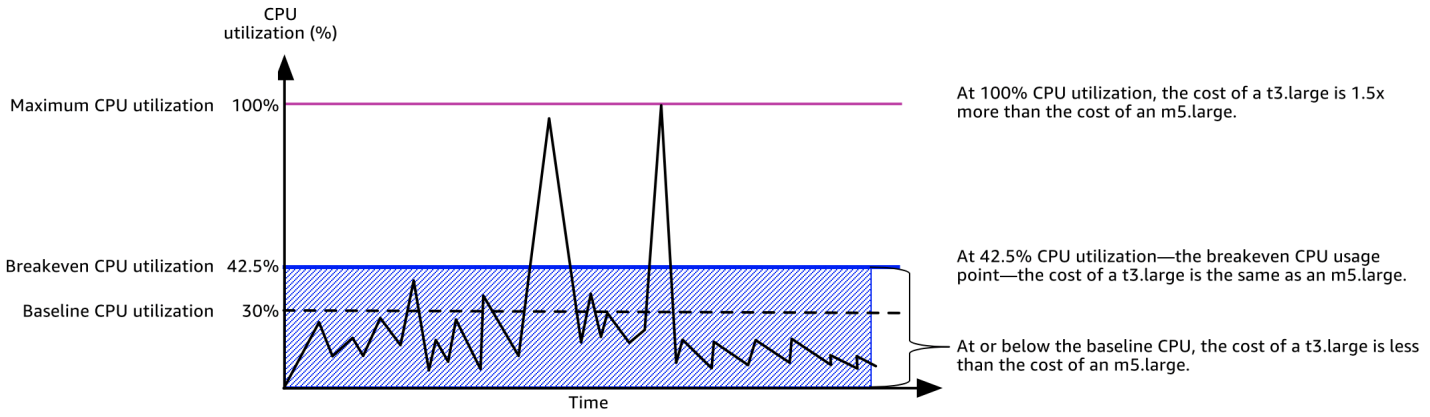
Kapan menggunakan mode tak terbatas versus CPU tetap

Saat menentukan apakah Anda harus menggunakan instans performa yang dapat melonjak dalam mode`unlimited`, seperti T3, atau instans performa tetap, seperti M5, Anda perlu menentukan penggunaan CPU yang impas. Penggunaan CPU yang impas untuk instans performa yang dapat melonjak adalah titik di mana instans performa yang dapat melonjak harganya sama dengan instans performa tetap. Penggunaan CPU yang impas membantu Anda menentukan hal berikut:

- Jika penggunaan CPU rata-rata selama periode 24 jam sama dengan atau di bawah penggunaan impas CPU, gunakan instans performa yang dapat melonjak di mode `unlimited` sehingga Anda bisa mendapatkan keuntungan dari harga yang lebih rendah dari instans performa yang dapat melonjak sekaligus mendapatkan kinerja yang sama sebagai instans performa tetap.
- Jika penggunaan CPU rata-rata selama periode 24 jam di atas penggunaan impas CPU, instans performa yang dapat melonjak akan lebih mahal daripada instans performa tetap yang berukuran setara. Jika instans T3 terus-menerus melonjak pada 100% CPU, Anda akan membayar sekitar 1,5 kali harga instans M5 yang berukuran setara.

Grafik berikut menunjukkan titik penggunaan impas CPU di mana biaya `t3.large` sama dengan `m5.large`. Titik penggunaan CPU yang impas untuk `t3.large` adalah 42,5%. Jika penggunaan CPU rata-rata adalah 42,5%, biaya menjalankan `t3.large` sama dengan `m5.large`, dan lebih mahal jika penggunaan CPU rata-rata di atas 42,5%. Jika beban kerja membutuhkan penggunaan

CPU rata-rata kurang dari 42,5%, Anda dapat memperoleh keuntungan dari harga `t3.large` yang lebih rendah sekaligus mendapatkan performa yang sama sebagai `m5.large`.



Tabel berikut menunjukkan cara menghitung ambang batas penggunaan impas CPU, sehingga Anda dapat menentukan kapan lebih murah untuk menggunakan instans performa yang dapat melonjak dalam mode `unlimited` atau instans performa tetap. Kolom di tabel diberi label A sampai K.

Tipe instans	v CPUs	Harga T3*/ jam	Harga M5*/ jam	Perbedaan harga	Pemanfaatan acuan T3 per vCPU (%)	Biaya per jam vCPU untuk kredit surplus	Biaya per menit vCPU	Menit lonjakan tambahan tersedia per vCPU	% CPU tambahan tersedia	% CPU titik impas
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	$0,0835	$0,096	$0,0125	30%	$0,05	$0,00083	15	12,5%	42,5%

* Harga berdasarkan us-east-1 dan Linux OS.

Tabel tersebut memberikan informasi berikut:

- Kolom A menunjukkan tipe instans, `t3.large`.

- Kolom B menunjukkan jumlah v CPUs untuk`t3.large`.
- Kolom C menunjukkan harga `t3.large` per jam.
- Kolom D menunjukkan harga `m5.large` per jam.
- Kolom E menunjukkan perbedaan harga antara `t3.large` dan `m5.large`.
- Kolom F menunjukkan pemanfaatan batas dasar per vCPU dari `t3.large`, yaitu 30%. Pada batas dasar, biaya per jam dari instans mencakup biaya penggunaan CPU.
- Kolom G menunjukkan tarif tambahan flat per jam vCPU yang dikenakan pada instans jika melonjak ke 100% CPU setelah kredit yang diperolehnya habis.
- Kolom H menunjukkan tarif tambahan flat per jam vCPU-menit yang dikenakan pada instans jika melonjak ke 100% CPU setelah kredit yang diperolehnya habis.
- Kolom I menunjukkan jumlah menit tambahan yang dapat dilonjakkan oleh `t3.large` per jam pada 100% CPU sementara membayar harga yang sama per jam sebagai `m5.large`.
- Kolom J menunjukkan penggunaan CPU tambahan (dalam %) di atas batas dasar yang instansnya dapat melonjak sementara membayar harga yang sama per jam sebagai `m5.large`.
- Kolom K menunjukkan penggunaan CPU yang impas (dalam %) sehingga `t3.large` dapat melonjak tanpa harus membayar lebih dari `m5.large`. Apa pun di atas ini, dan biaya `t3.large` lebih dari `m5.large`.

Tabel berikut menunjukkan penggunaan CPU yang impas (dalam%) untuk tipe instans T3 dibandingkan dengan tipe instans M5 yang berukuran serupa.

Tipe instans T3	Penggunaan CPU yang impas (dalam %) untuk T3 dibandingkan dengan M5
`t3.large`	42,5%
`t3.xlarge`	52,5%
`t3.2xlarge`	52,5%

Kredit surplus dapat dikenakan biaya

Jika pemanfaatan CPU rata-rata dari sebuah instans berada pada atau di bawah batas dasar, instans tersebut tidak dikenakan biaya tambahan. Karena sebuah instans memperoleh jumlah kredit

maksimum dalam periode 24 jam (misalnya, instans `t3.micro` dapat memperoleh maksimum 288 kredit dalam periode 24 jam), instans tersebut dapat menggunakan kredit surplus hingga maksimum itu tanpa dikenakan biaya.

Namun, jika pemanfaatan CPU tetap di atas batas dasar, instans tidak dapat memperoleh kredit yang cukup untuk membayar surplus kredit yang telah digunakan. Kredit surplus yang tidak dibayarkan akan dikenakan tarif tambahan tetap per vCPU-jam. Untuk informasi tentang tarif, lihat Harga Mode Tidak Terbatas T2/T3/T4g.

Kredit surplus yang digunakan lebih awal dikenai tagihan jika salah satu dari hal berikut terjadi:

- Kredit surplus yang digunakan melebihi jumlah kredit maksimum yang dapat diperoleh instans dalam periode 24 jam. Kredit surplus yang digunakan di atas jumlah maksimum akan ditagihkan pada akhir jam.
- Instans dihentikan atau diakhiri.
- instans dialihkan dari `unlimited` ke `standard`.

Kredit surplus yang dihabiskan dilacak oleh metrik. CloudWatch `CPUSurplusCreditBalance`
Kredit surplus yang dibebankan dilacak oleh metrik. CloudWatch `CPUSurplusCreditsCharged`
Untuk informasi selengkapnya, lihat CloudWatch Metrik tambahan untuk instans performa burstable.

Berapa biaya kinerja burstable tanpa batas?

Jika Anda menggunakan kredit surplus dan tidak dibayar dengan kredit yang diperoleh (lihatKredit surplus dapat dikenakan biaya), Anda membayar tarif tambahan tetap per VCPU-jam untuk kredit surplus. Tarif tercantum di bagian Harga Mode Tidak Terbatas T2/T3/T4G T2/T3 Harga Mode Tidak Terbatas Amazon EC2.

Tidak ada kredit peluncuran untuk instans T2 Tidak Terbatas

Instans T2 Standar menerima kredit peluncuran, tetapi tidak dengan instans T2 Tidak Terbatas. Instans T2 Tidak Terbatas dapat melonjak melampaui batas dasar kapan saja tanpa biaya tambahan, selama rata-rata penggunaan CPU berada pada atau di bawah batas dasar selama jangka waktu 24 jam bergulir atau masa pakainya, mana yang lebih pendek. Dengan demikian, instans T2 Tidak Terbatas tidak memerlukan kredit peluncuran untuk mencapai performa tinggi segera setelah peluncuran.

Jika instans T2 dialihkan dari `standard` ke `unlimited`, semua kredit peluncuran yang terkumpul dihapus dari `CPUCreditBalance` sebelum sisa `CPUCreditBalance` diteruskan.

Instans T4G, T3a, dan T3 tidak pernah menerima kredit peluncuran karena diluncurkan dalam mode Tidak Terbatas secara default, dan karenanya dapat meledak segera setelah memulai. Konfigurasi kredit mode Tidak Terbatas memungkinkan instans T4G, T3a, dan T3 menggunakan CPU sebanyak yang diperlukan untuk melampaui baseline dan selama diperlukan.

Mengaktifkan mode tidak terbatas

Anda dapat beralih dari `unlimited` ke `standard`, dan dari `standard` ke `unlimited`, kapan saja pada instans yang berjalan atau dihentikan. Untuk informasi selengkapnya, lihat Konfigurasikan spesifikasi kredit saat peluncuran dan Kelola spesifikasi kredit dari instance kinerja yang dapat meledak.

Anda dapat menetapkan `unlimited` sebagai opsi kredit default di tingkat akun per AWS Wilayah, per keluarga instans performa burstable, sehingga semua instance performa burstable baru di akun diluncurkan menggunakan opsi kredit default. Untuk informasi selengkapnya, lihat Mengelola spesifikasi kredit default untuk akun.

Anda dapat memeriksa apakah instans performa yang dapat melonjak Anda dikonfigurasi sebagai `unlimited` atau `standard` menggunakan konsol Amazon EC2 atau AWS CLI. Untuk informasi selengkapnya, lihat Konfigurasikan instance kinerja burstable.

Yang terjadi pada kredit saat beralih antara Tidak Terbatas dan Standar

`CPUCreditBalance`adalah CloudWatch metrik yang melacak jumlah kredit yang diperoleh oleh sebuah instance. `CPUSurplusCreditBalance`adalah CloudWatch metrik yang melacak jumlah kredit surplus yang dihabiskan oleh sebuah instance.

Jika Anda mengubah instans yang dikonfigurasi sebagai `unlimited` ke `standard`, hal berikut ini terjadi:

- Nilai `CPUCreditBalance` tetap tidak berubah dan diteruskan.
- Nilai `CPUSurplusCreditBalance` segera dikenakan tagihan.

Jika instans `standard` dialihkan ke `unlimited`, hal berikut ini terjadi:

- Nilai `CPUCreditBalance` yang berisi kredit yang diperoleh yang masih harus dibayar diteruskan.
- Untuk instans T2 Standard, semua kredit peluncuran dihapus dari`CPUCreditBalance` nilai, dan sisanya`CPUCreditBalance` nilai yang mengandung kredit yang diperoleh yang masih harus dibayar diteruskan.

Memantau penggunaan kredit

Untuk melihat apakah instans Anda menghabiskan lebih banyak kredit daripada yang disediakan baseline, Anda dapat menggunakan CloudWatch metrik untuk melacak penggunaan, dan Anda dapat mengatur alarm per jam untuk diberi tahu tentang penggunaan kredit. Untuk informasi selengkapnya, lihat Pantau kredit CPU untuk instans burstable.

Contoh mode tak terbatas untuk instance burstable

Contoh berikut menjelaskan penggunaan kredit untuk instans yang dikonfigurasi sebagai `unlimited`.

Contoh

- Contoh 1: Menjelaskan penggunaan kredit dengan T3 Tidak Terbatas
- Contoh 2: Menjelaskan penggunaan kredit dengan T2 Tidak Terbatas

Contoh 1: Menjelaskan penggunaan kredit dengan T3 Tidak Terbatas

Dalam contoh ini, Anda melihat pemanfaatan CPU dari instans `t3.nano` yang diluncurkan sebagai `unlimited`, dan caranya menggunakan kredit yang diperoleh dan surplus untuk mempertahankan pemanfaatan CPU.

Instans `t3.nano` memperoleh 144 kredit CPU selama periode 24 jam bergulir, yang dapat ditukarkan dengan 144 menit penggunaan vCPU. Ketika menghabiskan saldo kredit CPU-nya (diwakili oleh CloudWatch metrik`CPUCreditBalance`), ia dapat menghabiskan kelebihan kredit CPU — yang belum diperoleh — untuk meledak selama yang dibutuhkan. Karena instans `t3.nano` memperoleh maksimal 144 kredit dalam jangka waktu 24 jam, instans ini dapat menggunakan kredit surplus hingga maksimum tersebut tanpa langsung dikenakan biaya. Jika menghabiskan lebih dari 144 kredit CPU, instans ini akan dikenakan biaya untuk selisihnya di akhir jam.

Maksud dari contoh tersebut, yang diilustrasikan oleh grafik berikut, adalah untuk menunjukkan bagaimana sebuah instans dapat melonjak menggunakan surplus kredit bahkan setelah instans tersebut menghabiskan `CPUCreditBalance`. Alur kerja berikut mereferensikan titik-titik bernomor pada grafik:

P1 - Pada 0 jam pada grafik, instans diluncurkan sebagai `unlimited` dan langsung mulai mendapatkan kredit. Instans tetap diam sejak diluncurkan, yang artinya pemakaian CPU 0%, sehingga tidak ada kredit yang digunakan. Semua kredit yang tidak terpakai diakumulasi ke dalam

saldo kredit. Selama 24 jam pertama, `CPUCreditUsage` berada di 0, dan nilai `CPUCreditBalance` mencapai maksimum 144.

P2 - Untuk 12 jam ke depan, pemanfaatan CPU berada pada 2,5%, yang masih di bawah acuan 5%. Instans mendapatkan lebih banyak kredit daripada yang dibelanjakan, tetapi`CPUCreditBalance` nilai tidak dapat melebihi maksimum 144 kredit.

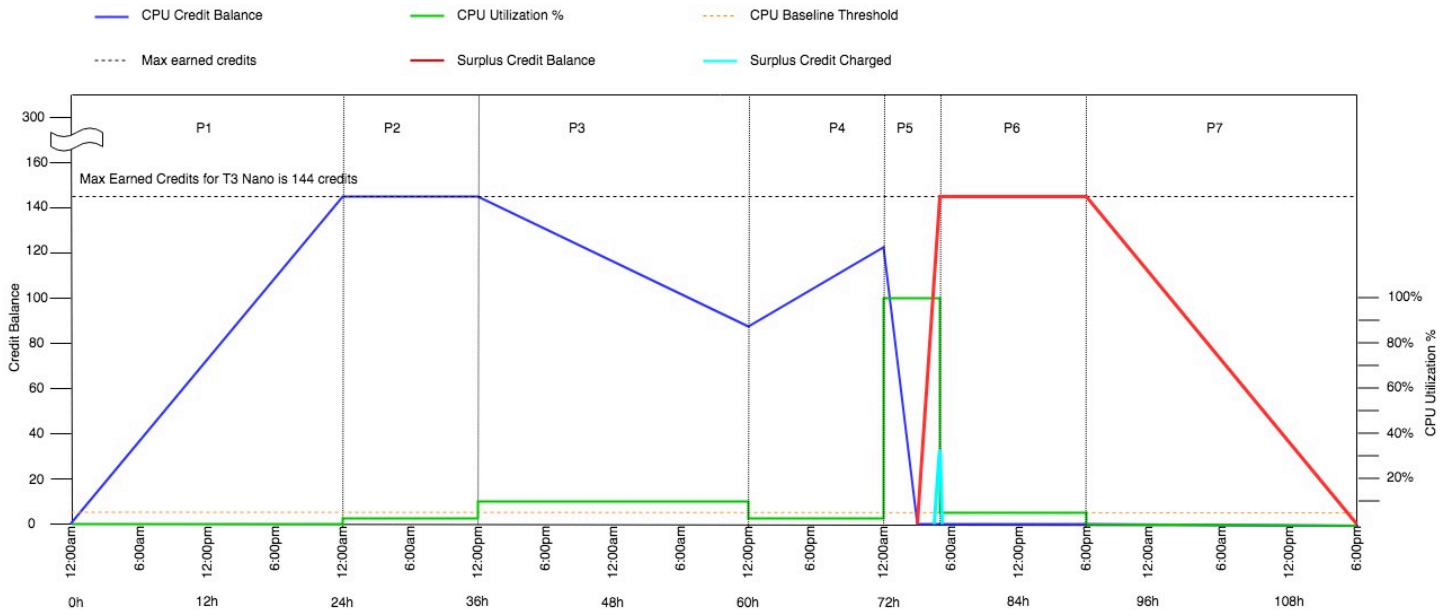
P3 - Untuk 24 jam ke depan, penggunaan CPU berada pada 7% (di atas acuan), yang membutuhkan penggunaan 57,6 kredit. Instans menggunakan lebih banyak kredit daripada yang diperolehnya, dan nilai `CPUCreditBalance` berkurang menjadi 86,4 kredit.

P4 - Selama 12 jam ke depan, pemanfaatan CPU menurun jadi 2,5% (di bawah acuan), yang membutuhkan penggunaan 36 kredit. Pada saat yang sama, instans tersebut mendapatkan 72 kredit. Instance mendapatkan lebih banyak kredit daripada yang dibelanjakan, dan`CPUCreditBalance` nilai meningkat menjadi 122 kredit.

P5 - Untuk 5 jam ke depan, instans meningkatkan pemanfaatan 100% CPU, dan menggunakan total 570 kredit untuk mempertahankan lonjakan. Sekitar satu jam dalam periode ini, instans menghabiskan seluruh `CPUCreditBalance` sebesar 122 kredit, dan mulai menggunakan kredit surplus untuk mempertahankan penggunaan CPU yang tinggi, dengan total 448 kredit surplus dalam periode ini (570-122=448). Saat nilai `CPUSurplusCreditBalance` mencapai 144 kredit CPU (maksimum yang dapat diperoleh instans `t3.nano` dalam periode 24 jam), kredit surplus yang digunakan setelahnya tidak dapat diimbangi dengan kredit yang diperoleh. Kredit surplus yang dihabiskan setelahnya berjumlah 304 kredit (448-144=304), yang menghasilkan sedikit biaya tambahan pada akhir jam untuk 304 kredit.

P6 - Untuk 13 jam ke depan, pemanfaatan CPU berada pada 5% (batas dasar). Instans tersebut mendapatkan kredit sebanyak yang digunakan, tanpa kelebihan untuk membayar `CPUSurplusCreditBalance`. Nilai `CPUSurplusCreditBalance` tetap sebesar 144 kredit.

P7 - Selama 24 jam terakhir dalam contoh ini, instans tidak aktif dan pemanfaatan CPU adalah 0%. Selama waktu ini, instans memperoleh 144 kredit, yang digunakan untuk membayar `CPUSurplusCreditBalance`.



Contoh 2: Menjelaskan penggunaan kredit dengan T2 Tidak Terbatas

Dalam contoh ini, Anda melihat pemanfaatan CPU dari instans `t2.nano` yang diluncurkan sebagai `unlimited`, dan caranya menggunakan kredit yang diperoleh dan surplus untuk mempertahankan pemanfaatan CPU.

Instans `t2.nano` memperoleh 72 kredit CPU selama periode 24 jam bergulir, yang dapat ditukarkan dengan 72 menit penggunaan vCPU. Ketika menghabiskan saldo kredit CPU-nya (diwakili oleh CloudWatch metrik`CPUCreditBalance`), ia dapat menghabiskan kelebihan kredit CPU — yang belum diperoleh — untuk meledak selama yang dibutuhkan. Karena instans `t2.nano` memperoleh maksimal 72 kredit dalam jangka waktu 24 jam, instans ini dapat menggunakan kredit surplus hingga maksimum tersebut tanpa langsung dikenakan biaya. Jika menghabiskan lebih dari 72 kredit CPU, instans ini akan dikenakan biaya untuk selisihnya di akhir jam.

Maksud dari contoh tersebut, yang diilustrasikan oleh grafik berikut, adalah untuk menunjukkan cara sebuah instans dapat melonjak menggunakan kredit surplus bahkan setelah instans tersebut menghabiskan `CPUCreditBalance`. Anda dapat mengasumsikan bahwa, pada awal lini waktu dalam grafik, instans memiliki saldo kredit yang masih harus didapat dengan besaran yang sama dengan jumlah kredit maksimum yang dapat diperoleh dalam 24 jam. Alur kerja berikut mereferensikan titik-titik bernomor pada grafik:

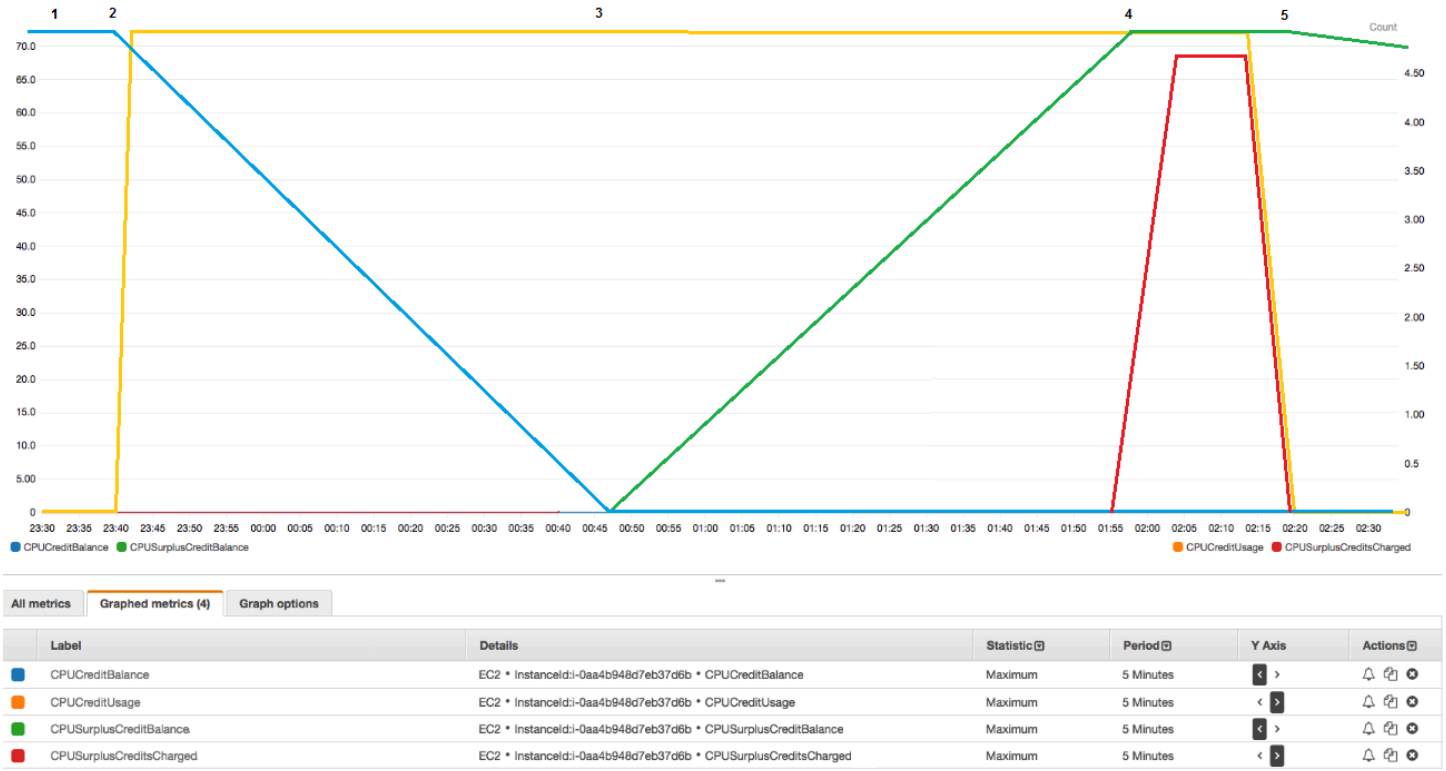
1 – Dalam 10 menit pertama, `CPUCreditUsage` berada di 0, dan nilai `CPUCreditBalance` tetap maksimal sebesar 72.

2 – Pada pukul 23:40, seiring dengan meningkatnya pemanfaatan CPU, instans menggunakan kredit CPU dan nilai `CPUCreditBalance` menurun.

3 – Sekitar pukul 00:47, instans menghabiskan seluruh `CPUCreditBalance`, dan mulai menggunakan kredit surplus untuk mempertahankan pemanfaatan CPU yang tinggi.

4 – Kredit Surplus dihabiskan sampai 01:55, saat nilai `CPUSurplusCreditBalance` mencapai 72 kredit CPU. Jumlah ini sama dengan maksimum yang dapat dihasilkan oleh instans `t2.nano` dalam periode 24 jam. Kredit surplus apa pun yang digunakan setelahnya tidak dapat diimbangi dengan kredit yang diperoleh dalam periode 24 jam, yang menghasilkan sedikit biaya tambahan di akhir jam.

5 – Instans terus menggunakan kredit surplus hingga sekitar pukul 02:20. Pada waktu ini, pemanfaatan CPU berada di bawah batas dasar, dan instans mulai memperoleh kredit sebesar 3 kredit per jam (atau 0,25 kredit setiap 5 menit), yang digunakan untuk membayar `CPUSurplusCreditBalance`. Setelah nilai `CPUSurplusCreditBalance` berkurang hingga menjadi 0, instans mulai mengumpulkan kredit yang diperoleh di `CPUCreditBalance` sebesar 0,25 kredit setiap 5 menit.



All metrics | Graphed metrics (4) | Graph options

Label	Details	Statistic	Period	Y Axis	Actions
CPUCreditBalance	EC2 • InstanceId:i-0aa4b948d7eb37d6b • CPUCreditBalance	Maximum	5 Minutes		
CPUCreditUsage	EC2 • InstanceId:i-0aa4b948d7eb37d6b • CPUCreditUsage	Maximum	5 Minutes		
CPUSurplusCreditBalance	EC2 • InstanceId:i-0aa4b948d7eb37d6b • CPUSurplusCreditBalance	Maximum	5 Minutes		
CPUSurplusCreditsCharged	EC2 • InstanceId:i-0aa4b948d7eb37d6b • CPUSurplusCreditsCharged	Maximum	5 Minutes		

Menghitung tagihan (instance Linux)

Kredit surplus biaya $0.05 per VCPU-jam. Instans menggunakan sekitar 25 kredit surplus antara 01:55 dan 02:20, yang setara dengan 0,42 vCPU-jam. Biaya tambahan untuk contoh ini adalah 0,42

VCPU-jam x $0,05/VCPU-jam = $0,021, dibulatkan menjadi $0,02. Berikut adalah tagihan akhir bulan untuk instans T2 Tidak Terbatas ini:

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

Menghitung tagihan (instance Windows)

Kredit surplus biaya $0.096 per VCPU-jam. Instans menggunakan sekitar 25 kredit surplus antara 01:55 dan 02:20, yang setara dengan 0,42 vCPU-jam. Biaya tambahan untuk contoh ini adalah 0,42 VCPU-jam x $0,096/VCPU-jam = $0,04032, dibulatkan menjadi $0,04. Berikut adalah tagihan akhir bulan untuk instans T2 Tidak Terbatas ini:

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

Anda dapat mengatur peringatan penagihan agar diberi tahu setiap jam tentang biaya yang timbul, dan mengambil tindakan jika diperlukan.

Mode standar untuk instans performa yang dapat melonjak

Instans performa yang dapat melonjak yang dikonfigurasi sebagai `standard` cocok untuk beban kerja dengan pemanfaatan CPU rata-rata yang secara konsisten di bawah pemanfaatan CPU batas dasar dari instans. Untuk melonjak di atas batas dasar, instans menggunakan kredit yang telah diakumulasikan dalam saldo kredit CPU. Jika instans hampir kehabisan kredit yang masih harus dibayar, pemanfaatan CPU secara bertahap diturunkan ke batas dasar, sehingga instans tidak mengalami penurunan performa yang tajam saat saldo kredit CPU yang masih harus dibayar habis. Untuk informasi selengkapnya, lihat Konsep kunci untuk instance kinerja yang dapat meledak.

Daftar Isi

- Konsep mode standar untuk instance burstable
  - Cara kerja instans performa yang dapat melonjak standar

- Kredit yang diluncurkan
- Batas kredit peluncuran
- Perbedaan antara kredit peluncuran dan kredit yang diperoleh
- Contoh mode standar untuk instance burstable
  - Contoh 1: Menjelaskan penggunaan kredit dengan T3 Standa
  - Contoh 2: Menjelaskan penggunaan kredit dengan T2 Standar
    - Periode 1: 1 – 24 jam
    - Periode 2: 25 – 36 jam
    - Periode 3: 37 – 61 jam
    - Periode 4: 62 – 72 jam
    - Periode 5: 73 – 75 jam
    - Periode 6: 76 – 90 jam
    - Periode 7: 91 – 96 jam

Konsep mode standar untuk instance burstable

Mode `standard` adalah opsi konfigurasi untuk instans performa yang dapat melonjak. Mode ini dapat diaktifkan atau dinonaktifkan kapan saja untuk instans yang berjalan atau dihentikan. Anda dapat menetapkan `standard` sebagai opsi kredit default di tingkat akun per AWS Wilayah, per keluarga instans performa burstable, sehingga semua instance performa burstable baru di akun diluncurkan menggunakan opsi kredit default.

Cara kerja instans performa yang dapat melonjak standar

Saat instans performa yang dapat melonjak dikonfigurasi sebagai `standard` berada dalam status berjalan, instans ini secara terus-menerus memperoleh (pada resolusi tingkat milidetik) set tingkat kredit yang diperoleh per jam. Untuk T2 Standar, saat instans dihentikan, semua kredit yang masih harus dibayar hilang, dan saldo kreditnya direset ke nol. Saat dimulai ulang, instans ini menerima set kredit peluncuran baru, dan mulai mengakumulasi kredit yang diperoleh. Untuk instans Standar T4G, T3a, dan T3, saldo kredit CPU bertahan selama tujuh hari setelah instans berhenti dan kredit hilang setelahnya. Jika Anda memulai instans dalam tujuh hari, tidak ada kredit yang hilang.

Instans T2 Standar menerima dua jenis kredit CPU: kredit yang diperoleh dan kredit peluncuran. Saat instans T2 Standar berada dalam status berjalan, instans ini secara terus-menerus memperoleh (pada resolusi tingkat milidetik) set tingkat kredit yang diperoleh per jam. Pada awalnya, instans ini

belum mendapatkan kredit untuk pengalaman startup yang baik; oleh karena itu, untuk memberikan pengalaman memulai yang baik, instans ini menerima kredit peluncuran di awal, yang digunakan pertama kali saat memperoleh kredit yang diakumulasi.

Instans T4G, T3a, dan T3 tidak menerima kredit peluncuran karena mendukung mode Tidak Terbatas. Konfigurasi kredit mode Tidak Terbatas memungkinkan instans T4G, T3a, dan T3 menggunakan CPU sebanyak yang diperlukan untuk melampaui baseline dan selama diperlukan.

Kredit yang diluncurkan

Instans T2 Standard mendapatkan 30 kredit peluncuran per vCPU saat diluncurkan atau dimulai, dan instans T1 Standard mendapatkan 15 kredit peluncuran. Misalnya, sebuah `t2.micro` instance memiliki satu vCPU dan mendapat 30 kredit peluncuran, sedangkan `t2.xlarge` instance memiliki empat v CPUs dan mendapat 120 kredit peluncuran. Kredit peluncuran didesain untuk memberikan pengalaman memulai yang baik untuk memungkinkan instans melonjak segera setelah peluncuran sebelum mereka memperoleh kredit yang diakumulasi.

Kredit peluncuran digunakan terlebih dahulu, sebelum kredit yang diperoleh. Kredit peluncuran yang tidak terpakai diakumulasikan dalam saldo kredit CPU, tetapi tidak dihitung dalam batas saldo kredit CPU. Misalnya, instans `t2.micro` memiliki batas saldo kredit CPU 144 kredit yang diperoleh. Jika instans diluncurkan dan tetap idle selama 24 jam, saldo kredit CPU mencapai 174 (30 kredit peluncuran + 144 kredit yang diperoleh), yang melebihi batas. Namun, setelah instans menggunakan 30 kredit peluncuran, saldo kredit tidak boleh melebihi 144. Untuk informasi selengkapnya tentang batas saldo kredit CPU untuk setiap ukuran instans, lihat tabel kredit.

Tabel berikut mencantumkan alokasi kredit CPU awal yang diterima saat peluncuran atau awal, dan jumlah vCPUs.

Tipe instans	Kredit yang diluncurkan	v CPUs
`t1.micro`	15	1
`t2.nano`	30	1
`t2.micro`	30	1
`t2.small`	30	1
`t2.medium`	60	2

Tipe instans	Kredit yang diluncurkan	v CPUs
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

Batas kredit peluncuran

Ada batasan berapa kali instans T2 Standar dapat menerima kredit peluncuran. Batas default-nya adalah 100 peluncuran atau permulaan semua instans T2 Standard yang digabungkan per akun, per Wilayah, per periode 24 jam bergulir. Misalnya, batas tercapai saat satu instans dihentikan dan dimulai 100 kali dalam periode 24 jam, atau saat 100 instans diluncurkan dalam periode 24 jam, atau kombinasi lain yang setara dengan 100 permulaan. Akun baru mungkin memiliki batas bawah, yang akan meningkat seiring waktu berdasarkan penggunaan Anda.

> **Tip**
>
> Untuk memastikan bahwa beban kerja Anda selalu mendapatkan performa yang dibutuhkan, beralihlah ke Mode tidak terbatas untuk instans performa yang dapat melonjak atau pertimbangkan untuk menggunakan ukuran instans yang lebih besar.

Perbedaan antara kredit peluncuran dan kredit yang diperoleh

Tabel berikut mencantumkan perbedaan antara kredit peluncuran dan kredit yang diperoleh.

	Kredit yang diluncurkan	Kredit yang diperoleh
Tingkat perolehan kredit	Instans T2 Standar memperoleh 30 kredit peluncuran per vCPU saat diluncurkan atau dimulai. Jika instans T2 dialihkan dari `unlimited` ke `standard`, instans ini tidak mendapatkan kredit peluncuran pada saat peralihan.	Setiap instans performa yang dapat melonjak T2 terus-menerus memperoleh (pada resolusi tingkat milidetik) tingkat kredit CPU yang ditetapkan per jam, bergantung pada ukuran instans. Untuk informasi selengkapnya tentang

	Kredit yang diluncurkan	Kredit yang diperoleh
		jumlah kredit CPU yang diperoleh per ukuran instans, lihat tabel kredit.
Batas perolehan kredit	Batas untuk menerima kredit peluncuran adalah 100 peluncuran atau permulaan semua instans T2 Standard yang digabungkan per akun, per Wilayah, per periode 24 jam bergulir. Akun baru mungkin memiliki batas bawah, yang akan meningkat seiring waktu berdasarkan penggunaan Anda.	Instans T2 tidak dapat mengakumulasi lebih banyak kredit daripada batas saldo kredit CPU. Jika saldo kredit CPU telah mencapai batasnya, kredit apa pun yang diperoleh setelah batas tercapai akan dibuang. Kredit peluncuran tidak termasuk dalam penghitungan batas. Untuk informasi selengkapnya tentang batas saldo kredit CPU untuk tiap ukuran instans T2, lihat tabel kredit.
Penggunaan kredit	Kredit peluncuran digunakan terlebih dahulu, sebelum kredit yang diperoleh.	Kredit yang diperoleh hanya digunakan setelah semua kredit peluncuran dihabiskan.
Kedaluwarsa kredit	Saat instans T2 Standar berjalan, kredit peluncuran tidak kedaluwarsa. Saat instans T2 Standar berhenti atau dialihkan ke T2 Tidak Terbatas, semua kredit peluncuran hilang.	Saat instans T2 berjalan, kredit yang diperoleh yang diakumulasi tidak kedaluwarsa. Saat instans T2 berhenti, semua kredit yang diperoleh yang diakumulasi akan hilang.

Jumlah kredit peluncuran yang masih harus dibayar dan kredit yang diperoleh yang masih harus dibayar dilacak oleh metrik. CloudWatch `CPUCreditBalance` Untuk informasi lebih lanjut, lihat`CPUCreditBalance` dalam CloudWatch tabel metrik.

Contoh mode standar untuk instance burstable

Contoh berikut menjelaskan penggunaan kredit saat instans dikonfigurasi sebagai `standard`.

Contoh

- Contoh 1: Menjelaskan penggunaan kredit dengan T3 Standa
- Contoh 2: Menjelaskan penggunaan kredit dengan T2 Standar

Contoh 1: Menjelaskan penggunaan kredit dengan T3 Standa

Dalam contoh ini, Anda melihat cara instans `t3.nano` yang diluncurkan sebagai `standard` memperoleh, mengakumulasi, dan menggunakan kredit yang diperoleh. Anda melihat cara saldo kredit mencerminkan kredit yang diperoleh yang diakumulasi.

Instans `t3.nano` yang berjalan memperoleh 144 kredit setiap 24 jam. Batas saldo kreditnya adalah 144 kredit yang diperoleh. Setelah batas tercapai, kredit baru yang diperoleh akan dibuang. Untuk informasi selengkapnya tentang jumlah kredit yang dapat diperoleh dan diakumulasi, lihat tabel kredit.

Anda dapat meluncurkan instans T3 Standar dan segera menggunakannya. Atau, Anda dapat meluncurkan instans T3 Standar dan membiarkannya idle selama beberapa hari sebelum menjalankan aplikasi di dalamnya. Digunakan atau tidaknya suatu instans akan menentukan apakah kredit akan digunakan atau diakumulasi. Jika sebuah instans tetap idle selama 24 jam sejak diluncurkan, saldo kredit mencapai batasnya, yang merupakan jumlah maksimum kredit yang diperoleh yang dapat diakumulasi.

Contoh ini menjelaskan sebuah instans yang tetap diam selama 24 jam sejak diluncurkan, dan memandu Anda melalui tujuh periode waktu selama periode 96 jam, yang menunjukkan tingkat di mana kredit diperoleh, diperoleh, digunakan, dan dibuang, serta nilai saldo kredit pada setiap akhir periode.

Alur kerja berikut mereferensikan titik-titik bernomor pada grafik:

P1 - Pada 0 jam pada grafik, instans diluncurkan sebagai `standard` dan langsung mulai mendapatkan kredit. Instans tetap diam sejak diluncurkan, yang artinya pemakaian CPU 0%, sehingga tidak ada kredit yang digunakan. Semua kredit yang tidak terpakai diakumulasi ke dalam saldo kredit. Selama 24 jam pertama, `CPUCreditUsage` berada di 0, dan nilai `CPUCreditBalance` mencapai maksimum 144.

P2 - Untuk 12 jam ke depan, pemanfaatan CPU berada pada 2,5%, yang masih di bawah acuan 5%. Instans mendapatkan lebih banyak kredit daripada yang digunakan, tetapi nilai `CPUCreditBalance` tidak dapat melebihi maksimum 144 kredit. Setiap kredit yang diperoleh yang melebihi batas akan dibuang.

P3 - Untuk 24 jam ke depan, penggunaan CPU berada pada 7% (di atas acuan), yang membutuhkan penggunaan 57,6 kredit. Instans menggunakan lebih banyak kredit daripada yang diperolehnya, dan nilai `CPUCreditBalance` berkurang menjadi 86,4 kredit.

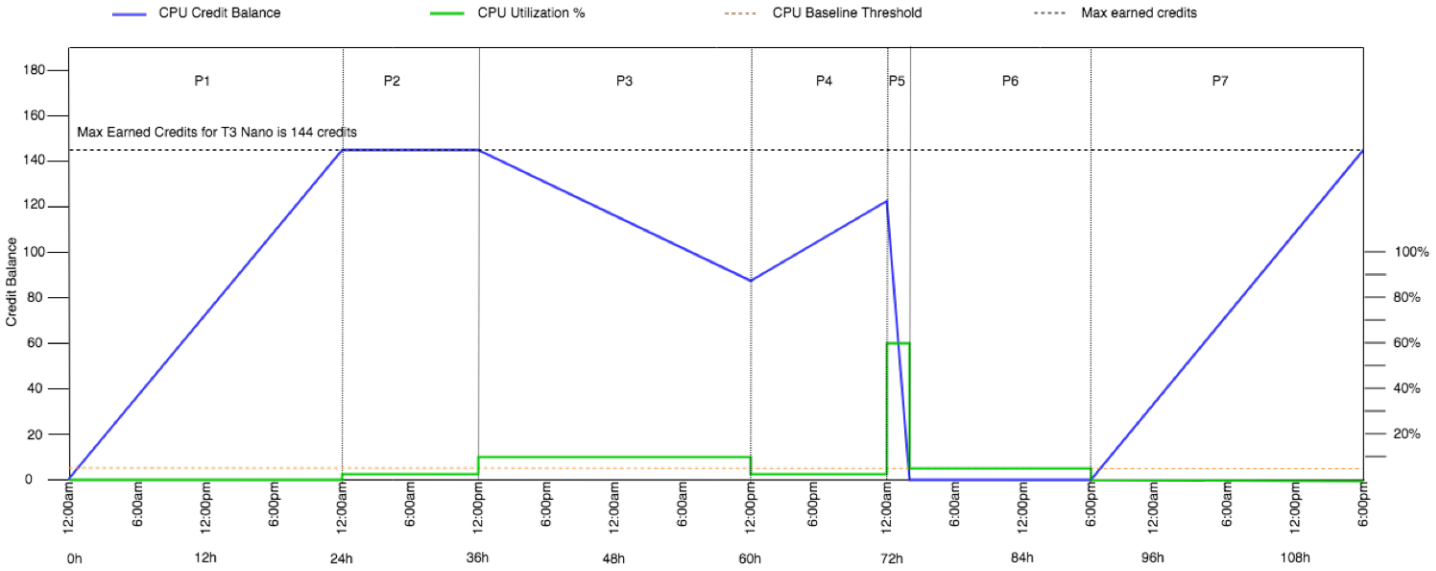
P4 - Selama 12 jam ke depan, pemanfaatan CPU menurun jadi 2,5% (di bawah acuan), yang membutuhkan penggunaan 36 kredit. Pada saat yang sama, instans tersebut mendapatkan 72 kredit.

Instans mendapatkan lebih banyak kredit daripada yang digunakan, dan nilai `CPUCreditBalance` meningkat menjadi 122 kredit.

P5 - Selama dua jam berikutnya, instans melonjak pada pemanfaatan 60% CPU, dan menghabiskan keseluruhan nilai `CPUCreditBalance` sebesar 122 kredit. Di akhir periode ini, dengan `CPUCreditBalance` berada di nol, pemanfaatan CPU dipaksa turun ke tingkat pemanfaatan garis dasar 5%. Pada garis dasar, instans mendapatkan kredit sebanyak yang digunakan.

P6 – Untuk 14 jam ke depan, pemanfaatan CPU berada pada 5% (garis dasar). Instans ini mendapatkan kredit sebanyak yang digunakan. Nilai `CPUCreditBalance` tetap 0.

P7 - Selama 24 jam terakhir dalam contoh ini, instans tidak aktif dan pemanfaatan CPU adalah 0%. Selama waktu ini, instans mendapatkan 144 kredit, yangn diakumulasi di `CPUCreditBalance`.



Contoh 2: Menjelaskan penggunaan kredit dengan T2 Standar

Dalam contoh ini, Anda melihat cara instans `t2.nano` yang diluncurkan sebagai `standard` memperoleh, mengakumulasi, dan menggunakan kredit peluncuran dan yang diperoleh. Anda melihat cara saldo kredit mencerminkan tidak hanya kredit yang diperoleh yang diakumulasi, tetapi juga kredit peluncuran diakumulasi.

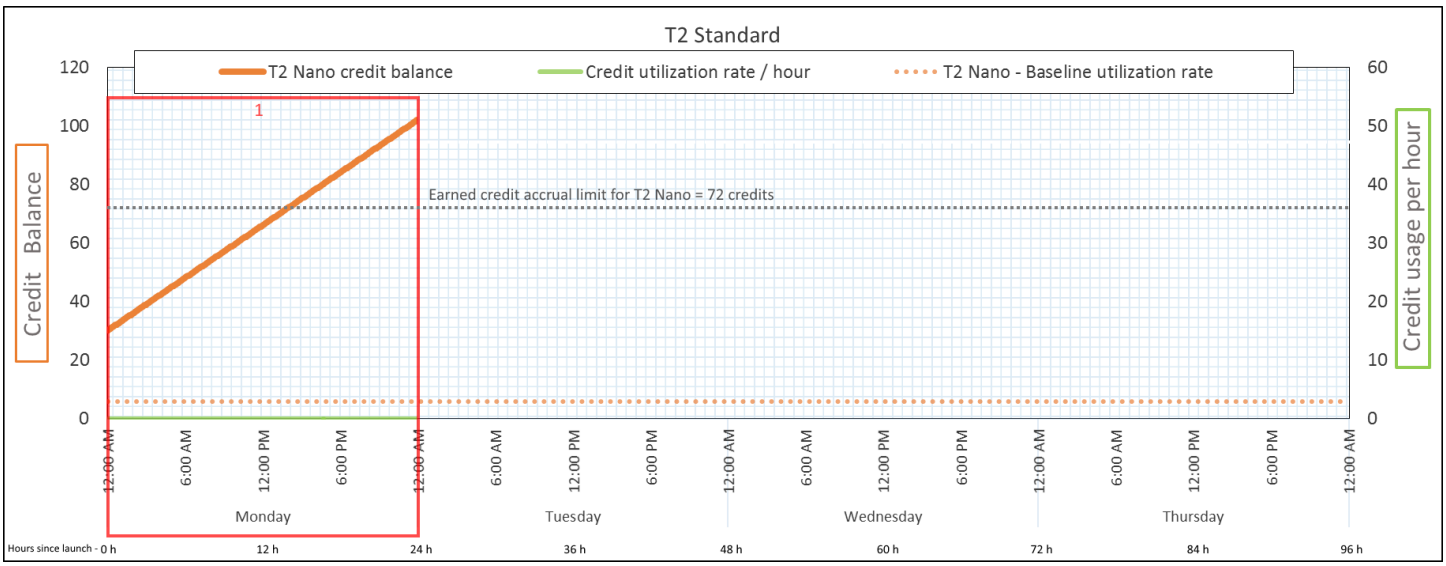
Sebuah instans `t2.nano` mendapat 30 kredit peluncuran saat diluncurkan, dan mendapatkan 72 kredit setiap 24 jam. Batas saldo kreditnya adalah 72 kredit yang diperoleh; kredit peluncuran tidak dihitung dalam batasan tersebut. Setelah batas tercapai, kredit baru yang diperoleh akan dibuang. Untuk informasi selengkapnya tentang jumlah kredit yang dapat diperoleh dan diakumulasi, lihat tabel kredit. Untuk informasi selengkapnya tentang batasn, lihat Batas kredit peluncuran.

Anda dapat meluncurkan instans T2 Standar dan segera menggunakannya. Atau, Anda dapat meluncurkan instans T2 Standar dan membiarkannya idle selama beberapa hari sebelum menjalankan aplikasi di dalamnya. Digunakan atau tidaknya suatu instans akan menentukan apakah kredit akan digunakan atau diakumulasi. Jika sebuah instans tetap idle selama 24 jam sejak diluncurkan, saldo kredit tampak melebihi batasnya karena saldo tersebut mencerminkan kredit yang diperoleh diakumulasi dan kredit peluncuran yang diakumulasi. Namun, setelah CPU digunakan, kredit peluncuran digunakan terlebih dahulu. Setelah itu, batas tersebut selalu mencerminkan jumlah maksimum kredit yang diperoleh yang dapat diakumulasi.

Contoh ini menjelaskan sebuah instans yang tetap diam selama 24 jam sejak diluncurkan, dan memandu Anda melalui tujuh periode waktu selama periode 96 jam, yang menunjukkan tingkat di mana kredit diperoleh, diperoleh, digunakan, dan dibuang, serta nilai saldo kredit pada setiap akhir periode.

Periode 1: 1 – 24 jam

Pada 0 jam pada grafik, instans T2 diluncurkan sebagai `standard` dan langsung mendapat 30 kredit peluncuran. Instans ini memperoleh kredit saat dalam kondisi berjalan. Instans tetap diam sejak diluncurkan, yang artinya pemakaian CPU 0%, sehingga tidak ada kredit yang digunakan. Semua kredit yang tidak terpakai diakumulasi ke dalam saldo kredit. Sekitar 14 jam setelah peluncuran, saldo kreditnya adalah 72 (30 kredit peluncuran + 42 kredit yang diperoleh), yang setara dengan yang dapat diperoleh instans dalam 24 jam. Pada 24 jam setelah peluncuran, saldo kredit melebihi 72 kredit karena kredit peluncuran yang tidak terpakai diakumulasikan ke saldo kredit—saldo kredit adalah 102 kredit: 30 kredit peluncuran + 72 kredit yang diperoleh.



Tingkat Penggunaan Kredit	0 kredit per 24 jam (pemanfaatan CPU 0%)
Tingkat Perolehan Kredit	72 kredit per 24 jam
Tingkat Pembuangan Kredit	0 kredit per 24 jam
Saldo Kredit	102 kredit (30 kredit peluncuran + 72 kredit yang diperoleh)

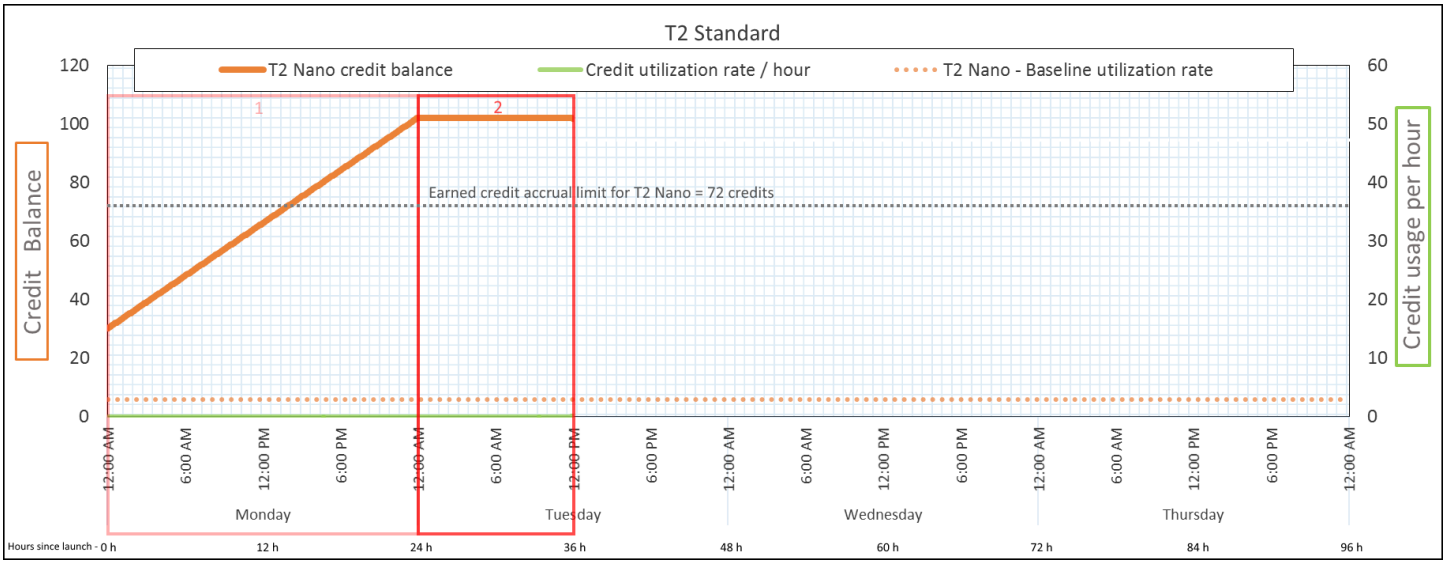
Kesimpulan

Jika tidak ada pemanfaatan CPU setelah peluncuran, instans memperoleh lebih banyak kredit daripada yang dapat diperolehnya dalam 24 jam (30 kredit peluncuran + 72 kredit yang diperoleh = 102 kredit).

Dalam skenario dunia nyata, instans EC2 menggunakan sejumlah kecil kredit saat meluncurkan dan menjalankan, yang mencegah saldo mencapai nilai teoretis maksimum dalam contoh ini.

Periode 2: 25 – 36 jam

Selama 12 jam berikutnya, instans terus idle dan memperoleh kredit, tetapi saldo kredit tidak bertambah. Saldo kredirt berhenti di 102 kredit (30 kredit peluncuran + 72 kredit yang diperoleh). Saldo kredit telah mencapai batas 72 kredit yang diperoleh yang diakumulasi, sehingga kredit yang baru diperoleh akan dibuang.



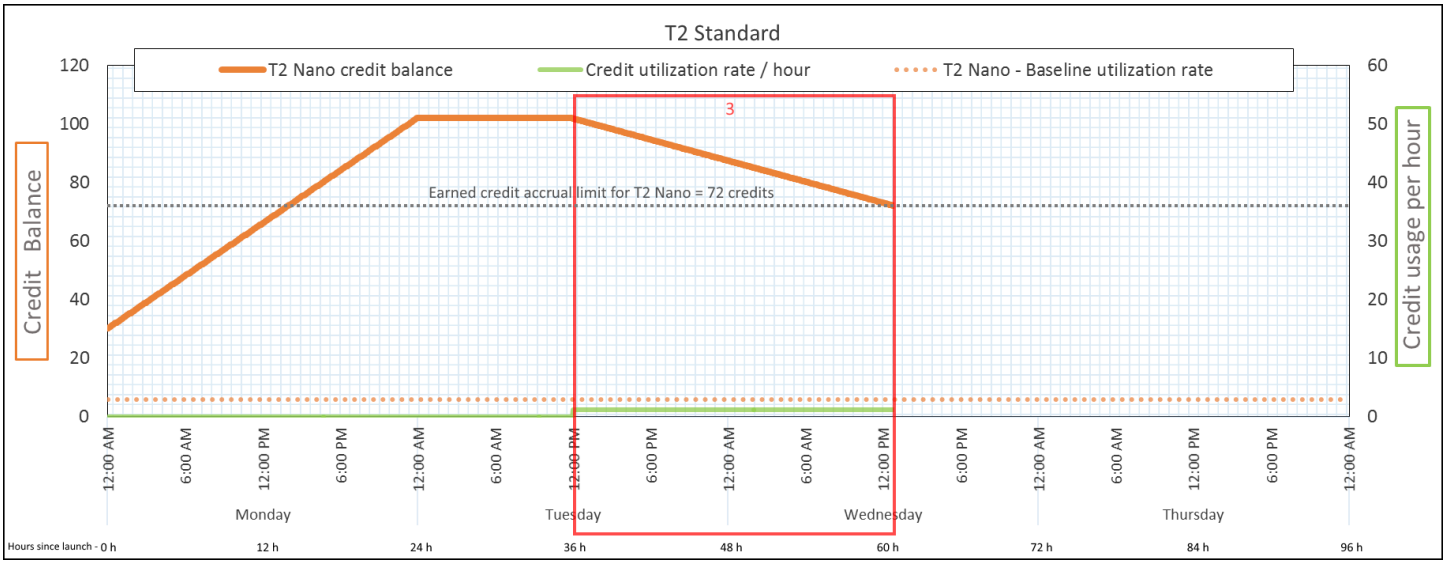
Tingkat Penggunaan Kredit	0 kredit per 24 jam (pemanfaatan CPU 0%)
Tingkat Perolehan Kredit	72 kredit per 24 jam (3 kredit per jam)
Tingkat Pembuangan Kredit	72 kredit per 24 jam (100% dari tingkat perolehan kredit)
Saldo Kredit	102 kredit (30 kredit peluncuran + 72 kredit yang diperoleh)—saldo tidak berubah

Kesimpulan

Sebuah instans terus-menerus memperoleh kredit, tetapi tidak dapat mengakumulasi lebih banyak kredit yang diperoleh jika saldo kredit telah mencapai batasnya. Setelah batasan tercapai, kredit yang baru diperoleh akan dibuang. Kredit peluncuran tidak termasuk dalam penghitungan batasan saldo kredit. Jika saldo termasuk kredit peluncuran yang diakumulasi, saldo tersebut tampak melebihi batas.

Periode 3: 37 – 61 jam

Selama 25 jam ke depan, instans menggunakan 2% CPU, yang membutuhkan 30 kredit. Pada periode yang sama memperoleh 75 kredit, tetapi saldo kredit menurun. Saldo menurun karena kredit peluncuran yang diakumulasi digunakan terlebih dahulu, sementara kredit yang baru diperoleh dibuang karena saldo kredit sudah mencapai batasan 72 kredit yang diperoleh.



Tingkat Penggunaan Kredit	28,8 kredit per 24 jam (1,2 kredit per jam, 2% pemanfaatan CPU, 40% dari tingkat perolehan kredit) —30 kredit selama 25 jam
Tingkat Perolehan Kredit	72 kredit per 24 jam
Tingkat Pembuangan Kredit	72 kredit per 24 jam (100% dari tingkat perolehan kredit)
Saldo Kredit	72 kredit (30 kredit peluncuran digunakan; 72 kredit yang diperoleh tetap tidak digunakan)

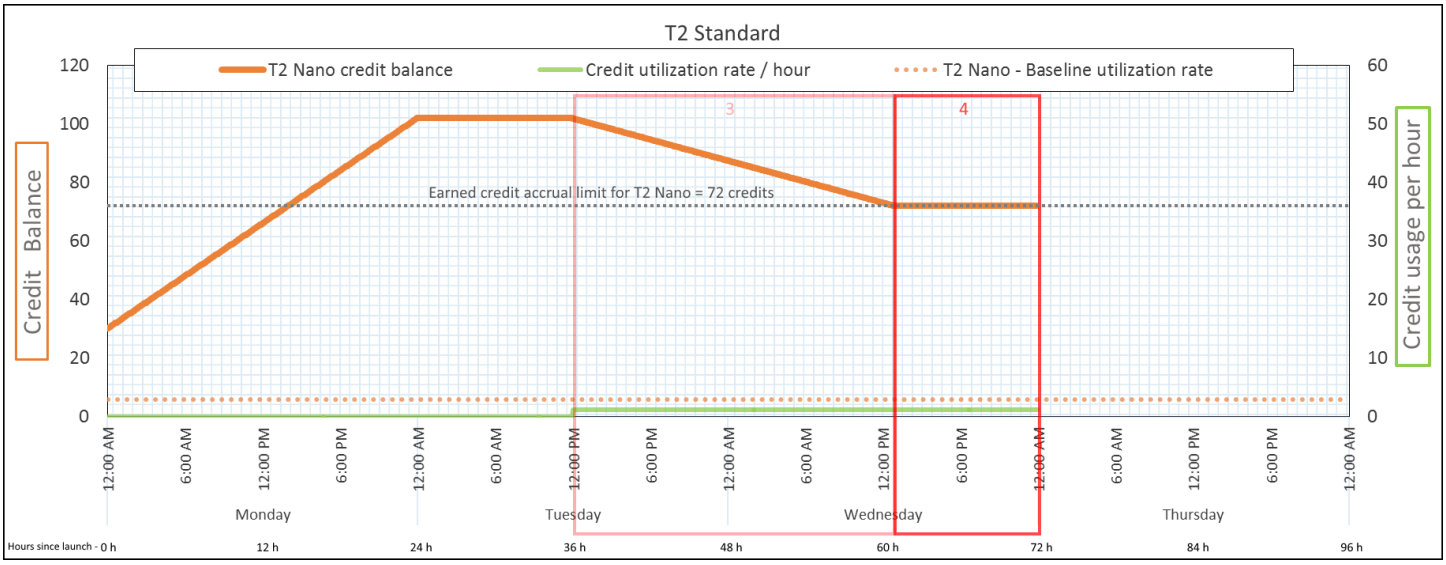
Kesimpulan

Sebuah instans menggunakan kredit peluncuran terlebih dahulu, sebelum menggunakan kredit yang diperoleh. Kredit peluncuran tidak termasuk dalam penghitungan batasan kredit. Setelah kredit peluncuran digunakan, saldonya tidak akan melebihi yang bisa diperoleh dalam 24 jam. Selain itu, saat berjalan, sebuah instans tidak dapat memperoleh lebih banyak kredit peluncuran.

Periode 4: 62 – 72 jam

Selama 11 jam ke depan, instans menggunakan 2% CPU, yang membutuhkan 13,2 kredit. Ini adalah pemanfaatan CPU yang sama seperti pada periode sebelumnya, tetapi saldo tidak berkurang. Saldo tetap berada di 72 kredit.

Saldo tidak berkurang karena tingkat pendapatan kredit lebih tinggi daripada tingkat penggunaan kredit. Saat instans menghabiskan 13,2 kredit, instans ini juga memperoleh 33 kredit. Namun, batas saldonya adalah 72 kredit, jadi setiap kredit yang diperoleh yang melebihi batas tersebut akan dibuang. Saldo mencapai titik datar di 72 kredit, yang berbeda dari puncak 102 kredit selama Periode 2, karena tidak ada kredit peluncuran yang diakumulasi.



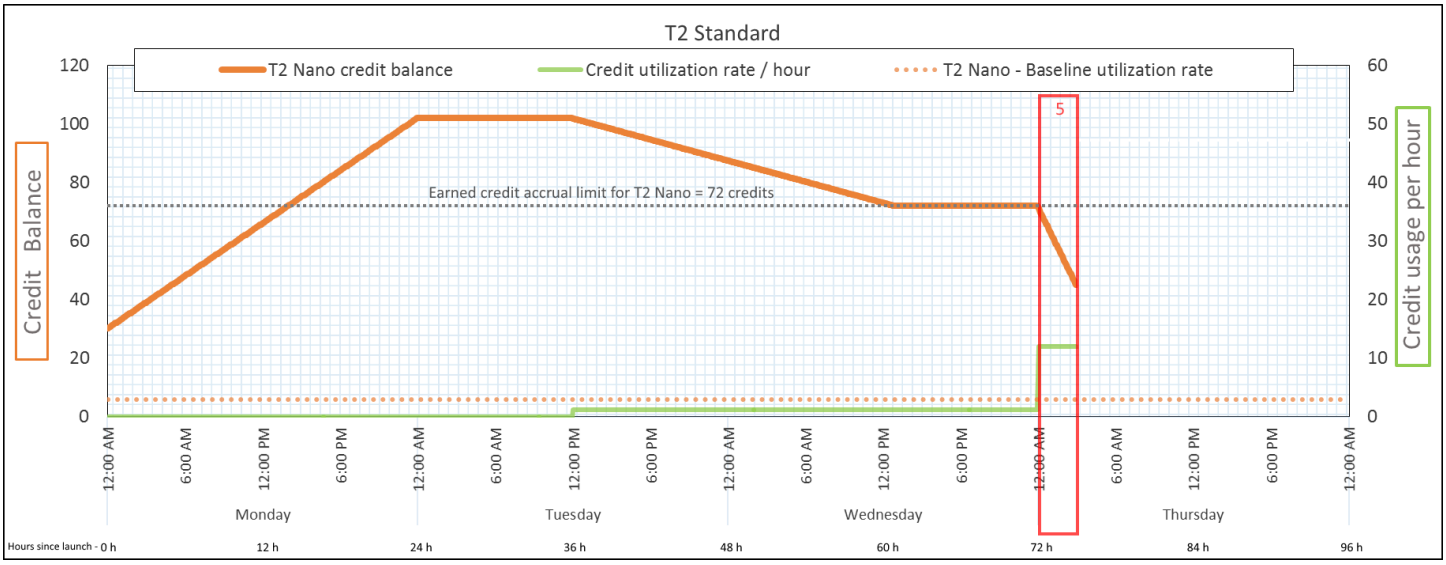
Tingkat Penggunaan Kredit	28,8 kredit per 24 jam (1,2 kredit per jam, 2% pemanfaatan CPU, 40% dari tingkat perolehan kredit) —13,2 kredit selama 11 jam
Tingkat Perolehan Kredit	72 kredit per 24 jam
Tingkat Pembuangan Kredit	43,2 kredit per 24 jam (60% dari tingkat perolehan kredit)
Saldo Kredit	72 kredit (0 kredit peluncuran, 72 kredit yang diperoleh)—saldo berada pada batasnya

Kesimpulan

Setelah kredit peluncuran digunakan, batas saldo kredit ditentukan oleh jumlah kredit yang dapat diperoleh instans dalam 24 jam. Jika instans mendapatkan lebih banyak kredit daripada yang digunakan, kredit yang baru diperoleh yang melebihi batas akan dibuang.

Periode 5: 73 – 75 jam

Selama tiga jam ke depan, instans melonjak pada 20% pemanfaatan CPU, yang membutuhkan 36 kredit. Instans ini memperoleh sembilan kredit dalam tiga jam yang sama, yang menghasilkan penurunan saldo bersih sebesar 27 kredit. Pada akhir tiga jam, saldo kredit adalah 45 kredit yang diperoleh yang diakumulasi.



Tingkat Penggunaan Kredit	288 kredit per 24 jam (12 kredit per jam, 20% pemanfaatan CPU, 400% dari tingkat perolehan kredit) —36 kredit selama 3 jam
Tingkat Perolehan Kredit	72 kredit per 24 jam (9 kredit selama 3 jam)
Tingkat Pembuangan Kredit	0 kredit per 24 jam
Saldo Kredit	45 kredit (saldo sebelumnya (72) - kredit yang digunakan (36) + kredit yang diperoleh (9)) —saldo menurun pada tingkat 216 kredit per 24 jam (tingkat penggunaan 288/24 + tingkat perolehan 72/24 = tingkat penurunan saldo 216/24)

Kesimpulan

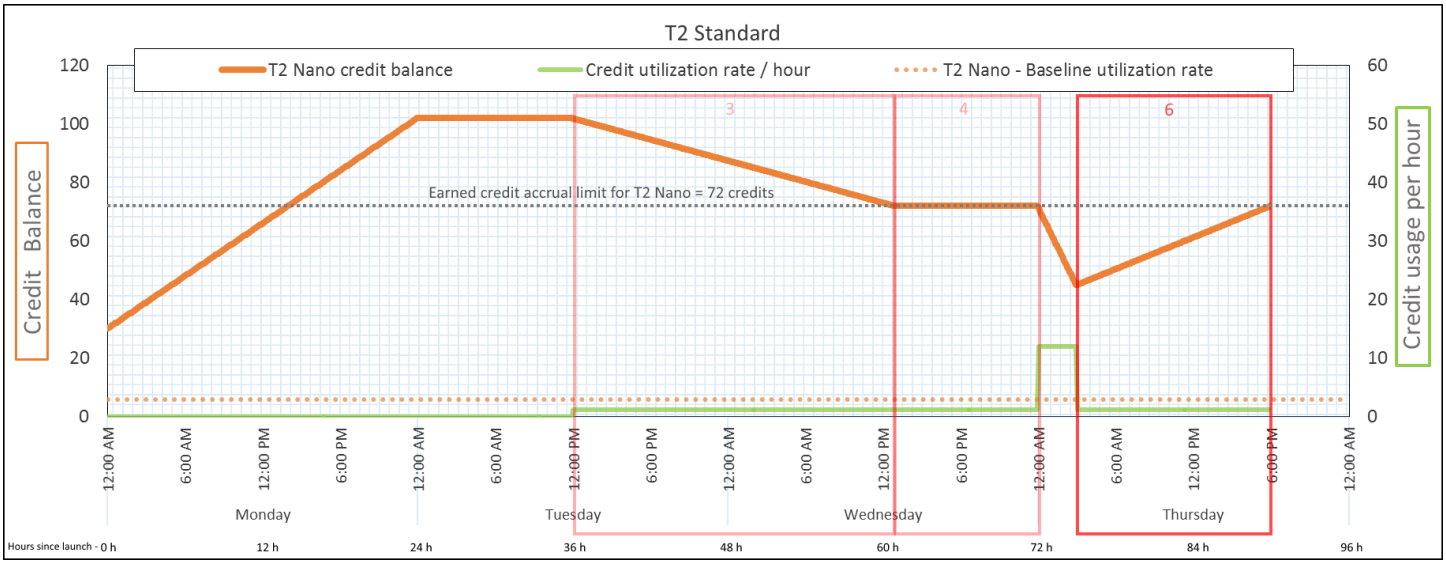
Jika sebuah instans menggunakan kredit lebih banyak daripada yang diperolehnya, saldo kreditnya menurun.

Periode 6: 76 – 90 jam

Selama 15 jam ke depan, instans menggunakan 2% CPU, yang membutuhkan 18 kredit. Ini adalah penggunaan CPU yang sama seperti pada Periode 3 dan 4. Namun, saldo meningkat pada periode ini, sedangkan pada Periode 3 menurun dan pada Periode 4 stabil.

Pada Periode 3, kredit peluncuran akumulasi digunakan, dan setiap kredit yang diperoleh yang melebihi batas kredit dibuang, yang mengakibatkan penurunan saldo kredit. Pada Periode 4, instans menggunakan lebih sedikit kredit daripada yang diperolehnya. Setiap kredit yang diperoleh yang melebihi batas dibuang, sehingga saldo menjadi stabil di maksimum 72 kredit.

Pada periode ini, tidak ada kredit peluncuran akumulasi, dan akumulasi jumlah kredit yang diperoleh dalam saldo di bawah batas. Tidak ada kredit yang diperoleh yang dibuang. Selain itu, instans tersebut mendapatkan lebih banyak kredit daripada yang digunakan, yang mengakibatkan peningkatan dalam saldo kredit.



Tingkat Penggunaan Kredit	28,8 kredit per 24 jam (1,2 kredit per jam, 2% pemanfaatan CPU, 40% dari tingkat perolehan kredit) —18 kredit selama 15 jam
Tingkat Perolehan Kredit	72 kredit per 24 jam (45 kredit selama 15 jam)
Tingkat Pembuangan Kredit	0 kredit per 24 jam
Saldo Kredit	72 kredit (saldo meningkat pada tingkat 43,2 kredit per 24 jam — tingkat perubahan = tingkat penggunaan 28,8/24 + tingkat perolehan 72/24)

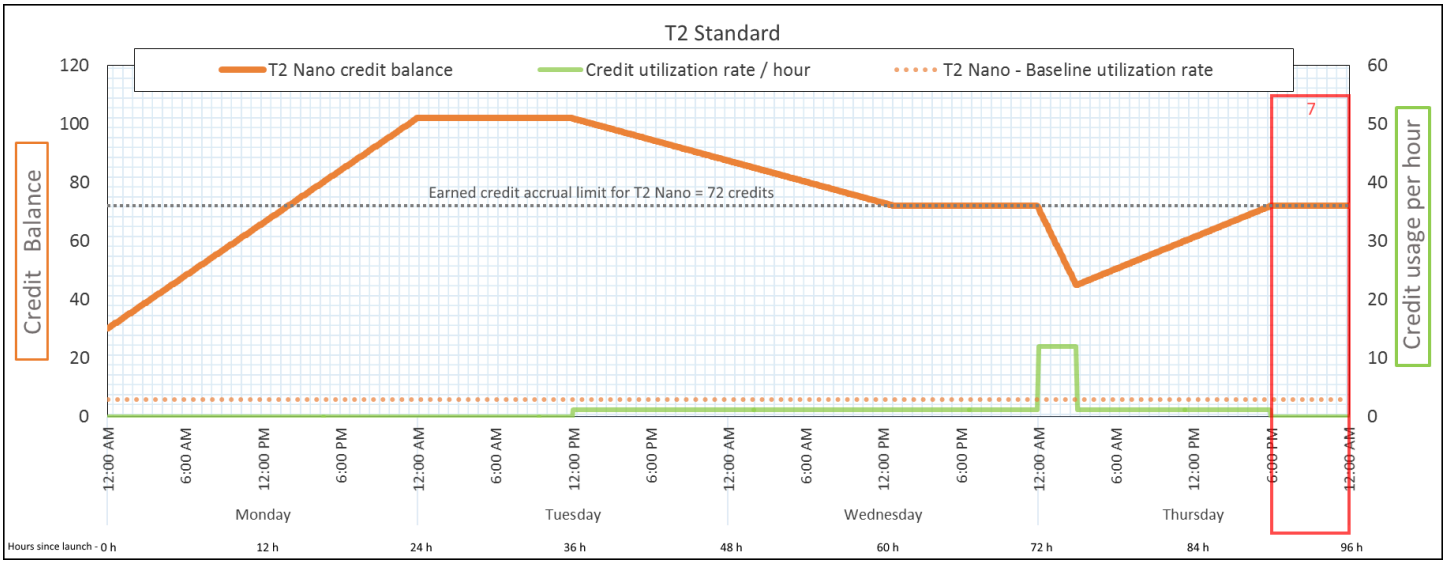
Kesimpulan

Jika sebuah instans menggunakan kredit lebih sedikit daripada yang diperolehnya, saldo kreditnya meningkat.

Periode 7: 91 – 96 jam

Selama enam jam berikutnya, instans tetap idle— pemakaian CPU 0%—dan tidak ada kredit yang digunakan. Ini adalah penggunaan CPU yang sama seperti di Periode 2, tetapi saldonya tidak berhenti di 102 kredit—saldo berhenti di 72 kredit, yang merupakan batas saldo kredit untuk instans.

Pada Periode 2, saldo kredit termasuk akumulasi 30 kredit peluncuran. Kredit peluncuran digunakan di Periode 3. Instans yang berjalan tidak bisa mendapatkan lebih banyak kredit peluncuran. Setelah batas saldo kredit CPU tercapai, kredit apa pun yang diperoleh setelah batas akan dibuang.



Tingkat Penggunaan Kredit	0 kredit per 24 jam (pemanfaatan CPU 0%)
Tingkat Perolehan Kredit	72 kredit per 24 jam
Tingkat Pembuangan Kredit	72 kredit per 24 jam (100% dari tingkat perolehan kredit)
Saldo Kredit	72 kredit (0 kredit peluncuran + 72 kredit perolehan)

Kesimpulan

Sebuah instans terus-menerus memperoleh kredit, tetapi tidak dapat mengakumulasi lebih banyak kredit yang diperoleh jika saldo kredit telah tercapai. Setelah batasan tercapai, kredit yang baru diperoleh akan dibuang. Batas saldo kredit ditentukan oleh jumlah kredit yang dapat diperoleh instans dalam 24 jam. Untuk informasi selengkapnya tentang batas saldo kredit, lihat tabel kredit.

Konfigurasikan instance kinerja burstable

Langkah-langkah untuk meluncurkan, memantau, dan memodifikasi instans kinerja burstable (instans T) serupa. Perbedaan utamanya adalah spesifikasi kredit default saat diluncurkan.

Setiap keluarga instans T dilengkapi dengan spesifikasi kredit default berikut:

- Instans T4G, T3a, dan T3 diluncurkan sebagai `unlimited`
- Instans T3 pada Host Khusus hanya dapat diluncurkan sebagai `standard`
- Instans T2 diluncurkan sebagai `standard`

Anda dapat mengubah spesifikasi kredit default untuk akun tersebut.

Tugas

- Konfigurasikan spesifikasi kredit saat peluncuran
- Konfigurasikan grup Auto Scaling untuk menetapkan spesifikasi kredit sebagai unlimited
- Kelola spesifikasi kredit dari instance kinerja yang dapat meledak
- Mengelola spesifikasi kredit default untuk akun

Konfigurasikan spesifikasi kredit saat peluncuran

Anda dapat meluncurkan instans T Anda dengan spesifikasi kredit `unlimited` atau`standard`.

Prosedur berikut menjelaskan cara menggunakan konsol EC2 atau. AWS CLI Untuk informasi tentang menggunakan grup Auto Scaling, lihat. Konfigurasikan grup Auto Scaling untuk menetapkan spesifikasi kredit sebagai unlimited

Console

Untuk mengonfigurasi spesifikasi kredit dari sebuah instans saat peluncuran

1. Ikuti prosedur untuk meluncurkan instans.
2. Pada Tipe instans, pilih tipe instans T.

3. Perluas Detail lanjutan. Untuk spesifikasi Kredit, pilih spesifikasi kredit.
4. Di panel Ringkasan, tinjau konfigurasi instans Anda, lalu pilih Luncurkan instans.

AWS CLI

Untuk mengatur spesifikasi kredit dari sebuah instans saat peluncuran

Gunakan perintah run-instance dengan opsi. `--credit-specification`

```
--credit-specification CpuCredits=unlimited
```

PowerShell

Untuk mengatur spesifikasi kredit dari sebuah instans saat peluncuran

Gunakan New-EC2Instancecmdlet dengan parameter. `-CreditSpecification_CpuCredit`

```
-CreditSpecification_CpuCredit unlimited
```

Konfigurasikan grup Auto Scaling untuk menetapkan spesifikasi kredit sebagai unlimited

Ketika instans T diluncurkan atau dimulai, mereka memerlukan kredit CPU untuk pengalaman bootstrap yang baik. Jika Anda menggunakan grup Auto Scaling untuk meluncurkan instans, sebaiknya konfigurasikan instans Anda sebagai `unlimited`. Jika Anda melakukannya, instans menggunakan surplus kredit saat diluncurkan atau dimulai ulang secara otomatis oleh grup Auto Scaling. Menggunakan kredit surplus mencegah pembatasan performa.

Membuat templat peluncuran

Anda harus menggunakan templat peluncuran untuk meluncurkan instans sebagai `unlimited` dalam grup Auto Scaling. Konfigurasi peluncuran tidak mendukung peluncuran instans sebagai `unlimited`.

Console

Untuk membuat template peluncuran yang menetapkan spesifikasi kredit

1. Ikuti Buat template peluncuran menggunakan prosedur pengaturan lanjutan di Panduan Pengguna Amazon EC2 Auto Scaling.
2. Dalam Konten templat peluncuran, untuk Tipe instans, pilih ukuran instans.

3. Untuk meluncurkan instans sebagai `unlimited` dalam grup Auto Scaling, pada Detail lanjutan, untuk Spesifikasi kredit, pilih Tak Terbatas.
4. Setelah Anda selesai menentukan parameter templat peluncuran, pilih Buat templat peluncuran.

AWS CLI

Untuk membuat template peluncuran yang menetapkan spesifikasi kredit

Gunakan perintah create-launch-template.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --version-description FirstVersion \
    --launch-template-data CreditSpecification={CpuCredits=unlimited}
```

PowerShell

Untuk membuat template peluncuran yang menetapkan spesifikasi kredit

Gunakan New-EC2LaunchTemplatecmdlet. Tentukan spesifikasi kredit untuk data template peluncuran sebagai berikut.

```
$creditSpec = New-Object Amazon.EC2.Model.CreditSpecificationRequest
$creditSpec.CpuCredits = "unlimited"
$launchTemplateData = New-Object Amazon.EC2.Model.RequestLaunchTemplateData
$launchTemplateData.CreditSpecification = $creditSpec
```

Kaitkan grup Auto Scaling dengan templat peluncuran

Untuk mengaitkan templat peluncuran dengan grup Auto Scaling, buat grup Auto Scaling menggunakan templat peluncuran, atau tambahkan templat peluncuran ke grup Auto Scaling yang sudah ada.

Console

Untuk membuat grup Auto Scaling menggunakan templat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Pada bilah navigasi di bagian atas layar, pilih kawasan yang sama yang Anda gunakan saat Anda membuat templat peluncuran.
3. Di panel navigasi, pilih Grup Auto Scaling, pilih Buat grup Auto Scaling.
4. Pilih Templat Peluncuran, pilih templat peluncuran Anda, lalu pilih Langkah Berikutnya.
5. Lengkapi bidang grup Auto Scaling. Setelah Anda selesai meninjau pengaturan konfigurasi di halaman Pratinjau, pilih Buat grup Auto Scaling. Untuk informasi selengkapnya, lihat Membuat Group Auto Scaling Menggunakan Templat Peluncuran di Panduan Pengguna Amazon EC2 Auto Scaling.

Untuk menambahkan templat peluncuran ke grup Auto Scaling yang ada

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah yang sama dengan yang Anda gunakan saat Anda membuat templat peluncuran.
3. Di panel navigasi, pilih Grup Auto Scaling.
4. Dari daftar grup Auto Scaling, pilih grup Auto Scaling, dan pilih Tindakan, Edit.
5. Pada tab Detail, untuk Templat Peluncuran, pilih templat peluncuran, lalu pilih Simpan.

AWS CLI

Untuk membuat grup Auto Scaling menggunakan templat peluncuran

Gunakan perintah create-auto-scaling-group dan tentukan parameter `--launch-template`.

Untuk menambahkan templat peluncuran ke grup Auto Scaling yang ada

Gunakan perintah update-auto-scaling-group dan tentukan parameter `--launch-template`.

PowerShell

Untuk membuat grup Auto Scaling menggunakan templat peluncuran

Gunakan New- ASAuto ScalingGroup cmdlet dan tentukan parameter `-LaunchTemplate_LaunchTemplateId` or`-LaunchTemplate_LaunchTemplateName`.

Untuk menambahkan templat peluncuran ke grup Auto Scaling yang ada

Gunakan Update- ASAuto ScalingGroup cmdlet dan tentukan parameter `-LaunchTemplate_LaunchTemplateId` atau`-LaunchTemplate_LaunchTemplateName`.

Kelola spesifikasi kredit dari instance kinerja yang dapat meledak

Anda dapat mengganti spesifikasi kredit dari instans T yang sedang berjalan atau berhenti kapan saja antara `unlimited` dan`standard`.

Perhatikan bahwa dalam mode `unlimited`, sebuah instans dapat menghabiskan kredit surplus, yang mungkin menimbulkan biaya tambahan. Untuk informasi selengkapnya, lihat Kredit surplus dapat dikenakan biaya.

Console

Untuk mengelola spesifikasi kredit dari sebuah instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans.
3. (Opsional) Pilih contoh. Pada tab Detailnya, temukan spesifikasi Kredit. Nilainya adalah `unlimited` atau `standard`.
4. (Opsional) Untuk mengubah spesifikasi kredit untuk beberapa instance secara bersamaan, pilih semuanya.
5. Pilih Tindakan, Pengaturan instans, Ubah spesifikasi kredit. Opsi ini diaktifkan hanya jika Anda memilih instance T.
6. Untuk mode Tidak Terbatas, pilih atau kosongkan kotak centang di samping setiap ID instance.

AWS CLI

Untuk mendapatkan spesifikasi kredit dari sebuah instance

Gunakan perintah describe-instance-credit-specifications. Jika Anda tidak menentukan ID instance, semua instance dengan spesifikasi kredit `unlimited` dikembalikan. Output juga akan mencakup contoh yang sebelumnya dikonfigurasi dengan spesifikasi `unlimited` kredit. Misalnya, jika Anda mengubah ukuran instans T3 menjadi instans M4, saat dikonfigurasi sebagai, `unlimited`Amazon EC2 mengembalikan instans M4.

```
aws ec2 describe-instance-credit-specifications \
    --instance-id i-1234567890abcdef0 \
    --query InstanceCreditSpecifications[].CpuCredits \
    --output text
```

Berikut ini adalah output contoh.

```
unlimited
```

Untuk mengatur spesifikasi kredit dari sebuah instans

Gunakan perintah modify-instance-credit-specification.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

PowerShell

Untuk mendapatkan spesifikasi kredit dari sebuah instance

Gunakan Get-EC2CreditSpecificationcmdlet.

```
(Get-EC2CreditSpecification `
    -InstanceId i-1234567890abcdef0).CpuCredits
```

Berikut ini adalah output contoh.

```
unlimited
```

Untuk mengatur spesifikasi kredit dari sebuah instans

Gunakan Edit-EC2InstanceCreditSpecificationcmdlet.

```
Edit-EC2InstanceCreditSpecification `
    -Region us-east-1 `
    -InstanceCreditSpecification @({InstanceId="i-1234567890abcdef0"
 CpuCredits="unlimited"})
```

Mengelola spesifikasi kredit default untuk akun

Setiap keluarga instans T dilengkapi dengan spesifikasi kredit default. Anda dapat mengubah spesifikasi kredit default untuk setiap keluarga instans T di tingkat akun per AWS Wilayah. Nilai yang valid untuk spesifikasi kredit default adalah `unlimited` dan`standard`.

Jika Anda menggunakan wizard peluncuran instans di konsol EC2 untuk meluncurkan instans, nilai yang Anda pilih untuk spesifikasi kredit akan menggantikan spesifikasi kredit default tingkat akun. Jika Anda menggunakan instance AWS CLI to launch, semua instans T baru dalam peluncuran akun menggunakan spesifikasi kredit default. Spesifikasi kredit untuk instans yang sedang berjalan atau dihentikan tidak terpengaruh.

Pertimbangan

Spesifikasi kredit default untuk keluarga instans hanya dapat dimodifikasi sekali dalam periode 5 menit bergulir, dan hingga empat kali dalam periode 24 jam bergulir.

Console

Untuk mengelola spesifikasi kredit default

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Untuk mengubah AWS Region, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Di panel navigasi, pilih Dasbor.
4. Pada kartu Atribut akun, di bawah Pengaturan, pilih Spesifikasi kredit default.
5. Pilih Kelola.
6. Untuk setiap keluarga instans, pilih Tak Terbatas atau Standard, lalu pilih Perbarui.

AWS CLI

Untuk mendapatkan spesifikasi kredit default

Gunakan perintah get-default-credit-specification.

```
aws ec2 get-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --query InstanceFamilyCreditSpecifications[].CpuCredits \
    --output text
```

Berikut ini adalah output contoh.

```
standard
```

Untuk mengatur spesifikasi kredit default

Gunakan perintah modify-default-credit-specification. Contoh berikut menetapkan nilai keunlimited.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

PowerShell

Untuk mendapatkan spesifikasi kredit default

Gunakan Get-EC2DefaultCreditSpecificationcmdlet.

```
(Get-EC2DefaultCreditSpecification `
    -Region us-east-1 `
    -InstanceFamily t2).CpuCredits
```

Berikut ini adalah output contoh.

```
standard
```

Untuk mengatur spesifikasi kredit default

Gunakan Edit-EC2DefaultCreditSpecificationcmdlet. Contoh berikut menetapkan nilai keunlimited.

```
Edit-EC2DefaultCreditSpecification `
    -Region us-east-1 `
    -InstanceFamily t2 `
    -CpuCredit unlimited
```

Pantau kredit CPU untuk instans burstable

EC2 mengirimkan metrik ke Amazon. CloudWatch Anda dapat melihat metrik kredit CPU di metrik Amazon EC2 per instans konsol atau menggunakan AWS CLI metrik untuk mencantumkan metrik untuk setiap instans. CloudWatch Untuk informasi selengkapnya, lihat CloudWatch metrik yang tersedia untuk instans Anda.

Daftar Isi

- CloudWatch Metrik tambahan untuk instans performa burstable
- Menghitung penggunaan kredit CPU

CloudWatch Metrik tambahan untuk instans performa burstable

Instans kinerja burstable memiliki CloudWatch metrik tambahan ini, yang diperbarui setiap lima menit:

- `CPUCreditUsage` – Jumlah kredit CPU yang digunakan selama periode pengukuran.
- `CPUCreditBalance` – Jumlah kredit CPU yang diakumulasi oleh instans. Saldo ini habis saat CPU melonjak dan kredit CPU digunakan lebih cepat daripada yang diperoleh.
- `CPUSurplusCreditBalance` – Jumlah kredit CPU surplus yang digunakan untuk mempertahankan pemanfaatan CPU saat nilai `CPUCreditBalance` adalah nol.
- `CPUSurplusCreditsCharged` – Jumlah kredit CPU surplus yang melebihi jumlah kredit CPU maksimum yang dapat diperoleh dalam periode 24 jam, dan dengan demikian menarik biaya tambahan.

Dua metrik terakhir hanya berlaku untuk instans yang dikonfigurasi sebagai `unlimited`.

Tabel berikut menjelaskan CloudWatch metrik untuk instance kinerja burstable. Untuk informasi selengkapnya, lihat CloudWatch metrik yang tersedia untuk instans Anda.

Metrik	Deskripsi
`CPUCreditUsage`	Jumlah kredit CPU yang digunakan oleh instans untuk pemanfaatan CPU. Satu kredit CPU sama dengan satu vCPU yang berjalan pada pemanfaatan 100% selama satu menit atau kombinasi yang setara dari CPUs v, pemanfaatan, dan waktu (misalnya, satu vCPU berjalan pada pemanfaatan 50% selama dua menit atau dua CPUs v berjalan pada pemanfaatan 25% selama dua menit). Metrik kredit CPU tersedia hanya dalam frekuensi lima menit. Jika Anda menentukan periode lebih dari lima menit, gunakan statistik, Sumbukan statistik.`Average` Unit: Kredit (vCPU-menit)

Metrik	Deskripsi
`CPUCreditBalance`	Jumlah kredit CPU yang diperoleh yang diakumulasi oleh instans sejak diluncurkan atau dimulai. Untuk T2 Standar, `CPUCreditBalance` juga mencakup jumlah kredit peluncuran yang telah diakumulasi. Kredit diakumulasi ke saldo kredit setelah diperoleh, dan dihapus dari saldo kredit saat digunakan. Saldo kredit memiliki batas maksimum, yang ditentukan oleh ukuran instans. Setelah batas tercapai, setiap kredit yang baru diperoleh akan dibuang. Untuk T2 Standar, kredit peluncuran tidak termasuk dalam penghitungan batas. Kredit dalam `CPUCreditBalance` tersedia untuk instans untuk digunakan hingga melonjak melebihi pemanfaatan CPU acuan. Saat sebuah instans berjalan, kredit di `CPUCreditBalance` tidak kedaluarsa. Ketika instans T4G, T3a atau T3 berhenti, `CPUCreditBalance` nilainya bertahan selama tujuh hari. Setelah itu, semua kredit akumulasi akan hilang. Saat instans T2 berhenti, nilai `CPUCreditBalance` tidak bertahan, dan semua kredit akumulasi akan hilang. Metrik kredit CPU tersedia pada frekuensi lima menit saja. Unit: Kredit (vCPU-menit)

Metrik	Deskripsi
`CPUSurplusCreditBalance`	Jumlah kredit surplus yang telah digunakan oleh instans `unlimited` saat nilai `CPUCreditBalance` miliknya adalah nol. Nilai `CPUSurplusCreditBalance` dibayarkan oleh dengan kredit CPU yang diperoleh. Jika jumlah kredit surplus melebihi jumlah kredit maksimum yang dapat diperoleh instans dalam jangka waktu 24 jam, kredit surplus yang digunakan di atas jumlah maksimum akan dikenakan biaya tambahan. Unit: Kredit (vCPU-menit)
`CPUSurplusCreditsCharged`	Jumlah kredit surplus yang digunakan yang tidak dibayarkan oleh kredit CPU yang diperoleh, dikenakan biaya tambahan. Kredit surplus yang digunakan akan dikenai biaya jika salah satu dari hal berikut terjadi: • Kredit surplus yang digunakan melampaui jumlah kredit maksimum yang bisa didapatkan oleh instans dalam periode 24 jam. Kredit surplus yang digunakan di atas jumlah maksimum akan dikenai biaya pada akhir jam. • Instans dihentikan atau diakhiri. • Instans dialihkan dari `unlimited` ke `standard`. Unit: Kredit (vCPU-menit)

Menghitung penggunaan kredit CPU

Penggunaan kredit CPU dari instance dihitung menggunakan CloudWatch metrik instans yang dijelaskan dalam tabel sebelumnya.

Amazon EC2 mengirimkan metrik ke CloudWatch setiap lima menit. Referensi ke nilai sebelumnya dari metrik pada titik waktu mana pun menyiratkan nilai sebelumnya dari metrik, yang dikirimkan lima menit yang lalu.

Menghitung penggunaan kredit CPU untuk instans Standar

- Saldo kredit CPU meningkat jika pemanfaatan CPU di bawah garis dasar, ketika kredit yang digunakan kurang dari kredit yang diakumulasi dalam interval lima menit sebelumnya.
- Saldo kredit CPU berkurang jika pemakaian CPU di atas garis dasar, ketika kredit yang digunakan lebih dari kredit yang diperoleh dalam interval lima menit sebelumnya.

Secara matematis, hal tersebut ditangkap oleh persamaan berikut:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

Ukuran instans menentukan jumlah kredit yang dapat diperoleh instans per jam dan jumlah kredit yang diperoleh yang dapat diakumulasi dalam saldo kredit. Untuk informasi tentang jumlah kredit yang diperoleh per jam, dan batas saldo kredit untuk setiap ukuran instans, lihat tabel kredit.

Contoh

Contoh ini menggunakan instans `t3.nano`. Untuk menghitung nilai `CPUCreditBalance` instans, gunakan persamaan sebelumnya sebagai berikut:

- `CPUCreditBalance` – Saldo kredit saat ini yang akan dihitung.
- `prior CPUCreditBalance` – Saldo kredit lima menit lalu. Dalam contoh ini, instans telah mengakumulasi dua kredit.
- `Credits earned per hour` – Sebuah instans `t3.nano` memperoleh enam kredit per jam.
- `5/60`- Mewakili interval lima menit antara CloudWatch publikasi metrik. Kalikan kredit yang diperoleh per jam dengan 5/60 (lima menit) untuk mendapatkan jumlah kredit yang diperoleh instans dalam lima menit terakhir. Instans `t3.nano` memperoleh 0,5 kredit setiap lima menit.
- `CPUCreditUsage` – Banyaknya kredit yang digunakan instans dalam lima menit terakhir. Dalam contoh ini, instans menggunakan satu kredit dalam lima menit terakhir.

Dengan menggunakan nilai-nilai ini, Anda dapat menghitung nilai `CPUCreditBalance`:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Menghitung penggunaan kredit CPU untuk instans Tidak Terbatas

Ketika instans performa yang dapat melonjak perlu melonjak di atas garis dasar, instans akan menggunakan kredit yang diakumulasi sebelum mengunakan kredit surplus. Saat menggunakan saldo kredit CPU yang diakumulasi, instans dapat menggunakan kredit surplus untuk melonjakkan CPU selama yang dibutuhkannya. Saat pemanfaatan CPU turun di bawah garis dasar, kredit surplus akan dibayarkan sebelum instans mengakumulasi kredit yang diperoleh.

Kami menggunakan istilah `Adjusted balance` dalam persamaan berikut untuk mencerminkan aktivitas yang terjadi dalam interval lima menit ini. Kami menggunakan nilai ini untuk sampai pada nilai untuk `CPUCreditBalance` dan `CPUSurplusCreditBalance` CloudWatch metrik.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

Nilai `0` untuk `Adjusted balance` menunjukkan bahwa instans menggunakan semua kredit yang diperoleh untuk melonjak, dan tidak ada kredit surplus yang digunakan. Hasilnya, baik `CPUCreditBalance` dan `CPUSurplusCreditBalance` diatur ke `0`.

Nilai `Adjusted balance` positif menunjukkan bahwa kredit yang diperoleh yang diakumulasi oleh instans, dan kredit surplus sebelumnya, jika ada, telah dibayarkan. Oleh karena itu, nilai `Adjusted balance` ditetapkan ke `CPUCreditBalance` dan `CPUSurplusCreditBalance` diatur ke `0`. Ukuran instans menentukan jumlah kredit maksimum yang dapat diperoleh.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
CPUSurplusCreditBalance = 0
```

Nilai `Adjusted balance` negatif menunjukkan bahwa instans menggunakan semua kredit yang diperoleh yang diakumulasi dan, selain itu, juga menggunakan kredit surplus untuk melonjak. Oleh karena itu, nilai `Adjusted balance` ditetapkan ke `CPUSurplusCreditBalance` dan `CPUCreditBalance` diatur ke `0`. Sekali lagi, ukuran instans menentukan jumlah kredit maksimum yang dapat diakumulasikan.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
```

```
CPUCreditBalance = 0
```

Jika kredit surplus yang digunakan melebihi kredit maksimum yang dapat diakumulasi oleh instans, saldo kredit surplus diatur ke maksimum, seperti yang ditunjukkan dalam persamaan sebelumnya. Kredit surplus yang tersisa dikenakan tagihan sebagaimana direpresentasikan oleh metrik `CPUSurplusCreditsCharged`.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Akhirnya, saat instans berakhir, semua kredit surplus yang dilacak oleh `CPUSurplusCreditBalance` dikenakan tagihan. Jika instans dialihkan dari `unlimited` ke `standard`, setiap `CPUSurplusCreditBalance` yang tersisa juga dikenakan biaya.

Akselerasi kinerja dengan instans GPU

Instans berbasis GPU menyediakan akses ke NVIDIA GPUs dengan ribuan core komputasi. Anda dapat menggunakan instans ini untuk mengakselerasi aplikasi ilmiah, rekayasa, dan rendering dengan memanfaatkan kerangka kerja komputasi paralel CUDA atau Open Computing Language (OpenCL). Anda juga dapat menggunakannya untuk aplikasi grafik, termasuk streaming game, streaming aplikasi 3-D, dan beban kerja grafis lainnya.

Sebelum Anda dapat mengaktifkan atau mengoptimalkan instance berbasis GPU, Anda harus menginstal driver yang sesuai, sebagai berikut:

- Untuk menginstal driver NVIDIA pada instance dengan GPU NVIDIA yang terpasang, seperti instance P3 atau G4dn, lihat. Driver NVIDIA
- Untuk menginstal driver AMD pada instance dengan GPU AMD yang terpasang, seperti instance G4ad, lihat. Driver AMD

Daftar Isi

- Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon
- Optimalkan pengaturan GPU di instans Amazon EC2
- Mengatur tampilan 4K Ganda pada instans Linux G4ad
- Memulai instans yang dipercepat GPU

Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon

Untuk mengaktifkan GRID Virtual Applications pada instance berbasis GPU yang memiliki NVIDIA GPUs (NVIDIA GRID Virtual Workstation diaktifkan secara default), Anda harus menentukan jenis produk untuk driver. Proses yang Anda gunakan tergantung pada sistem operasi instans Anda.

Instans Linux

Untuk mengaktifkan GRID Virtual Applications pada instans Linux Anda

1. Buat file `/etc/nvidia/gridd.conf` dari file templat yang disediakan.

   ```
   [ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
   ```

2. Buka file `/etc/nvidia/gridd.conf` dalam editor teks favorit Anda.
3. Temukan baris `FeatureType`, dan atur ke `0`. Kemudian, tambahkan baris dengan `IgnoreSP=TRUE`.

   ```
   FeatureType=0 IgnoreSP=TRUE
   ```

4. Simpan file dan keluar.
5. Mulai ulang instans untuk mengambil konfigurasi baru.

   ```
   [ec2-user ~]$ sudo reboot
   ```

Instans Windows

Untuk mengaktifkan GRID Virtual Applications pada instans Windows Anda

1. Jalankan regedit.exe untuk membuka editor registri.
2. Navigasi ke `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global \GridLicensing`.
3. Buka menu konteks (klik kanan) di panel kanan dan pilih Baru, WORD.
4. Untuk Nama , masukkanFeatureType dan ketik`Enter` .
5. Buka menu konteks (klik kanan) diFeatureType dan pilih Modifikasi .
6. Pada Data nilai, masukkan `0` untuk Aplikasi Virtual NVIDIA GRID dan pilih OK.
7. Buka menu konteks (klik kanan) di panel kanan dan pilih Baru, WORD.

8. Untuk Nama, masukkan IgnoreSP dan ketik `Enter`.
9. Buka menu konteks (klik kanan) pada IgnoreSP dan pilih Modifikasi.
10. Untuk Nilai data, ketik 1 dan pilih OK.
11. Tutup editor registri.

Optimalkan pengaturan GPU di instans Amazon EC2

Ada beberapa pengoptimalan pengaturan GPU yang dapat Anda lakukan untuk mencapai performa terbaik pada instans GPU NVIDIA. Dengan beberapa tipe instans ini, driver NVIDIA menggunakan fitur lonjak otomatis, yang memvariasikan kecepatan clock GPU. Dengan menonaktifkan autoboost dan menyetel kecepatan clock GPU ke frekuensi maksimumnya, Anda dapat secara konsisten mencapai kinerja maksimum dengan instans GPU Anda.

Optimalkan pengaturan GPU di Linux

1. Konfigurasikan pengaturan GPU agar menjadi persisten. Perintah ini memerlukan waktu beberapa menit untuk dijalankan.

   ```
   [ec2-user ~]$ sudo nvidia-persistenced
   ```

2. [Hanya instance G3, dan P2] Nonaktifkan fitur autoboost untuk semua GPUs yang ada di instance.

   ```
   [ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
   ```

3. Atur semua kecepatan clock GPU ke frekuensi maksimumnya. Gunakan kecepatan clock memori dan grafis yang ditentukan dalam perintah berikut.

   Beberapa versi driver NVIDIA tidak mendukung pengaturan kecepatan clock aplikasi, dan menampilkan kesalahan `"Setting applications clocks is not supported for GPU..."`, yang bisa Anda abaikan.

   - Instans G3:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
     ```

   - Instans G4dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- Instans G5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
```

- Instans G6, G6f, Gr6, dan Gr6f:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
```

- Contoh G6e:

```
[ec2-user ~]$ sudo nvidia-smi -ac 9001,2520
```

- Contoh G7e:

```
[ec2-user ~]$ sudo nvidia-smi -ac 12481,2430
```

- Instans P2:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- Instans P3 dan P3dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- Instans P4d:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- Instans P4de:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Instans P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

- Instans P5e dan P5en:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3201,1980
```

- Contoh P6-B200:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3996,1965
```

- Contoh P6-B300:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3996,2032
```

Optimalkan pengaturan GPU di Windows

1. Buka PowerShell jendela dan arahkan ke folder instalasi NVIDIA.

```
PS C:\> cd "C:\Windows\System32\DriverStore\FileRepository\nvgridsw_aws.inf_*\"
```

2. [Hanya instance G3, dan P2] Nonaktifkan fitur autoboost untuk semua GPUs yang ada di instance.

```
PS C:\> .\nvidia-smi --auto-boost-default=0
```

3. Atur semua kecepatan clock GPU ke frekuensi maksimumnya. Gunakan kecepatan clock memori dan grafis yang ditentukan dalam perintah berikut.

   Beberapa versi driver NVIDIA tidak mendukung pengaturan kecepatan clock aplikasi, dan menampilkan kesalahan `"Setting applications clocks is not supported for GPU..."`, yang bisa Anda abaikan.

   - Instans G3:

```
PS C:\> .\nvidia-smi -ac "2505,1177"
```

   - Instans G4dn:

```
PS C:\> .\nvidia-smi -ac "5001,1590"
```

   - Instans G5:

```
PS C:\> .\nvidia-smi -ac "6250,1710"
```

- Instans G6, G6f, Gr6, dan Gr6f:

```
PS C:\> .\nvidia-smi -ac "6251,2040"
```

- Contoh G6e:

```
PS C:\> .\nvidia-smi -ac "9001,2520"
```

- Instans P2:

```
PS C:\> .\nvidia-smi -ac "2505,875"
```

- Instans P3 dan P3dn:

```
PS C:\> .\nvidia-smi -ac "877,1530"
```

Mengatur tampilan 4K Ganda pada instans Linux G4ad

Setelah meluncurkan instans G4ad, Anda dapat mengatur tampilan 4K ganda.

Untuk menginstal driver AMD dan mengkonfigurasi layar ganda

1. Hubungkan ke instans Linux Anda untuk mendapatkan alamat Bus PCI dari GPU yang ingin Anda targetkan untuk dual 4K (2x4k):

   ```
   lspci -vv | grep -i amd
   ```

   Output Anda serupa dengan berikut ini:

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
   ```

2. Harap perhatikan, alamat bus PCI adalah 00:1e.0 pada output di atas. Buat file bernama `/etc/modprobe.d/amdgpu.conf` dan tambahkan:

```
options amdgpu virtual_display=0000:00:1e.0,2
```

3. Untuk menginstal driver AMD di Linux, lihatDriver AMD untuk instans EC2 Anda. Jika Anda sudah menginstal driver GPU AMD, Anda perlu membangun kembali modul kernel amdgpu melalui dkms.
4. Gunakan file xorg.conf di bawah ini untuk menentukan topologi layar ganda (2x4K) dan simpan file di `/etc/X11/xorg.conf`:

```
~$ cat /etc/X11/xorg.conf
Section "ServerLayout"
    Identifier     "Layout0"
    Screen          0 "Screen0"
    Screen        1 "Screen1"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection

Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
```

```
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection

Section "Screen"
```

```
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

5. Siapkan DCV dengan mengikuti petunjuk dalam menyiapkan desktop interaktif.
6. Setelah pengaturan DCV selesai, lakukan reboot.
7. Pastikan driver berfungsi:

   ```
   dmesg | grep amdgpu
   ```

   Responsnya akan terlihat seperti berikut:

   ```
   Initialized amdgpu
   ```

8. Anda akan melihat di output untuk `DISPLAY=:0 xrandr -q` bahwa Anda memiliki 2 tampilan virtual yang terhubung:

   ```
   ~$ DISPLAY=:0 xrandr -q
   Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
   Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
    0mm x 0mm
    4096x3112  60.00
    3656x2664  59.99
    4096x2160  60.00
    3840x2160  60.00
    1920x1200  59.95
    1920x1080  60.00
    1600x1200  59.95
    1680x1050  60.00
    1400x1050  60.00
    1280x1024  59.95
    1440x900 59.99
    1280x960 59.99
    1280x854 59.95
    1280x800 59.96
   ```

```
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
 640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
640x480  59.94 59.94
```

9. Saat Anda terhubung ke DCV, ubah resolusi menjadi 2x4K, yang mengonfirmasi bahwa dukungan monitor ganda terdaftar oleh DCV.

Siapkan desktop interaktif untuk Linux

Setelah Anda mengonfirmasi bahwa instans Linux Anda telah menginstal driver GPU AMD dan amdgpu sedang digunakan, Anda dapat menginstal manajer desktop interaktif. Kami merekomendasikan lingkungan desktop MATE untuk kompatibilitas dan performa terbaik.

Prasyarat

Buka editor teks dan simpan yang berikut ini sebagai file bernama `xorg.conf`. Anda akan memerlukan file ini pada instans Anda.

```
Section "ServerLayout"
Identifier     "Layout0"
Screen          0 "Screen0"
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
```

```
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
Section "Screen"
Identifier     "Screen0"
Device         "Device0"
Monitor        "Monitor0"
DefaultDepth   24
Option         "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual    3840 2160
    Depth      32
EndSubSection
EndSection
```

Untuk menyiapkan desktop interaktif di Amazon Linux 2

1. Instal repositori EPEL.

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install epel -y
   ```

2. Instal desktop MATE.

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install mate-desktop1.x -y
   [ec2-user ~]$ sudo yum groupinstall "MATE Desktop" -y
   [ec2-user ~]$ sudo systemctl disable firewalld
   ```

3. Salin file `xorg.conf` ke `/etc/X11/xorg.conf`.
4. Boot ulang instans.

   ```
   [ec2-user ~]$ sudo reboot
   ```

5. (Opsional) Instal server Amazon DCV untuk menggunakan Amazon DCV sebagai protokol tampilan berkinerja tinggi, lalu sambungkan ke sesi Amazon DCV menggunakan klien pilihan Anda.

Untuk menyiapkan desktop interaktif di Ubuntu

1. Instal desktop MATE.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y
$ sudo apt purge ifupdown -y
```

2. Salin file `xorg.conf` ke `/etc/X11/xorg.conf`.
3. Boot ulang instans.

```
$ sudo reboot
```

4. Instal enkoder AMF untuk versi Ubuntu yang sesuai.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Opsional) Instal server Amazon DCV untuk menggunakan Amazon DCV sebagai protokol tampilan berkinerja tinggi, lalu sambungkan ke sesi Amazon DCV menggunakan klien pilihan Anda.
6. Setelah penginstalan DCV memberikan izin video Pengguna DCV:

```
$ sudo usermod -aG video dcv
```

Untuk menyiapkan desktop interaktif di CentOS

1. Instal repositori EPEL.

```
$ sudo yum update -y
$ sudo yum install epel-release -y
```

2. Instal desktop MATE.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ sudo systemctl disable firewalld
```

3. Salin file `xorg.conf` ke `/etc/X11/xorg.conf`.
4. Boot ulang instans.

```
$ sudo reboot
```

5. (Opsional) Instal server Amazon DCV untuk menggunakan Amazon DCV sebagai protokol tampilan berkinerja tinggi, lalu sambungkan ke sesi Amazon DCV menggunakan klien pilihan Anda.

Memulai instans yang dipercepat GPU

Generasi terbaru dari jenis instans akselerasi GPU, seperti yang ditunjukkan dalam daftar berikut memberikan kemampuan kinerja tertinggi untuk pembelajaran mendalam dan aplikasi komputasi kinerja tinggi (HPC). Pilih tautan jenis instans untuk mempelajari lebih lanjut tentang kemampuannya.

- Keluarga P6
- Keluarga P6
- Keluarga P5

Untuk daftar lengkap spesifikasi tipe instans untuk tipe instans yang dipercepat, lihat Komputasi yang dipercepat dalam referensi Jenis EC2 Instance Amazon.

Konfigurasi perangkat lunak

Cara termudah untuk memulai dengan jenis instans akselerasi GPU generasi terbaru adalah dengan meluncurkan instance dari AMI Pembelajaran AWS Mendalam yang telah dikonfigurasi sebelumnya dengan semua perangkat lunak yang diperlukan. Untuk informasi terbaru AWS Deep Learning AMIs untuk digunakan dengan jenis instans akselerasi GPU, lihat DLAMI yang Didukung P6 di Panduan Pengembang.AWS Deep Learning AMIs

Jika Anda perlu membuat AMI khusus untuk meluncurkan instance yang menghosting pembelajaran mendalam atau aplikasi HPC, kami sarankan Anda menginstal versi perangkat lunak minimum berikut di atas gambar dasar Anda.

Tipe instans	Pengemudi NVIDIA	CUDA	NVIDIA GDRCopy	Pemasang EFA	NCCL	EFA K8s [1]
G7e	575	12.9	2.5	1.45.0	2.28.3	0.5.10
P5	530	12.1	2.3	1.24.1	2.18.3	0.4.4
P5.4xbesar	530	12.1	2.3	1.43,1 [2]	2.18.3	0.4.4

Tipe instans	Pengemudi NVIDIA	CUDA	NVIDIA GDRCopy	Pemasang EFA	NCCL	EFA K8s [1]
P5e	550	12.1	2.3	1.24.1	2.18.3	0.5.5
P5en	550	12.1	2.3	1.24.1	2.18.3	0.5.6
P6-B200	570	12.8	2.5	1.41.0	2.26.2-1	0.5.10
P6e- 00 GB2	570	12.8	2.5	1.41.0	2.26.2-1	0.5.10
P6-B300	580	13,0	2.5	1.44.0	2.28.3	0.5.10

[1] Kolom EFA K8s berisi versi minimum yang direkomendasikan untuk. `aws-efa-k8s-device-plugin`

[2] Ada masalah kompatibilitas yang mempengaruhi `P5.4xlarge` contoh ketika GPU-to-GPU komunikasi menggunakan Elastic Fabric Adapter (EFA) dan NVIDIA Collective Communications Library (NCCL). Untuk mengurangi masalah, atur variabel lingkungan `FI_HMEM_DISABLE_P2P` ke`1`, dan pastikan Anda menginstal EFA versi 1.43.1 atau yang lebih baru.

> **Note**
>
> Jika Anda menggunakan versi 1.41.0 dari installer EFA, disertakan dengan itu. `aws-ofi-nccl plugin` Untuk versi installer EFA sebelumnya, gunakan `aws-ofi-nccl plugin` versi `1.7.2-aws` atau yang lebih baru.

Kami juga menyarankan agar Anda mengonfigurasi instans agar tidak menggunakan status C yang lebih dalam. Untuk informasi selengkapnya, lihat Kinerja tinggi dan latensi rendah dengan membatasi status C yang lebih dalam di Panduan Pengguna Amazon Linux 2. GPU AWS Deep Learning Base terbaru telah AMIs dikonfigurasi sebelumnya untuk tidak menggunakan C-state yang lebih dalam.

Untuk konfigurasi jaringan dan Elastic Fabric Adapter (EFA) lihat. Maksimalkan bandwidth jaringan pada instans Amazon EC2 dengan beberapa kartu jaringan

Instans Mac Amazon EC2

Instans Mac EC2 ideal untuk mengembangkan, membangun, menguji, dan menandatangani aplikasi untuk platform Apple, seperti iPhone, iPad, Mac, Vision Pro, Apple Watch, Apple TV, dan Safari. Anda dapat terhubung ke instans Mac Anda menggunakan SSH atau Apple Remote Desktop (ARD).

> **Note**
>
> Unit penagihan adalah host khusus. Instans yang berjalan pada host itu tidak dikenai biaya tambahan.

Instans Amazon EC2 Mac secara native mendukung sistem operasi macOS.

- Instans EC2 x86 Mac (`mac1.metal`) dibangun di atas perangkat keras mini Mac 2018 yang ditenagai oleh prosesor Core i7 generasi kedelapan GHz Intel 3,2 (Coffé Lake), 6 inti fisik dan 12 logis, dan memori 32 GiB.
- Instans EC2 M1 Mac (`mac2.metal`) dibangun di atas perangkat keras mini Mac 2020 yang ditenagai oleh prosesor silikon Apple M1, 8 inti CPU, 8 inti GPU, memori 16 GiB, dan Apple Neural Engine 16-core.
- Instans EC2 M1 Ultra Mac (`mac2-m1ultra.metal`) dibangun pada perangkat keras Mac Studio 2022 yang ditenagai oleh prosesor silikon Apple M1 Ultra, 20 inti CPU, 64 inti GPU, memori 128 GiB, dan Apple Neural Engine 32-inti.
- Instans EC2 M2 Mac (`mac2-m2.metal`) dibangun di atas perangkat keras mini Mac 2023 yang ditenagai oleh prosesor silikon Apple M2, 8 inti CPU, 10 inti GPU, memori 24 GiB, dan Apple Neural Engine 16-core.
- Instans EC2 M2 Pro Mac (`mac2-m2pro.metal`) dibangun di atas perangkat keras mini Mac 2023 yang ditenagai oleh prosesor silikon Apple M2 Pro, 12 inti CPU, 19 inti GPU, memori 32 GiB, dan Apple Neural Engine 16-core.
- Instans EC2 M4 Mac (`mac-m4.metal`) dibangun di atas perangkat keras mini Mac 2024 yang ditenagai oleh prosesor silikon Apple M4, 10 inti CPU, 10 inti GPU, memori 24 GiB, dan Apple Neural Engine 16-core.
- Instans EC2 M4 Pro Mac (`mac-m4pro.metal`) dibangun di atas perangkat keras mini Mac 2024 yang ditenagai oleh prosesor silikon Apple M4 Pro, 14 inti CPU, 20 inti GPU, memori 48 GiB, dan Apple Neural Engine 16-core.

Host Khusus Amazon EC2 Mac mendukung pemulihan otomatis Host Khusus dan pemeliharaan host berbasis reboot.

Daftar Isi

- Pertimbangan-pertimbangan
- Kesiapan instans
- macOS EC2 AMIs
- EC2 macOS Init
- Monitor Sistem Amazon EC2 untuk macOS
- Sumber daya terkait
- Luncurkan instance Mac menggunakan Konsol Manajemen AWS atau AWS CLI
- Connect ke instans Mac Anda menggunakan SSH atau GUI
- Perbarui sistem operasi dan perangkat lunak pada instans Amazon EC2 Mac
- Meningkatkan ukuran volume EBS di instans Mac Anda
- Menghentikan atau menghentikan instans Amazon EC2 Mac Anda
- Konfigurasikan Perlindungan Integritas Sistem untuk instans Amazon EC2 Mac
- Temukan versi macOS yang didukung untuk Host Khusus Amazon EC2 Mac
- Berlangganan notifikasi AMI macOS
- Ambil macOS IDs AWS Systems Manager AMI menggunakan Parameter Store API
- Catatan rilis macOS Amazon EC2 AMIs

Pertimbangan-pertimbangan

Pertimbangan berikut berlaku untuk instans Mac:

- Instans Mac hanya tersedia sebagai instans bare metal di Host Khusus, dengan masa alokasi minimal 24 jam sebelum Anda dapat membagikan Host Khusus. Anda dapat meluncurkan satu instans Mac per Host Khusus. Anda dapat berbagi Host Khusus dengan AWS akun atau unit organisasi dalam AWS organisasi Anda, atau seluruh AWS organisasi.
- Instans Mac tersedia dalam berbagai jenis Wilayah AWS. Untuk daftar ketersediaan instans Mac di masing-masing instans Wilayah AWS, lihat jenis instans Amazon EC2 menurut Wilayah.
- Instans Mac hanya tersedia sebagai Instans Sesuai Permintaan. Instans tersebut tidak tersedia sebagai Instans Spot atau Instans Terpesan. Anda dapat menghemat uang pada instans Mac dengan membeli Savings Plans.

- Kompatibilitas berbagai jenis instans Mac dengan MacOS Amazon Machine Images (AMIs) tertentu bervariasi. Untuk informasi selengkapnya, lihat Catatan rilis macOS Amazon EC2 AMIs.
- EBShotplug didukung.
- AWS tidak mengelola atau mendukung SSD internal pada perangkat keras Apple. Kami sangat menyarankan Anda menggunakan volume Amazon EBS sebagai gantinya. EBSvolume memberikan manfaat elastisitas, ketersediaan, dan daya tahan yang sama pada instans Mac seperti halnya pada instans EC2 lainnya.
- Sebaiknya gunakan volume Amazon EBS dengan 10.000 IOPS dan 400 MiB/s throughput dengan instans Mac untuk kinerja optimal. Untuk informasi selengkapnya, lihat Jenis volume Amazon EBS di Panduan Pengguna Amazon EBS.
- Instans Mac mendukung Amazon EC2 Auto Scaling.
- Pada instans x86 Mac, pembaruan perangkat lunak otomatis dinonaktifkan. Kami merekomendasikan Anda untuk menerapkan pembaruan dan mengujinya pada instans Anda sebelum memasukkan instans ke dalam proses produksi. Untuk informasi selengkapnya, lihat Perbarui sistem operasi dan perangkat lunak pada instans Amazon EC2 Mac.
- Ketika Anda menghentikan atau mengakhiri instans Mac, alur kerja scrubbing dilakukan pada Host Khusus. Untuk informasi selengkapnya, lihat Menghentikan atau menghentikan instans Amazon EC2 Mac Anda.
- **Important**

  Fitur Apple Intelligence tidak tersedia saat mem-boot perangkat keras Mac dari volume eksternal. Saat instans EC2 Mac boot dari volume EBS eksternal secara default, mereka tidak mendukung fitur Apple Intelligence.
- **Warning**

  Jangan gunakan FileVault. Jika Anda mengaktifkan FileVault, host gagal untuk boot karena partisi terkunci. Jika enkripsi data diperlukan, gunakan enkripsi Amazon EBS untuk menghindari masalah boot dan dampak kinerja. Dengan enkripsi Amazon EBS, operasi enkripsi terjadi di server host, memastikan keamanan keduanya data-at-rest dan data-in-transit antara instans dan penyimpanan EBS terlampir. Untuk informasi selengkapnya, lihat enkripsi Amazon EBS di Panduan Pengguna Amazon EBS.

Kesiapan instans

Setelah meluncurkan instans Mac, Anda harus menunggu hingga instans siap sebelum dapat terhubungkan ke instans tersebut. Untuk AWS AMI yang dijual dengan instans Mac x86 atau instans Apple silicon Mac, waktu peluncuran dapat berkisar dari sekitar 6 menit hingga 20 menit. Bergantung pada ukuran volume Amazon EBS yang dipilih, penyertaan skrip tambahan ke data pengguna, atau perangkat lunak tambahan yang dimuat pada macOS AMI kustom, waktu peluncuran mungkin meningkat.

Anda dapat menggunakan skrip shell kecil, seperti yang di bawah ini, untuk melakukan polling describe-instance-status API untuk mengetahui kapan instance siap untuk dihubungkan. Dalam perintah berikut, ganti ID instans contoh dengan milik Anda.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-1234567890abcdef0 \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

macOS EC2 AMIs

Amazon EC2 macOS dirancang untuk menyediakan lingkungan yang stabil, aman, dan mempunyai performa tinggi untuk beban kerja developer yang berjalan pada instans Mac Amazon EC2. EC2 AMIs macOS mencakup paket yang memungkinkan integrasi AWS yang mudah, seperti alat konfigurasi peluncuran dan pustaka serta alat AWS populer.

Untuk informasi selengkapnya tentang EC2 macOS AMIs, lihat. Catatan rilis macOS Amazon EC2 AMIs

AWS menyediakan EC2 macOS AMIs yang diperbarui secara teratur yang mencakup pembaruan paket yang dimiliki oleh AWS dan versi macOS terbaru yang telah diuji sepenuhnya. Selain itu, AWS menyediakan pembaruan AMIs dengan pembaruan versi minor terbaru atau pembaruan versi utama segera setelah mereka dapat sepenuhnya diuji dan diperiksa. Jika Anda tidak perlu menyimpan data atau melakukan penyesuaian pada instans Mac, Anda bisa mendapatkan pembaruan terkini dengan meluncurkan instans baru menggunakan AMI saat ini dan kemudian mengakhiri instans sebelumnya. Atau, Anda dapat memilih pembaruan mana yang akan diterapkan pada instans Mac Anda.

Untuk informasi tentang cara berlangganan notifikasi macOS AMI, lihat. Berlangganan notifikasi AMI macOS

EC2 macOS Init

EC2macOS Init digunakan untuk menginisialisasi instance EC2 Mac saat diluncurkan. Init ini menggunakan grup prioritas untuk menjalankan grup logis tugas pada saat bersamaan.

File plist yang diluncurkan adalah `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. File untuk Init macOS EC2 terletak di `/usr/local/aws/ec2-macos-init`.

Untuk informasi lebih lanjut, lihat https://github.com/aws/ec2-macos-init.

Monitor Sistem Amazon EC2 untuk macOS

Monitor Sistem Amazon EC2 untuk macOS menyediakan metrik pemanfaatan CPU ke Amazon. CloudWatch Ini mengirimkan metrik ini ke CloudWatch lebih dari perangkat serial khusus dalam periode 1 menit. Anda dapat mengaktifkan atau menonaktifkan agen ini sebagai berikut. Agen tidak diaktifkan secara default.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> Monitor Sistem Amazon EC2 untuk macOS saat ini tidak didukung pada instans Apple silikon Mac.

Sumber daya terkait

Untuk informasi tentang harga, lihat Harga.

Untuk informasi selengkapnya tentang instans Mac, lihat Instans Mac Amazon EC2.

Untuk informasi selengkapnya tentang spesifikasi perangkat keras dan performa jaringan instans Mac, lihat Instans tujuan umum.

Luncurkan instance Mac menggunakan Konsol Manajemen AWS atau AWS CLI

Instans EC2 Mac memerlukan Host Khusus. Pertama-tama, Anda harus mengalokasikan host ke akun Anda, kemudian meluncurkan instans ke host.

Anda dapat meluncurkan instance Mac menggunakan Konsol Manajemen AWS atau file AWS CLI.

Luncurkan instans Mac menggunakan konsol

Untuk meluncurkan instans Mac ke Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Alokasikan Dedicated Host, sebagai berikut:
   a. Di panel navigasi, pilih Host Khusus.
   b. Pilih Alokasikan Host Khusus, lalu lakukan hal berikut:
      i. Untuk keluarga Instance, pilih keluarga Instance Mac. Jika keluarga instans tidak muncul dalam daftar, berarti tidak didukung di Wilayah yang saat ini dipilih.
      ii. Untuk tipe Instance, pilih jenis instance berdasarkan keluarga instance yang dipilih.
      iii. Untuk Zona Ketersediaan, pilih Zona Ketersediaan untuk Host Khusus.
      iv. Untuk Jumlah, biarkan di 1.
      v. Pilih Alokasikan.
3. Luncurkan instans pada host, sebagai berikut:
   a. Pilih Host Khusus yang Anda buat, lalu lakukan hal berikut:
      i. Pilih Tindakan, Luncurkan instans ke host.
      ii. Pada Aplikasi dan Gambar OS (Amazon Machine Image), pilih AMI macOS.
      iii. Di bawah Jenis instans, pilih jenis instans Mac.
      iv. Pada Detail lanjutan, pastikan bahwa Penghunian, Host penghunian oleh, dan ID host penghunian telah dikonfigurasi sebelumnya berdasarkan Host Khusus yang Anda buat. Perbarui Afinitas penghunian sesuai kebutuhan.
      v. Selesaikan wizard, tentukan volume EBS, grup keamanan, dan pasangan kunci yang diperlukan.
      vi. Di panel Ringkasan, pilih Luncurkan instans.
   b. Halaman konfirmasi memberi tahu Anda bahwa instans Anda akan diluncurkan. Pilih Lihat semua instans untuk menutup halaman konfirmasi dan kembali ke konsol. Status awal dari sebuah instans adalah `pending`. Instans siap ketika statusnya berubah menjadi `running` dan lolos pemeriksaan status.

Luncurkan instance Mac menggunakan AWS CLI

Mengalokasikan Host Khusus

Gunakan perintah allocate-hosts berikut untuk mengalokasikan Host Khusus untuk instance Mac Anda, ganti `instance-type` dengan jenis instance mac yang valid, dan `region` dan `availability-zone` dengan yang sesuai untuk lingkungan Anda.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

Luncurkan instans di host

Gunakan perintah run-instance berikut untuk meluncurkan instance Mac, sekali lagi mengganti `instance-type` dengan jenis instance mac yang valid, dan `region` dan `availability-zone` dengan yang digunakan sebelumnya.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

Status awal dari sebuah instans adalah `pending`. Instans siap ketika statusnya berubah menjadi `running` dan lolos pemeriksaan status. Gunakan describe-instance-statusperintah berikut untuk menampilkan informasi status untuk instance Anda.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Berikut ini adalah contoh output untuk sebuah instans yang sedang berjalan dan telah lulus pemeriksaan status.

```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
```

```
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            }
        }
    ]
}
```

Connect ke instans Mac Anda menggunakan SSH atau GUI

Anda dapat terhubung ke instance Mac menggunakan SSH atau antarmuka pengguna grafis (GUI).

Beberapa pengguna dapat mengakses OS secara bersamaan. Biasanya ada sesi pengguna 1:1: GUI, karena layanan Berbagi Layar bawaan pada port 5900. Menggunakan SSH dalam macOS mendukung beberapa sesi hingga batas “Sesi Maks” dalam `sshd_config` file.

Terhubung ke instans Anda menggunakan SSH

Instans Mac Amazon EC2 tidak mengizinkan SSH root jarak jauh secara default. ec2-userAkun dikonfigurasi untuk masuk dari jarak jauh menggunakan SSH. ec2-userAkun ini juga memiliki sudo hak istimewa. Setelah Anda terhubung ke instans, Anda dapat menambahkan pengguna lain.

Untuk mendukung koneksi ke instans Anda menggunakan SSH, luncurkan instans menggunakan pasangan kunci dan grup keamanan yang mengizinkan akses SSH, dan pastikan bahwa instans tersebut memiliki konektivitas internet. Anda menyediakan file `.pem` untuk pasangan kunci saat Anda terhubung ke instans.

Gunakan prosedur berikut untuk menghubungkan ke instans Mac Anda menggunakan klien SSH. Jika Anda menemui kesalahan saat mencoba untuk terhubung ke instans, lihat Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda.

Untuk terhubung ke instans Anda menggunakan SSH

1. Pastikan bahwa komputer lokal Anda memiliki klien SSH yang terinstal dengan memasukkan ssh di baris perintah. Jika komputer Anda tidak mengenali perintah tersebut, cari klien SSH untuk sistem operasi Anda lalu instal.
2. Dapatkan nama DNS publik dari instans Anda. Dengan menggunakan konsol Amazon EC2, Anda dapat menemukan nama DNS publik di tab Detail dan tab Jaringan. Dengan menggunakan AWS CLI, Anda dapat menemukan nama DNS publik menggunakan perintah describe-instance.
3. Temukan file `.pem` untuk pasangan kunci yang Anda tentukan saat meluncurkan instans.
4. Hubungkan ke instans Anda menggunakan perintah ssh berikut, yang menentukan nama DNS publik dari instans dan file `.pem`.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

Autentikasi kata sandi dinonaktifkan untuk mencegah serangan kata sandi brute-force. Sebelum Anda membuat perubahan pada konfigurasi SSH, buka `/usr/local/aws/ec2-macos-init/init.toml` dan atur `secureSSHDConfig` ke`false`.

Hubungkan ke antarmuka pengguna grafis (GUI) instans Anda

Gunakan prosedur berikut untuk terhubung ke GUI instans Anda menggunakan VNC, Apple Remote Desktop (ARD), atau aplikasi Apple Screen Sharing (disertakan dengan macOS).

> **Note**
>
> macOS 10.14 dan setelahnya hanya mengizinkan kontrol jika Berbagi Layar diaktifkan melalui Preferensi Sistem.

Untuk terhubung ke instans Anda menggunakan klien ARD atau klien VNC

1. Pastikan komputer lokal Anda menginstal klien ARD atau klien VNC yang mendukung ARD. Pada macOS, Anda dapat memanfaatkan aplikasi Berbagi Layar bawaan. Jika tidak, cari ARD untuk sistem operasi Anda dan instal.
2. Dari komputer lokal Anda, hubungkan ke instans Anda menggunakan SSH.
3. Siapkan kata sandi untuk akun ec2-user menggunakan perintah passwd sebagai berikut.

```
[ec2-user ~]$ sudo passwd ec2-user
```

4. Instal dan mulai macOS Screen Sharing menggunakan perintah berikut.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

5. Putuskan sambungan dari instans dengan mengetik exit dan menekan Enter.
6. Dari komputer Anda, hubungkan ke instans Anda menggunakan perintah ssh berikut ini. Selain opsi yang ditunjukkan di bagian sebelumnya, gunakan opsi -L untuk mengaktifkan penerusan port dan meneruskan semua lalu lintas di port lokal 5900 ke server ARD pada instans.

```
ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

7. Dari komputer lokal Anda, gunakan klien ARD atau klien VNC yang mendukung ARD untuk terhubung ke `localhost:5900`. Misalnya, gunakan aplikasi Berbagi Layar pada macOS sebagai berikut:

   a. Buka Finder dan pilih Go.

   b. Pilih Hubungkan ke Server.

   c. Di bidang Alamat Server, masukkan `vnc://localhost:5900`.

   d. Masuk seperti yang diminta, gunakan **`ec2-user`** sebagai nama pengguna dan kata sandi yang Anda buat untuk akun pengguna ec2.

Mengubah resolusi layar macOS di instans Mac

Setelah tersambung ke instans Mac EC2 menggunakan klien ARD atau klien VNC yang mendukung ARD, Anda dapat mengubah resolusi layar lingkungan macOS menggunakan alat atau utilitas macOS yang tersedia untuk umum, seperti displayplacer.

Untuk mengubah resolusi layar menggunakan displayplacer

1. Instal displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Tampilkan informasi layar saat ini dan kemungkinan resolusi layar.

```
[ec2-user ~]$ displayplacer list
```

3. Terapkan resolusi layar yang diinginkan.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

Contoh:

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Perbarui sistem operasi dan perangkat lunak pada instans Amazon EC2 Mac

Topik berikut menjelaskan cara memperbarui sistem operasi dan perangkat lunak pada instance Apple silikon Mac (Mac2, Mac2-M1Ultra, Mac2-m2, Mac2-M2Pro, Mac-M4, dan Mac-M4Pro) dan instance Mac x86 (Mac1).

Warning

Instalasi versi beta atau pratinjau macOS hanya tersedia di instance Apple silicon Mac. Amazon EC2 tidak memenuhi syarat versi beta atau pratinjau macOS dan tidak memastikan instans akan tetap berfungsi setelah pembaruan ke versi macOS praproduksi.
Mencoba menginstal versi beta atau pratinjau macOS di instans Amazon EC2 x86 Mac akan menyebabkan degradasi Host Khusus Amazon EC2 Mac saat Anda menghentikan atau mengakhiri instans, dan akan menghambat Anda untuk memulai atau meluncurkan instans baru di host tersebut.

Note

Jika Anda melakukan pembaruan macOS di tempat sebelum AWS merilis AMI resmi, pembaruan hanya berlaku untuk host yang dipilih. Jika Anda memiliki host lain, atau jika Anda meluncurkan host baru, Anda harus melakukan proses pembaruan yang sama pada host tersebut juga. Setiap versi macOS memerlukan versi firmware minimum pada

perangkat keras Apple Mac yang mendasarinya. Pembaruan di tempat hanya memperbarui firmware pada host yang dipilih dan tidak mentransfer ke host lain yang ada atau baru. Untuk memeriksa versi macOS mana yang kompatibel dengan Host Khusus Amazon EC2 Mac, lihat Menemukan versi macOS yang didukung untuk Host Khusus Amazon EC2 Mac Anda.

Perbarui perangkat lunak pada instans Mac Apple silicon

Prasyarat

Karena pembaruan dalam konfigurasi driver jaringan, driver ENA versi 1.0.2 tidak kompatibel dengan macOS 13.3 dan yang lebih baru. Jika Anda ingin menginstal versi beta, pratinjau, atau produksi macOS versi 13.3 atau setelahnya dan belum menginstal driver ENA terbaru, gunakan prosedur berikut untuk menginstal versi driver yang baru.

Untuk menginstal driver ENA versi baru

1. Di jendela Terminal, sambungkan ke instans Mac Apple silicon menggunakan SSH.
2. Perbarui Homebrew dan unduh aplikasi ENA ke dalam `Applications` file menggunakan perintah berikut.

```
[ec2-user ~]$ brew update
```

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

3. Putuskan sambungan dari instans Anda dengan mengetik exit dan menekan kembali.
4. Gunakan klien VNC untuk mengaktifkan aplikasi ENA.
   a. Siapkan klien VNC menggunakan Hubungkan ke antarmuka pengguna grafis (GUI) instans Anda.
   b. Setelah Anda terhubung ke instans Anda menggunakan aplikasi Berbagi Layar, buka folder Aplikasi dan buka aplikasi ENA.
   c. Pilih Aktifkan
   d. Untuk mengonfirmasi bahwa driver diaktifkan dengan benar, jalankan perintah berikut di jendela Terminal. Output dari perintah menunjukkan bahwa driver lama dalam keadaan diakhiri dan driver baru dalam keadaan diaktifkan.

```
systemextensionsctl list;
```

e. Setelah Anda memulai ulang instans, hanya driver baru yang akan hadir.

Lakukan pembaruan perangkat lunak

Pada instans Mac Apple silicon, Anda harus menyelesaikan beberapa langkah untuk melakukan pembaruan sistem operasi di tempat. Ini termasuk mendelegasikan kepemilikan volume root Amazon EBS ke pengguna administratif volume root EBS. Anda dapat memilih untuk melakukan ini secara otomatis menggunakan Amazon EC2 API, atau Anda dapat melakukannya secara manual dengan menjalankan perintah pada instance Anda.

Automated volume ownership delegation (Recommended)

Pertimbangan-pertimbangan

- Diperlukan waktu antara 30 dan 90 menit untuk menyelesaikan tugas delegasi kepemilikan volume. Selama waktu ini, instance tidak dapat dijangkau.
- Versi macOS berikut didukung:
  - Mac2 | Mac2-M1Ultra - macOS Ventura (versi 13.0 atau yang lebih baru)
  - Mac2-m2 | Mac2-M2Pro - macOS Ventura (versi 13.2 atau yang lebih baru)
  - Mac-M4 | Mac-M4Pro - macOS Sequoia (versi 15.6 atau yang lebih baru)
- Instans harus memiliki hanya satu volume yang dapat di-boot, dan setiap volume terlampir hanya dapat memiliki satu pengguna admin tambahan.

Langkah 1: Tetapkan kata sandi dan aktifkan token aman untuk pengguna administratif volume root EBS

Anda harus menyetel kata sandi dan mengaktifkan token aman untuk pengguna administratif volume root Amazon EBS (`ec2-user`).

> **Note**
>
> Kata sandi dan token aman disetel saat pertama kali Anda terhubung ke instans Apple silikon Mac menggunakan GUI. Jika sebelumnya Anda terhubung ke instance menggunakan GUI, Anda tidak perlu melakukan langkah-langkah ini.

1. Connect ke instance menggunakan SSH.
2. Atur kata sandi untuk `ec2-user` pengguna.

```
$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

3. Aktifkan token aman untuk `ec2-user` pengguna. Untuk `-oldPassword`, tentukan kata sandi yang sama dari langkah sebelumnya. Untuk `-newPassword`, tentukan kata sandi yang berbeda. Perintah berikut mengasumsikan bahwa Anda memiliki kata sandi lama dan baru yang disimpan dalam `.txt` file.

```
$ sysadminctl -oldPassword `cat old_password.txt` -newPassword `cat
 new_password.txt`
```

4. Verifikasi bahwa token aman diaktifkan.

```
$ sysadminctl -secureTokenStatus ec2-user
```

Langkah 2: Delegasikan kepemilikan volume root Amazon EBS ke pengguna administratif volume root EBS

Untuk mendelegasikan kepemilikan, Anda harus membuat tugas delegasi kepemilikan volume.

1. Gunakan perintah create-delegate-mac-volume-ownership-task untuk membuat tugas. Untuk `--instance-id`, tentukan ID instance. Untuk `--mac-credentials`, tentukan kredensil berikut:
   - Pengguna administratif disk internal
     - Nama pengguna - Hanya pengguna administratif default (`aws-managed-user`) yang didukung dan digunakan secara default. Anda tidak dapat menentukan pengguna administratif yang berbeda.
     - Kata sandi — Jika Anda tidak mengubah kata sandi default untuk `aws-managed-user`, tentukan kata sandi default, yang kosong. Jika tidak, tentukan kata sandi Anda.
   - Pengguna administratif volume root Amazon EBS
     - Nama pengguna — Jika Anda tidak mengubah pengguna administratif default, tentukan `ec2-user`. Jika tidak, tentukan nama pengguna untuk pengguna administratif Anda.

- Kata sandi - Tentukan kata sandi yang Anda tetapkan untuk pengguna admin volume root pada Langkah 1 di atas.

```
aws ec2 create-delegate-mac-volume-ownership-task \
--instance-id i-1234567890abcdef0 \
--mac-credentials file://mac-credentials.json
```

Berikut ini adalah isi dari `mac-credentials.json` file yang direferensikan dalam contoh sebelumnya.

```
{
  "internalDiskPassword":"internal-disk-admin_password",
  "rootVolumeUsername":"root-volume-admin_username",
  "rootVolumepassword":"root-volume-admin_password"
}
```

2. Tunggu tugas delegasi kepemilikan volume selesai dan instance kembali ke keadaan sehat. Gunakan perintah describe-mac-modification-tasks. Untuk`--mac-modification-task-id`, tentukan ID tugas delegasi kepemilikan volume dari langkah sebelumnya.

```
aws ec2 describe-mac-modification-tasks \
--mac-modification-task-id task-id
```

3. Setelah tugas delegasi kepemilikan volume selesai, lanjutkan ke Langkah 3.

Langkah 3: Perbarui perangkat lunak

Setelah Anda mendelegasikan kepemilikan volume root Amazon EBS, ikuti langkah-langkah yang dijelaskan dalam Perbarui perangkat lunak pada instans Mac x86 (di bawah) untuk memperbarui perangkat lunak.

Manual volume ownership delegation

Saat Anda mengerjakan prosedur ini, Anda membuat dua kata sandi. Satu kata sandi adalah untuk pengguna administratif volume root Amazon EBS (`ec2-user`), dan kata sandi lainnya adalah untuk pengguna administratif disk internal (`aws-managed-user`). Ingat kata sandi ini karena Anda akan menggunakannya saat Anda mengerjakan prosedur.

> **Note**
>
> Dengan prosedur ini di macOS Big Sur, Anda hanya dapat melakukan pembaruan kecil seperti memperbarui dari macOS Big Sur 11.7.3 ke macOS Big Sur 11.7.4. Untuk macOS Monterey atau lebih tinggi, Anda dapat melakukan pembaruan perangkat lunak utama.

Untuk mengakses disk internal

1. Dari komputer lokal Anda, di Terminal, sambungkan ke instans Apple silicon Mac Anda menggunakan SSH dengan perintah berikut. Untuk informasi selengkapnya, lihat Terhubung ke instans Anda menggunakan SSH.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

2. Instal dan mulai macOS Screen Sharing menggunakan perintah berikut.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/
   com.apple.screensharing.plist
   ```

3. Tetapkan kata sandi untuk `ec2-user` dengan perintah berikut. Ingat kata sandi karena Anda akan menggunakannya nanti.

   ```
   [ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
   ```

4. Putuskan sambungan dari instans dengan mengetik exit dan menekan return.
5. Dari komputer lokal Anda, di Terminal, hubungkan kembali ke instans Anda dengan terowongan SSH ke port VNC menggunakan perintah berikut.

   ```
   ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-
   dns-name
   ```

   > **Note**
   >
   > Jangan keluar dari sesi SSH ini sampai koneksi VNC berikut dan langkah-langkah GUI selesai. Ketika instans dimulai ulang, koneksi akan menutup secara otomatis.

6. Dari komputer lokal Anda, hubungkan ke `localhost:5900` menggunakan langkah-langkah berikut:

   a. Buka Finder dan pilih Go.

   b. Pilih Hubungkan ke Server.

   c. Di bidang Alamat Server, masukkan `vnc://localhost:5900`.

7. Di jendela macOS, sambungkan ke sesi jarak jauh instans Apple silicon Mac seperti kata sandi `ec2-user` yang Anda buat di Langkah 3.

8. Akses disk internal, bernama InternalDisk, menggunakan salah satu opsi berikut.

   a. Untuk macOS Ventura atau di atasnya: Buka Pengaturan Sistem, pilih Umum di panel kiri, lalu Startup Disk di kanan bawah panel.

   b. Untuk macOS Monterey atau di bawahnya: Buka Preferensi Sistem, pilih Mulai Disk, lalu buka kunci panel dengan memilih ikon kunci di kiri bawah jendela.

> **Tip pemecahan masalah**
>
> Jika Anda perlu memasang disk internal, jalankan perintah berikut di Terminal.
>
> ```
> APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
>  "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
>  diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
> ```

9. Pilih disk internal, bernama InternalDisk, dan pilih Restart. Pilih Mulai Ulang lagi saat diminta.

> **Important**
>
> Jika disk internal diberi nama Macintosh HD InternalDisk, instans Anda harus dihentikan dan dimulai ulang sehingga host khusus dapat diperbarui. Untuk informasi selengkapnya, lihat Menghentikan atau menghentikan instans Amazon EC2 Mac Anda.

Gunakan prosedur berikut untuk mendelegasikan kepemilikan kepada pengguna administratif. Ketika Anda menyambung kembali ke instans Anda dengan SSH, lakukan boot dari disk internal menggunakan user administratif khusus (`aws-managed-user`). Kata sandi awal untuk `aws-`

`managed-user` adalah kosong, jadi Anda perlu menimpanya pada koneksi pertama Anda. Kemudian, Anda perlu mengulangi langkah-langkah untuk menginstal dan memulai MacOS Screen Sharing karena volume boot telah berubah.

Untuk mendelegasikan kepemilikan kepada administrator pada volume Amazon EBS

1. Dari komputer lokal Anda, di Terminal, sambungkan ke instans Apple silicon Mac Anda menggunakan perintah berikut.

   ```
   ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
   ```

2. Saat Anda menerima peringatan `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, gunakan salah satu perintah berikut untuk mengatasi masalah ini.

   a. Hapus host yang dikenal menggunakan perintah berikut. Kemudian, ulangi langkah sebelumnya.

   ```
   rm ~/.ssh/known_hosts
   ```

   b. Tambahkan berikut ini ke perintah SSH di langkah sebelumnya.

   ```
   -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
   ```

3. Tetapkan kata sandi untuk `aws-managed-user` dengan perintah berikut. Kata sandi awal `aws-managed-user` adalah kosong, jadi Anda perlu menimpanya pada koneksi pertama Anda.

   a.
   ```
   [aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
   ```

   b. Saat Anda menerima prompt `Permission denied. Please enter user's old password:`, tekan enter.

   > **Tip pemecahan masalah**
   >
   > Jika Anda mendapatkan kesalahan `passwd: DS error: eDSAuthFailed`, gunakan perintah berikut.
   >
   > ```
   > [aws-managed-user ~]$ sudo passwd aws-managed-user
   > ```

4. Instal dan mulai macOS Screen Sharing menggunakan perintah berikut.

```
[aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/
com.apple.screensharing.plist
```

5. Putuskan sambungan dari instans dengan mengetik exit dan menekan return.
6. Dari komputer lokal Anda, di Terminal, hubungkan kembali ke instans Anda dengan terowongan SSH ke port VNC menggunakan perintah berikut.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-
public-dns-name
```

7. Dari komputer lokal Anda, hubungkan ke `localhost:5900` menggunakan langkah-langkah berikut:

   a. Buka Finder dan pilih Go.

   b. Pilih Hubungkan ke Server.

   c. Di bidang Alamat Server, masukkan `vnc://localhost:5900`.

8. Di jendela macOS, sambungkan ke sesi jarak jauh instans Apple silicon Mac seperti kata sandi `aws-managed-user` yang Anda buat di Langkah 3.

> **Note**
>
> Saat diminta untuk masuk dengan ID Apple Anda, pilih Atur Nanti.

9. Akses volume Amazon EBS menggunakan salah satu opsi berikut.

   a. Untuk macOS Ventura atau lebih baru: Buka Pengaturan Sistem, pilih Umum di panel kiri, lalu Startup Disk di kanan bawah panel.

   b. Untuk macOS Monterey atau sebelumnya: Buka Preferensi Sistem, pilih Mulai Disk, lalu buka kunci panel dengan memilih ikon kunci di kiri bawah jendela.

> **Note**
>
> Sampai reboot berlangsung, ketika dimintai kata sandi administrator, gunakan kata sandi yang Anda tetapkan di atas untuk `aws-managed-user`. Kata sandi ini mungkin berbeda dari yang Anda tetapkan untuk `ec2-user` atau akun administrator default

pada instans Anda. Petunjuk berikut menentukan kapan harus menggunakan kata sandi administrator instans Anda.

10. Pilih volume Amazon EBS (volume yang tidak disebutkan InternalDiskdi jendela Disk Startup) dan pilih Restart.

> **Note**
>
> Jika Anda memiliki beberapa volume Amazon EBS yang dapat di-boot yang terpasang pada instans Apple silicon Mac Anda, pastikan untuk menggunakan nama unik untuk setiap volume.

11. Konfirmasikan mulai ulang, lalu pilih Otorisasi Pengguna saat diminta.
12. Pada panel Otorisasi pengguna pada volume ini, pastikan bahwa pengguna administratif (`ec2-user` secara default) telah dipilih, lalu pilih Otorisasi.
13. Masukkan `ec2-user` kata sandi yang Anda buat di Langkah 3 dari prosedur sebelumnya, lalu pilih Lanjutkan.
14. Masukkan kata sandi untuk pengguna administratif khusus (`aws-managed-user`) saat diminta.
15. Dari komputer lokal Anda, di Terminal, sambungkan kembali ke instans Anda menggunakan SSH dengan nama pengguna. `ec2-user`

> **Tip pemecahan masalah**
>
> Jika Anda mendapatkan peringatan `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, jalankan perintah berikut dan hubungkan kembali ke instans Anda menggunakan SSH.
>
> ```
> rm ~/.ssh/known_hosts
> ```

16. Untuk melakukan pembaruan perangkat lunak, gunakan perintah di bawah Perbarui perangkat lunak pada instans Mac x86.

Perbarui perangkat lunak pada instans Mac x86

Pada instans x86, Anda dapat menginstal pembaruan sistem operasi dari Apple menggunakan perintah.`softwareupdate`

Untuk menginstal pembaruan sistem operasi dari Apple pada instans Mac x86

1. Daftar paket dengan pembaruan yang tersedia menggunakan perintah berikut.

   ```
   [ec2-user ~]$ softwareupdate --list
   ```

2. Menginstal semua pembaruan atau hanya pembaruan tertentu. Untuk menginstal pembaruan tertentu, gunakan perintah berikut.

   ```
   [ec2-user ~]$ sudo softwareupdate --install label
   ```

   Untuk menginstal semua pembaruan, gunakan perintah berikut.

   ```
   [ec2-user ~]$ sudo softwareupdate --install --all --restart
   ```

Administrator sistem dapat digunakan AWS Systems Manager untuk meluncurkan pembaruan sistem operasi yang telah disetujui sebelumnya pada instance Mac x86. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Systems Manager.

Anda dapat menggunakan Homebrew untuk menginstal pembaruan paket di AMI EC2 macOS, sehingga Anda memiliki versi terbaru dari paket-paket ini di instance Anda. Anda juga dapat menggunakan Homebrew untuk menginstal dan menjalankan aplikasi macOS umum di Amazon EC2 macOS. Untuk informasi selengkapnya, lihat Dokumentasi Homebrew.

Untuk menginstal pembaruan menggunakan Homebrew

1. Perbarui Homebrew menggunakan perintah berikut.

   ```
   [ec2-user ~]$ brew update
   ```

2. Daftar paket dengan pembaruan yang tersedia menggunakan perintah berikut.

   ```
   [ec2-user ~]$ brew outdated
   ```

3. Menginstal semua pembaruan atau hanya pembaruan tertentu. Untuk menginstal pembaruan tertentu, gunakan perintah berikut.

```
[ec2-user ~]$ brew upgrade package name
```

Untuk menginstal semua pembaruan, gunakan perintah berikut.

```
[ec2-user ~]$ brew upgrade
```

Meningkatkan ukuran volume EBS di instans Mac Anda

Anda dapat meningkatkan ukuran volume Amazon EBS pada instans Mac Anda. Untuk informasi selengkapnya, lihat Volume Elastis Amazon EBS di Panduan Pengguna Amazon EBS.

Setelah Anda meningkatkan ukuran volumenya, Anda harus meningkatkan ukuran kontainer APFS sebagai berikut.

Tingkatkan ruang disk yang tersedia untuk digunakan

1. Menentukan apakah mulai ulang diperlukan. Jika Anda mengubah ukuran volume EBS pada instans Mac yang sedang berjalan, Anda harus melakukan boot ulang pada instans tersebut agar volume baru tersedia. Jika modifikasi ruang disk dilakukan selama waktu peluncuran, maka boot ulang tidak akan diperlukan.

   Lihat status ukuran disk saat ini:

```
[ec2-user ~]$  diskutil list external physical
/dev/disk0 (external, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:                 GUID_partition_scheme           *322.1 GB     disk0
   1:                 EFI EFI                          209.7 MB     disk0s1
   2:                 Apple_APFS Container disk2       321.9 GB     disk0s2
```

2. Salin dan tempel perintah berikut ini.

```
[ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
d" " -f8)
yes | sudo diskutil repairDisk $PDISK
```

3. Salin dan tempel perintah berikut ini.

```
[ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
```

Menghentikan atau menghentikan instans Amazon EC2 Mac Anda

Bila Anda menghentikan instans Mac, maka instans tersebut tetap berada di dalam status `stopping` selama sekitar 15 menit sebelum memasuki status.`stopped`

Saat Anda menghentikan atau mengakhiri instans Mac, Amazon EC2 melakukan alur kerja scrubbing pada Host Khusus dasar untuk menghapus SSD internal, untuk membersihkan variabel NVRAM persisten, dan memperbarui ke firmware perangkat terbaru. Ini memastikan bahwa instance Mac memberikan keamanan dan privasi data yang sama seperti instans EC2 Nitro lainnya. Ini juga memungkinkan Anda untuk menjalankan AMI macOS terbaru. Selama alur kerja scrubbing, Host Khusus sementara memasuki status tertunda. Pada instans x86 Mac, alur kerja scrubbing mungkin membutuhkan waktu hingga 50 menit untuk menyelesaikannya. Jika Amazon EC2 perlu memperbarui firmware perangkat, alur kerja mungkin memakan waktu hingga 3 jam untuk menyelesaikannya. Pada instance Apple silicon Mac, alur kerja scrubbing mungkin membutuhkan waktu hingga 4,5 jam untuk diselesaikan.

Anda tidak dapat memulai instans Mac yang dihentikan atau meluncurkan instans Mac baru sampai setelah alur kerja scrubbing selesai, yang mana pada saat itu Host Khusus memasuki status.`available`

Pengukuran dan penagihan dijeda saat Host Khusus memasuki status.`pending` Anda tidak dikenai biaya untuk alur kerja scrubbing.

Lepaskan Host Khusus untuk instans Mac Anda

Saat Anda selesai dengan instans Mac, Anda dapat melepaskan Host Khusus. Sebelum Anda dapat melepaskan Host Khusus, Anda harus menghentikan atau mengakhiri instans Mac. Anda tidak dapat melepaskan host hingga periode alokasi melebihi minimal 24 jam.

Untuk melepas Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans dan pilih Status instans, lalu pilih Hentikan instans atau Akhiri instans.

4. Di panel navigasi, pilih Host Khusus.
5. Pilih Host Khusus dan pilih Tindakan, Lepas host.
6. Ketika diminta konfirmasi, pilih Lepaskan.

Konfigurasikan Perlindungan Integritas Sistem untuk instans Amazon EC2 Mac

Anda dapat mengonfigurasi pengaturan Perlindungan Integritas Sistem (SIP) untuk instans Mac x86 dan instans Apple silicon Mac. SIP adalah fitur keamanan macOS penting yang membantu mencegah eksekusi kode yang tidak sah dan modifikasi tingkat sistem. Untuk informasi selengkapnya, lihat Tentang Perlindungan Integritas Sistem.

Anda dapat mengaktifkan atau menonaktifkan SIP sepenuhnya, atau Anda dapat mengaktifkan atau menonaktifkan pengaturan SIP tertentu secara selektif. Disarankan agar Anda menonaktifkan SIP hanya sementara untuk melakukan tugas-tugas yang diperlukan, dan kemudian mengaktifkannya kembali sesegera mungkin. Meninggalkan SIP dinonaktifkan dapat membuat instance Anda rentan terhadap kode berbahaya.

Konfigurasi SIP didukung di semua AWS Wilayah di mana instans Amazon EC2 Mac didukung.

Topik

- Pertimbangan-pertimbangan
- Konfigurasi SIP default
- Periksa konfigurasi SIP Anda
- Prasyarat untuk instance Apple silicon Mac
- Konfigurasikan pengaturan SIP
- Periksa status tugas konfigurasi SIP

Pertimbangan-pertimbangan

- Jenis instans Amazon EC2 Mac berikut dan versi macOS didukung:
  - Mac1 | Mac2 | Mac2-M1Ultra - macOS Ventura (versi 13.0 atau yang lebih baru)
  - Mac2-m2 | Mac2-M2Pro - macOS Ventura (versi 13.2 atau yang lebih baru)
  - Mac-M4 | Mac-M4Pro - macOS Sequoia (versi 15.6 atau yang lebih baru)

> **Note**
>
> Versi beta dan pratinjau macOS tidak didukung.

- Anda dapat menentukan konfigurasi SIP khusus untuk mengaktifkan atau menonaktifkan pengaturan SIP individual secara selektif. Jika Anda menerapkan konfigurasi kustom, sambungkan ke instans dan verifikasi pengaturan untuk memastikan bahwa persyaratan Anda diterapkan dengan benar dan berfungsi sebagaimana dimaksud.

  Konfigurasi SIP mungkin berubah dengan pembaruan macOS. Kami menyarankan Anda meninjau pengaturan SIP khusus setelah upgrade versi macOS apa pun untuk memastikan kompatibilitas berkelanjutan dan fungsionalitas yang tepat dari konfigurasi keamanan Anda.
- Untuk instance Mac x86, pengaturan SIP diterapkan pada tingkat instans. Setiap volume root yang melekat pada instance akan secara otomatis mewarisi pengaturan SIP yang dikonfigurasi.

  Untuk instance Apple silicon Mac, pengaturan SIP diterapkan pada tingkat volume. Volume root yang dilampirkan ke instance tidak mewarisi pengaturan SIP. Jika Anda melampirkan volume root lain, Anda harus mengkonfigurasi ulang pengaturan SIP ke status yang diperlukan.
- Diperlukan waktu hingga 90 menit untuk menyelesaikan tugas konfigurasi SIP. Instance tetap tidak dapat dijangkau saat tugas konfigurasi SIP sedang berlangsung.
- Konfigurasi SIP tidak ditransfer ke snapshot atau AMIs yang kemudian Anda buat dari instance.
- Instans Apple silicon Mac harus memiliki hanya satu volume yang dapat di-boot, dan setiap volume terlampir hanya dapat memiliki satu pengguna admin tambahan.

Konfigurasi SIP default

Tabel berikut mencantumkan konfigurasi SIP default untuk instance Mac x86 dan instance Apple silicon Mac.

	Instans Apple silikon Mac	contoh x86 Mac
Apple Internal	Diaktifkan	Dinonaktifkan
Perlindungan Sistem File	Diaktifkan	Dinonaktifkan
Sistem Dasar	Diaktifkan	Diaktifkan

	Instans Apple silikon Mac	contoh x86 Mac
Pembatasan Debugging	Diaktifkan	Diaktifkan
Pembatasan Dtrace	Diaktifkan	Diaktifkan
Penandatanganan Kext	Diaktifkan	Diaktifkan
Perlindungan Nvram	Diaktifkan	Diaktifkan

Periksa konfigurasi SIP Anda

Kami menyarankan Anda memeriksa konfigurasi SIP Anda sebelum dan sesudah membuat perubahan untuk memastikan bahwa konfigurasi tersebut dikonfigurasi seperti yang diharapkan.

Untuk memeriksa konfigurasi SIP untuk instans Amazon EC2 Mac

Connect ke instance menggunakan SSH, dan kemudian jalankan perintah berikut di baris perintah.

```
$ csrutil status
```

Berikut ini adalah output contoh.

```
System Integrity Protection status: enabled.

Configuration:
    Apple Internal: enabled
    Kext Signing: disabled
    Filesystem Protections: enabled
    Debugging Restrictions: enabled
    DTrace Restrictions: enabled
    NVRAM Protections: enabled
    BaseSystem Verification: disabled
```

Prasyarat untuk instance Apple silicon Mac

Sebelum Anda dapat mengonfigurasi pengaturan SIP untuk instance Apple silicon Mac, Anda harus mengatur kata sandi dan mengaktifkan token aman untuk pengguna administratif volume root Amazon EBS ()`ec2-user`.

> **Note**
>
> Kata sandi dan token aman disetel saat pertama kali Anda terhubung ke instans Apple silikon Mac menggunakan GUI. Jika sebelumnya Anda terhubung ke instans menggunakan GUI, atau jika Anda menggunakan instance Mac x86, Anda tidak perlu melakukan langkah-langkah ini.

> **Note**
>
> Semua nama pengguna dan kata sandi macOS yang digunakan untuk otentikasi macOS harus antara 4 dan 16 karakter untuk digunakan dengan panggilan API pengaturan SIP.

Untuk mengatur kata sandi dan mengaktifkan token aman untuk pengguna administratif volume root EBS

1. Connect ke instance menggunakan SSH.
2. Atur kata sandi untuk `ec2-user` pengguna.

```
$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

3. Aktifkan token aman untuk `ec2-user` pengguna. Untuk `-oldPassword`, tentukan kata sandi yang sama dari langkah sebelumnya. Untuk `-newPassword`, tentukan kata sandi yang berbeda. Perintah berikut mengasumsikan bahwa Anda memiliki kata sandi lama dan baru yang disimpan dalam `.txt` file.

```
$ sysadminctl -oldPassword `cat old_password.txt` -newPassword `cat
 new_password.txt`
```

4. Verifikasi bahwa token aman diaktifkan.

```
$ sysadminctl -secureTokenStatus ec2-user
```

Konfigurasikan pengaturan SIP

Saat Anda mengonfigurasi pengaturan SIP untuk instans Anda, Anda dapat mengaktifkan atau menonaktifkan semua pengaturan SIP, atau Anda dapat menentukan konfigurasi khusus yang secara selektif mengaktifkan atau menonaktifkan pengaturan SIP tertentu.

> **Note**
>
> Jika Anda menerapkan konfigurasi kustom, sambungkan ke instans dan verifikasi pengaturan untuk memastikan bahwa persyaratan Anda diterapkan dengan benar dan berfungsi sebagaimana dimaksud.
> Konfigurasi SIP mungkin berubah dengan pembaruan macOS. Kami menyarankan Anda meninjau pengaturan SIP khusus setelah upgrade versi macOS apa pun untuk memastikan kompatibilitas berkelanjutan dan fungsionalitas yang tepat dari konfigurasi keamanan Anda.

Untuk mengkonfigurasi pengaturan SIP untuk instance Anda, Anda harus membuat tugas konfigurasi SIP. Tugas konfigurasi SIP menentukan pengaturan SIP untuk instance Anda.

Saat membuat konfigurasi SIP untuk instance Apple silicon Mac, Anda harus menentukan kredensi berikut:

- Pengguna administratif disk internal
  - Nama pengguna - Hanya pengguna administratif default (`aws-managed-user`) yang didukung dan digunakan secara default. Anda tidak dapat menentukan pengguna administratif yang berbeda.
  - Kata sandi — Jika Anda tidak mengubah kata sandi default untuk`aws-managed-user`, tentukan kata sandi default, yang kosong. Jika tidak, tentukan kata sandi Anda.
- Pengguna administratif volume root Amazon EBS
  - Nama pengguna — Jika Anda tidak mengubah pengguna administratif default, tentukan`ec2-user`. Jika tidak, tentukan nama pengguna untuk pengguna administratif Anda.
  - Kata sandi — Anda harus selalu menentukan kata sandi.

Gunakan metode berikut untuk membuat tugas konfigurasi SIP.

Console

Untuk membuat tugas konfigurasi SIP menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans dan kemudian pilih instans Amazon EC2 Mac.
3. Di tab Keamanan, pilih Ubah Mac, Ubah Perlindungan Integritas Sistem.
4. Untuk mengaktifkan semua pengaturan SIP, pilih Aktifkan SIP. Untuk menonaktifkan semua pengaturan SIP, hapus Aktifkan SIP.
5. Untuk menentukan konfigurasi khusus yang secara selektif mengaktifkan atau menonaktifkan pengaturan SIP tertentu, pilih Tentukan konfigurasi SIP khusus, lalu pilih pengaturan SIP untuk mengaktifkan, atau hapus pengaturan SIP untuk menonaktifkan.
6. Tentukan kredensil untuk pengguna volume root dan pemilik disk internal.
7. Pilih Buat tugas modifikasi SIP.

AWS CLI

Untuk membuat tugas konfigurasi SIP menggunakan AWS CLI

Gunakan protection-modification-task perintah create-mac-system-integrity-.

Aktifkan atau nonaktifkan semua pengaturan SIP

Untuk sepenuhnya mengaktifkan atau menonaktifkan semua pengaturan SIP, gunakan hanya `--mac-system-integrity-protection-status` parameter.

Contoh perintah berikut memungkinkan semua pengaturan SIP.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status enabled \
--mac-credentials file://mac-credentials.json
```

Tentukan konfigurasi SIP khusus

Untuk menentukan konfigurasi SIP khusus yang secara selektif mengaktifkan atau menonaktifkan pengaturan SIP tertentu, tentukan `--mac-system-integrity-protection-status` dan `--`

`mac-system-integrity-protection-configuration` parameter. Dalam hal ini, gunakan `mac-system-integrity-protection-status` untuk menentukan status SIP keseluruhan, dan gunakan `mac-system-integrity-protection-configuration` untuk mengaktifkan atau menonaktifkan pengaturan SIP individu secara selektif.

Contoh perintah berikut membuat tugas konfigurasi SIP untuk mengaktifkan semua pengaturan SIP, kecuali `NvramProtections` dan`FilesystemProtections`.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status enabled \
--mac-system-integrity-protection-configuration
 "NvramProtections=disabled, FilesystemProtections=disabled" \
--mac-credentials file://mac-credentials.json
```

Contoh perintah berikut membuat tugas konfigurasi SIP untuk menonaktifkan semua pengaturan SIP, kecuali`DtraceRestrictions`.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status disabled \
--mac-system-integrity-protection-configuration "DtraceRestrictions=enabled" \
--mac-credentials file://mac-credentials.json
```

Isi **`mac-credentials.json`** file

Berikut ini adalah isi dari `mac-credentials.json` file yang direferensikan dalam contoh sebelumnya.

```
{
  "internalDiskPassword":"internal-disk-admin_password",
  "rootVolumeUsername":"root-volume-admin_username",
  "rootVolumepassword":"root-volume-admin_password"
}
```

Periksa status tugas konfigurasi SIP

Gunakan salah satu metode berikut untuk memeriksa status tugas konfigurasi SIP.

Console

Untuk melihat tugas konfigurasi SIP menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans dan kemudian pilih instans Amazon EC2 Mac.
3. Di tab Keamanan, gulir ke bawah ke bagian tugas modifikasi Mac.

AWS CLI

Untuk memeriksa status tugas konfigurasi SIP menggunakan AWS CLI

Gunakan perintah describe-mac-modification-tasks.

Temukan versi macOS yang didukung untuk Host Khusus Amazon EC2 Mac

Anda dapat melihat versi macOS terbaru yang didukung oleh Host Khusus Amazon EC2 Mac Anda. Dengan fungsi ini, Anda dapat memvalidasi apakah Host Khusus dapat mendukung peluncuran instans dengan versi macOS pilihan Anda.

Setiap versi macOS memerlukan versi firmware minimum pada Apple Mac yang mendasarinya agar berhasil boot. Versi firmware Apple Mac dapat menjadi usang jika Mac Dedicated Host yang dialokasikan tetap menganggur untuk jangka waktu yang lama atau jika memiliki instance yang berjalan lama di dalamnya.

Untuk memastikan dukungan untuk versi macOS terbaru, Anda dapat menghentikan atau menghentikan instans pada Host Khusus Mac yang dialokasikan. Ini memicu alur kerja penggosokan host dan memperbarui firmware pada Apple Mac yang mendasarinya untuk mendukung versi macOS terbaru. Host Khusus dengan instans yang berjalan lama akan diperbarui secara otomatis saat Anda menghentikan atau menghentikan instance yang sedang berjalan.

Untuk informasi selengkapnya tentang alur kerja scrubbing, lihat. Menghentikan atau menghentikan instans Amazon EC2 Mac Anda

Untuk informasi selengkapnya tentang meluncurkan instance Mac, lihatLuncurkan instance Mac menggunakan Konsol Manajemen AWS atau AWS CLI.

Anda dapat melihat informasi tentang versi macOS terbaru yang didukung pada Host Khusus yang dialokasikan menggunakan konsol Amazon EC2 atau. AWS CLI

Console

Untuk melihat informasi firmware Host Khusus menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Di halaman Detail Host Khusus, di bawah Versi macOS terbaru yang didukung, Anda dapat melihat versi macOS terbaru yang dapat didukung oleh host.

AWS CLI

Untuk melihat informasi firmware Host Khusus menggunakan AWS CLI

Gunakan `describe-mac-hosts`perintah, ganti `region` dengan yang sesuai AWS Region.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
                  "12.7.3"
              ]
          }
      ]
  }
```

Berlangganan notifikasi AMI macOS

Untuk diberi tahu saat baru AMIs dirilis atau ketika BridgeOS telah diperbarui, berlangganan pemberitahuan menggunakan Amazon SNS.

Untuk informasi selengkapnya tentang AMIs macOS EC2, lihat. Catatan rilis macOS Amazon EC2 AMIs

Untuk berlangganan notifikasi AMI macOS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.

2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah ini karena notifikasi SNS tempat Anda berlangganan ada di Wilayah ini.
3. Di panel navigasi, pilih Langganan.
4. Pilih Buat langganan.
5. Untuk kotak dialog Buat langganan, lakukan hal berikut:

   a. Untuk Topik ARN, salin dan tempel salah satu Nama Sumber Daya Amazon berikut ()ARNs:

      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates`**
      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates`**

   b. Untuk Protokol, pilih salah satu dari berikut ini:

      - Email:

        Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi. Setelah Anda berlangganan, Anda akan menerima pesan konfirmasi dengan baris subjek `AWS Notification - Subscription Confirmation`. Buka email dan pilih Konfirmasi berlangganan untuk menyelesaikan langganan Anda

      - SMS:

        Untuk Titik Akhir, ketik nomor telepon yang bisa Anda gunakan untuk menerima notifikasi.

      - AWS Lambda, Amazon SQS, Amazon Data Firehose (Pemberitahuan datang dalam format JSON):

        Untuk Titik akhir, masukkan ARN untuk fungsi Lambda, antrean SQS, atau aliran Firehose yang dapat Anda gunakan untuk menerima notifikasi.

   c. Pilih Buat langganan.

Setiap kali macOS AMIs dirilis, kami mengirim pemberitahuan kepada pelanggan topik tersebut. `amazon-ec2-macos-ami-updates` Kapan pun bridgeOS diperbarui, kami akan mengirimkan notifikasi kepada pelanggan topik.`amazon-ec2-bridgeos-updates` Jika Anda tidak ingin lagi menerima notifikasi ini, gunakan prosedur berikut untuk berhenti berlangganan.

Untuk membatalkan langganan notifikasi AMI macOS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.

2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah ini karena notifikasi SNS dibuat di Wilayah ini.
3. Di panel navigasi, pilih Langganan.
4. Pilih langganan, lalu pilih Tindakan, Hapus langganan. Saat diminta konfirmasi, pilih Hapus.

Ambil macOS IDs AWS Systems Manager AMI menggunakan Parameter Store API

Anda harus menentukan AMI saat meluncurkan instans. AMI khusus untuk sistem operasi AWS Region, dan arsitektur prosesor. Anda dapat melihat semua macOS AMIs di AWS Region dan mengambil macOS AMI terbaru dengan menanyakan AWS Systems Manager Parameter Store API. Dengan menggunakan parameter publik ini, Anda tidak perlu mencari macOS AMI secara manual. IDs Parameter publik tersedia untuk keduanya x86 dan ARM64 macOS AMIs, dan dapat diintegrasikan dengan templat Anda yang ada AWS CloudFormation .

Izin yang diperlukan

Untuk melakukan tindakan ini, prinsipal IAM harus memiliki izin untuk memanggil tindakan `ssm:GetParameter` API.

Untuk melihat daftar semua macOS AMIs saat ini AWS Region menggunakan AWS CLI

Gunakan get-parameters-by-pathperintah berikut untuk melihat daftar semua macOS AMIs di Wilayah saat ini.

```
aws ssm get-parameters-by-path --path /aws/service/ec2-macos --recursive --query
 "Parameters[].Name"
```

Untuk mengambil ID AMI dari macOS AMI utama terbaru menggunakan AWS CLI

Gunakan perintah get-parameter berikut dengan sub-parameter. `image_id` Dalam contoh berikut, ganti `sonoma` dengan versi mayor yang didukung macOS, `x86_64_mac` dengan prosesor, dan `region-code` dengan AWS Region dukungan yang Anda inginkan ID macOS AMI terbaru.

```
aws ssm get-parameter --name /aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id
 --region region-code
```

Untuk informasi selengkapnya, lihat Memanggil parameter publik AMI untuk macOS di AWS Systems Manager Panduan Pengguna.

Catatan rilis macOS Amazon EC2 AMIs

Informasi berikut memberikan detail tentang paket yang disertakan secara default di EC2 macOS AMIs dan merangkum perubahan untuk setiap rilis EC2 macOS AMI.

Untuk informasi tentang cara berlangganan notifikasi macOS AMI, lihat. Berlangganan notifikasi AMI macOS

Instans Mac dapat menjalankan salah satu sistem operasi berikut:

- macOS Mojave (versi 10.14) (hanya instans x86 Mac)
- macOS Catalina (versi 10.15) (hanya instans x86 Mac)
- macOS Big Sur (versi 11) (instans x86 dan M1 Mac)
- macOS Monterey (versi 12) (instans x86 dan M1 Mac)
- macOS Ventura (versi 13) (semua instans Mac, instans M2 dan M2 Pro Mac mendukung macOS Ventura versi 13.2 atau setelahnya)
- macOS Sonoma (versi 14) (semua instans Mac)
- macOS Sequoia (versi 15) (semua instance Mac)

> **Note**
>
> Instans Mac M4 dan M4 Pro mendukung macOS Sequoia versi 15.6 atau yang lebih baru.

Menyetujui Kebijakan Privasi Jaringan Lokal untuk macOS Sequoia

macOS Sequoia (versi 15) memiliki fitur Privasi Jaringan Lokal baru yang memengaruhi pengguna layanan berbasis IP lokal, termasuk Layanan Metadata Instans Amazon EC2 (IMDS).

> **Important**
>
> Untuk memastikan bahwa Anda memiliki akses tanpa gangguan ke layanan berbasis IP lokal, gunakan langkah-langkah berikut untuk menyetujui kebijakan Privasi Jaringan Lokal.

Untuk menyetujui Kebijakan Privasi Jaringan Lokal

1. Hubungkan ke antarmuka pengguna grafis (GUI) instans Anda.

2. Ikuti petunjuk di layar untuk menyetujui kebijakan Privasi Jaringan Lokal.
3. Setelah menyetujui kebijakan tersebut, buat AMI instans EC2 Mac Anda. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.

Setiap instans EC2 Mac yang diluncurkan dari AMI yang baru dibuat akan mempertahankan izin Privasi Jaringan Lokal.

Paket default disertakan dalam Amazon EC2 macOS AMIs

Tabel berikut menjelaskan paket yang disertakan secara default di macOS AMIs EC2.

Paket	Catatan rilis
EC2macOS Init	https://github.com/aws/ec2-macos-init/tags
EC2macOS Utils	https://github.com/aws/ec2-macos-utils/tags
AmazonAgen SSM	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) versi 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Alat Baris Perintah untuk Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2 Instance Connect	https://github.com/aws/aws-ec2-instance-connect-config/releases
Safari	https://developer.apple.com/documentation/safari-release-notes

Pembaruan macOS AMI Amazon EC2

Tabel berikut menjelaskan perubahan yang disertakan dalam rilis macOS AMI EC2. Perhatikan bahwa beberapa perubahan berlaku untuk semua AMIs macOS EC2, sedangkan yang lain hanya berlaku untuk sebagian dari ini. AMIs

Pembaruan macOS AMI EC2

Rilis	Perubahan
2026.03.17	Rilis macOS Tahoe 26.3.1 • Apa yang baru dalam pembaruan untuk macOS Tahoe 26 • Alat Baris Perintah yang Diperbarui ke 26.3 • Diperbarui `awscli` ke 2.34.10 • Diperbarui Homebrew ke 5.1.0

2026.03.03	Semua AMIs
	• Diperbarui `awscli` ke 2.33.31
	• Diperbarui Homebrew ke 5.0.15
	
	Rilis macOS Sonoma 14.8.4
	• Konten keamanan macOS Sonoma 14.8.4
	• Diperbarui Safari ke 26.3
	  • Konten keamanan Safari 26.3
	
	Rilis macOS Sequoia 15.7.4
	• Konten keamanan macOS Sequoia 15.7.4
	• Diperbarui Safari ke 26.3
	  • Konten keamanan Safari 26.3
	
	Rilis macOS Tahoe 26.3
	• Konten keamanan macOS Tahoe 26.3

2025.12.26	Semua AMIs • Diperbarui `awscli` ke 2.32.19 • Diperbarui `amazon-ssm-agent` ke 3.3.3270.0

Rilis	Perubahan

	• Diperbarui Homebrew ke 5.0.6
	
	Rilis macOS Sonoma 14.8.3
	
	• Konten keamanan macOS Sonoma 14.8.3
	• Diperbarui Safari ke 26.2
	  • Konten keamanan Safari 26.2
	
	Rilis macOS Sequoia 15.7.3
	
	• Konten keamanan macOS Sequoia 15.7.3
	• Diperbarui Safari ke 26.2
	  • Konten keamanan Safari 26.2
	• Alat Baris Perintah yang Diperbarui menjadi 26.2
	
	Rilis macOS Tahoe 26.2
	
	• Konten keamanan macOS Tahoe 26.2
	• Alat Baris Perintah yang Diperbarui menjadi 26.2

Rilis	Perubahan

2025.12.17	Semua AMIs
	• Diperbarui `awscli` ke 2.32.16
	• Diperbarui Homebrew ke 5.0.5
	
	Rilis macOS Sonoma 14.8.2
	• Konten keamanan macOS Sonoma 14.8.2
	• Diperbarui Safari ke 26.1
	  • Konten keamanan Safari 26.1
	
	Rilis macOS Sequoia 15.7.2
	• Konten keamanan macOS Sequoia 15.7.2
	• Diperbarui Safari ke 26.1
	  • Konten keamanan Safari 26.1
	• Alat Baris Perintah yang Diperbarui ke 26.1
	
	Rilis macOS Tahoe 26.1
	• Konten keamanan macOS Tahoe 26.1
	• Alat Baris Perintah yang Diperbarui ke 26.1

Rilis	Perubahan

2025.11.18	Semua AMIs
	
	• Diperbarui `awscli` ke 2.31.35
	• Diperbarui `ec2-macos-init` ke 1.5.13
	• Diperbarui `ec2-macos-utils` ke 1.0.7
	• Diperbarui Homebrew ke 5.0.1
	
	Rilis macOS Sonoma 14.8.1
	
	• Konten keamanan macOS Sonoma 14.8.1
	• Diperbarui Safari ke 26.0.1
	  • Konten keamanan Safari 26.0.1
	
	Rilis macOS Sequoia 15.7.1
	
	• Konten keamanan macOS Sequoia 15.7.1
	• Diperbarui Safari ke 26.0.1
	  • Konten keamanan Safari 18.6
	• Alat Baris Perintah yang Diperbarui ke 26.0
	
	Rilis macOS Tahoe 26.0.1
	
	• Konten keamanan macOS Tahoe 26.0.1
	• Alat Baris Perintah yang Diperbarui ke 26.0

Rilis	Perubahan
2025.09.04	Semua AMIs • Diperbarui `awscli` ke 2.28.19 • Diperbarui `ec2-instance-connect` ke 2.0.0-5 • Diperbarui Homebrew ke 4.6.7 Rilis macOS Ventura 13.7.8 • Konten keamanan macOS Ventura 13.7.8 Rilis macOS Sonoma 14.7.8 • Konten keamanan macOS Sonoma 14.7.8 Rilis macOS Sequoia 15.6.1 • Konten keamanan macOS Sequoia 15.6.1

Rilis	Perubahan

2025.08.05	Semua AMIs
	• Diperbarui `awscli` ke 2.28.0
	• Diperbarui Homebrew ke 4.5.13
	
	Rilis macOS Ventura 13.7.7
	• Konten keamanan macOS Ventura 13.7.7
	• Diperbarui Safari ke 18.6
	  • Konten keamanan Safari 18.6
	
	Rilis macOS Sonoma 14.7.7
	• Konten keamanan macOS Sonoma 14.7.7
	• Diperbarui Safari ke 18.6
	  • Konten keamanan Safari 18.6
	
	Rilis macOS Sequoia 15.6
	• Konten keamanan macOS Sequoia 15.6
	• Diperbarui AWS ENA Ethernet ke 2.0.0

Rilis	Perubahan

2025.06.27	Semua AMIs
	• Diperbarui `awscli` ke 2.27.40
	• Diperbarui Homebrew ke 4.5.7
	• Gambar x86_64 yang dimigrasi ke ENA Ethernet dext AWS
	
	Rilis macOS Ventura 13.7.6
	• Konten keamanan macOS Ventura 13.7.6
	• Diperbarui Safari ke 18,5
	  • Konten keamanan Safari 18.5
	
	Rilis macOS Sonoma 14.7.6
	• Konten keamanan macOS Sonoma 14.7.6
	• Diperbarui Safari ke 18,5
	  • Konten keamanan Safari 18.5
	
	Rilis macOS Sequoia 15.5
	• Konten keamanan macOS Sequoia 15.5
	• Alat Baris Perintah yang Diperbarui ke 16.4
	• Diperbarui AWS ENA Ethernet ke 1.0.9

Rilis	Perubahan

2025.05.21	Semua AMIs
	
	• Diperbarui `awscli` ke 2.27.7
	• Diperbarui `ec2-macos-init` ke 1.5.11
	• Diperbarui `ec2-macos-utils` ke 1.0.5
	• Diperbarui Homebrew ke 4.5.1
	
	Rilis macOS Ventura 13.7.5
	
	• Konten keamanan macOS Ventura 13.7.5
	• Diperbarui Safari ke 18.4
	  • Konten keamanan Safari 18.4
	
	Rilis macOS Sonoma 14.7.5
	
	• Konten keamanan macOS Sonoma 14.7.5
	• Diperbarui Safari ke 18.4
	  • Konten keamanan Safari 18.4
	
	Rilis macOS Sequoia 15.4.1
	
	• Konten keamanan macOS Sequoia 15.4.1
	• Alat Baris Perintah yang Diperbarui ke 16.3

Rilis	Perubahan

2025.05.05	Semua AMIs
	• Diperbarui `awscli` ke 2.27.1
	• Diperbarui `ec2-macos-init` ke 1.5.11
	• Diperbarui `ec2-macos-system-monitor` ke 1.3.1
	• Diperbarui `ec2-macos-utils` ke 1.0.5
	• Diperbarui Homebrew ke 4.4.32
	
	Rilis macOS Ventura 13.7.5
	• Konten keamanan macOS Ventura 13.7.5
	• Diperbarui Safari ke 18.4
	  • Konten keamanan Safari 18.4
	
	Rilis macOS Sonoma 14.7.5
	• Konten keamanan macOS Sonoma 14.7.5
	• Diperbarui Safari ke 18.4
	  • Konten keamanan Safari 18.4
	
	Rilis macOS Sequoia 15.4.1
	• Konten keamanan macOS Sequoia 15.4.1

Rilis	Perubahan
2025.03.18	Semua AMIs • Diperbarui `awscli` ke 2.24.2 • Diperbarui Homebrew ke 4.4.20 Rilis macOS Sequoia 15.3.1 • Konten keamanan macOS Sequoia 15.3.1 Rilis macOS Sonoma 14.7.4 • Konten keamanan macOS Sonoma 14.7.4 • Diperbarui Safari ke 18.3 Rilis macOS Ventura 13.7.4 • Konten keamanan macOS Ventura 13.7.4 • Diperbarui Safari ke 18.3

Rilis	Perubahan
2025.01.24	Semua AMIs • Diperbarui `awscli` ke 2.22.33 • Diperbarui Homebrew ke 4.4.15 Rilis macOS Sequoia 15.2 • Konten keamanan macOS Sequoia 15.2 • Alat Baris Perintah yang Diperbarui ke 16.2 Rilis macOS Sonoma 14.7.2 • Konten keamanan macOS Sonoma 14.7.2 • Diperbarui Safari ke 18.2 • Alat Baris Perintah yang Diperbarui ke 16.2 Rilis macOS Ventura 13.7.2 • Konten keamanan macOS Ventura 13.7.2 • Diperbarui Safari ke 18.2

Rilis	Perubahan
2024.12.20	Semua AMIs • Diperbarui Homebrew ke 4.4.8 • Diperbarui `aws-cli` ke 2.22.5 • Diperbarui `amazon-ssm-agent` ke 3.3.987.0 Rilis macOS Sequoia 15.1.1 • Konten keamanan macOS Sequoia 15.1.1 Rilis macOS Sonoma 14.7.1 • Konten keamanan macOS Sonoma 14.7.1 • Diperbarui Safari ke 18.1.1 Rilis macOS Ventura 13.7.1 • Konten keamanan macOS Ventura 13.7.1 • Diperbarui Safari ke 18.1.1

Rilis	Perubahan

2024.10.28	Semua AMIs
	• Diperbarui Homebrew ke 4.4.2
	• Diperbarui `aws-cli` ke 2.18.13
	• Diperbarui `amazon-ssm-agent` ke 3.3.987.0
	• Diperbarui `ec2-macos-init` ke 1.5.10
	• Diperbarui `ec2-macos-utils` ke 1.0.4
	
	Rilis macOS Sequoia 15.0
	• Konten keamanan macOS Sequoia 15
	
	Rilis macOS Sonoma 14.7
	• Konten keamanan macOS Sonoma 14.7.
	• Alat Baris Perintah yang Diperbarui ke 16.0
	• Diperbarui Safari ke 18.0.1
	  • Konten keamanan Safari 18
	
	Rilis macOS Ventura 13.7
	• Konten keamanan macOS Ventura 13.7
	• Diperbarui Safari ke 18.0.1
	  • Konten keamanan Safari 18

Rilis	Perubahan

2024.08.20	Semua AMIs
	• Diperbarui Homebrew ke 4.3.14
	• Diperbarui `aws-cli` ke 2.17.29
	
	Rilis macOS Sonoma 14.6.1
	• Tidak ada entri CVE yang diterbitkan.
	
	Rilis macOS Ventura 13.6.9
	• Tidak ada entri CVE yang diterbitkan.
	• Diperbarui Safari ke 17.6
	  • Konten keamanan Safari 17.6
	
	Rilis macOS Monterey 12.7.6
	• Konten keamanan macOS Monterey 12.7.6
	• Diperbarui Safari ke 17.6
	  • Konten keamanan Safari 17.6

Rilis	Perubahan

2024.06.07	Semua AMIs
	• Diperbarui Homebrew ke 4.3.1-1
	• Diperbarui `aws-cli` ke 2.15.56
	• Diperbarui `amazon-ssm-agent` ke 3.3.380.0-1
	
	Rilis macOS Sonoma 14.5
	• Konten keamanan macOS Sonoma 14.5
	
	Rilis macOS Ventura 13.6.7
	• Konten keamanan macOS Ventura 13.6.7
	• Diperbarui Safari ke 17.5
	  • Konten keamanan Safari 17.5
	
	Rilis macOS Monterey 12.7.5
	• Konten keamanan macOS Monterey 12.7.5
	• Diperbarui Safari ke 17.5
	  • Konten keamanan Safari 17.5

Rilis	Perubahan

2024.04.12	Semua AMIs
	• Diperbarui Homebrew ke 4.2.16-1
	• Diperbarui `aws-cli` ke 2.15.36
	
	Rilis macOS Sonoma 14.4.1
	• Konten keamanan macOS Sonoma 14.4.1
	
	Rilis macOS Ventura 13.6.6
	• Konten keamanan macOS Ventura 13.6.6
	• Diperbarui Safari ke 17.4.1
	  • Konten keamanan Safari 17.4.1
	
	Untuk macOS Monterey
	• Diperbarui Safari ke 17.4.1
	  • Konten keamanan Safari 17.4.1

Jenis instans Amazon EBS yang dioptimalkan

Instans Amazon EBS yang dioptimalkan menggunakan tumpukan konfigurasi yang dioptimalkan dan menyediakan bandwidth tambahan khusus untuk Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O dan lalu lintas lainnya dari instans Anda.

Ketika dilampirkan ke instans yang dioptimalkan EBS, volume General Purpose SSD (`gp2`dan`gp3`) dirancang untuk memberikan setidaknya 90 persen dari kinerja IOPS yang disediakan 99 persen dari waktu pada tahun tertentu, dan volume SSD (`io1`dan`io2`) IOPS Provisioned dirancang untuk memberikan setidaknya 90 persen dari kinerja IOPS yang disediakan 99,9 persen dari waktu pada tahun tertentu. Throughput Optimized HDD (`st1`) dan Cold HDD (`sc1`) memberikan setidaknya 90 persen dari kinerja throughput yang diharapkan 99 persen dari waktu pada tahun tertentu. Periode yang tidak dipatuhi kurang lebih didistribusikan secara seragam, menargetkan 99 persen total

throughput yang diharapkan setiap jam. Untuk informasi selengkapnya, lihat Jenis volume Amazon EBS di Panduan Pengguna Amazon EBS.

Beberapa jenis instance dioptimalkan EBS secara default, dan tidak perlu mengaktifkannya dan tidak berpengaruh jika Anda mencoba menonaktifkannya. Jenis instans lain secara opsional mendukung pengoptimalan EBS dan Anda dapat mengaktifkannya selama atau setelah peluncuran dengan biaya tambahan per jam. Beberapa tipe instance tidak mendukung optimasi EBS.

Untuk spesifikasi dan fitur tipe instans terperinci, lihat Panduan Jenis Instans Amazon EC2.

Pertimbangan-pertimbangan

- Kinerja EBS instans dibatasi oleh batas kinerja tipe instans, atau kinerja agregat dari volume terlampirnya, mana yang lebih kecil. Untuk mencapai performa EBS maksimum, instans harus memiliki volume terlampir yang memberikan performa gabungan yang sama atau lebih besar dari performa instans maksimum. Misalnya, untuk mencapai `80,000` IOPS`r6i.16xlarge`, instance harus memiliki setidaknya `5` `gp2` volume yang disediakan dengan `16,000` IOPS masing-masing (5volume x IOPS = `16,000` IOPS), atau volume dapat disediakan dengan `80,000` IOPS. `1` `gp3` `80,000` Kami menyarankan Anda memilih jenis instans yang menyediakan throughput Amazon EBS yang lebih berdedikasi daripada kebutuhan aplikasi Anda; jika tidak, koneksi antara Amazon EBS dan Amazon EC2 dapat menjadi hambatan kinerja.
- Jumlah maksimum volume Amazon EBS yang dapat dilampirkan ke instans bergantung pada tipe instans dan ukuran instans. Untuk informasi selengkapnya, lihat Batas volume Amazon EBS untuk instans Amazon EC2.
- IOPS maksimum dan batas throughput saling bergantung. Tergantung pada I/O ukuran Anda, Anda mungkin mencapai satu batas sebelum yang lain, yang dapat memengaruhi kinerja secara keseluruhan. Untuk hasil yang optimal, pertimbangkan kedua batasan saat merencanakan beban kerja Anda.

EBS dioptimalkan secara default

Jenis contoh berikut adalah EB—dioptimalkan secara default. Tidak perlu mengaktifkan optimisasi EBS dan tidak akan ada pengaruh jika Anda menonaktifkan optimasi EBS.

Contoh

- Tujuan umum
- Komputasi yang dioptimalkan

- Memori yang dioptimalkan
- Penyimpanan yang dioptimalkan
- Komputasi yang dipercepat
- Komputasi performa tinggi

Tujuan umum

> **Note**
>
> Jenis instans M8a, M8g, M8gd, M8i, M8id, M8i-flex mendukung pembobotan bandwidth yang dapat dikonfigurasi. Dengan jenis instans ini, Anda dapat mengoptimalkan bandwidth instans untuk kinerja jaringan atau kinerja Amazon EBS. Tabel berikut menunjukkan kinerja bandwidth Amazon EBS default untuk jenis instans ini. Untuk informasi selengkapnya, lihat EC2 konfigurasi pembobotan bandwidth contoh.

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
a1.medium [1]	300	3500	37,50	437.50	2500	20000
a1.large [1]	525	3500	65.62	437.50	4000	20000
a1.xlarge [1]	800	3500	100.00	437.50	6000	20000
a1.2xlarge [1]	1750	3500	218.75	437.50	10000	20000
a1.4xlarge [2]	3500		437.5		20000	
a1.metal [2]	3500		437.5		20000	
m4.large [2]	450		56,25		3600	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m4.xlarge [2]	750		93,75		6000	
m4.2xlarge [2]	1000		125,0		8000	
m4.4xlarge [2]	2000		250.0		16000	
m4.10xlarge [2]	4000		500,0		32000	
m4.16xlarge [2]	10000		1250.0		65000	
m5.large [1]	650	4750	81,25	593,75	3600	18750
m5.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
m5.4xlarge [2]	4750		593,75		18750	
m5.8xlarge [2]	6800		850.0		30000	
m5.12xlarge [2]	9500		1187,5		40000	
m5.16xlarge [2]	13600		1700.0		60000	
m5.24xlarge [2]	19000		2375.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m5.metal [2]	19000		2375.0		80000	
m5a.large [1]	650	2880	81,25	360.00	3600	16000
m5a.xlarge [1]	1085	2880	135.62	360.00	6000	16000
m5a.2xlarge [1]	1580	2880	197.50	360.00	8333	16000
m5a.4xlarge [2]	2880		360.0		16000	
m5a.8xlarge [2]	4750		593,75		20000	
m5a.12xlarge [2]	6780		847.5		30000	
m5a.16xlarge [2]	9500		1187,5		40000	
m5a.24xlarge [2]	13750		1718.75		60000	
m5ad.large [1]	650	2880	81,25	360.00	3600	16000
m5ad.xlarge [1]	1085	2880	135.62	360.00	6000	16000
m5ad.2xlarge [1]	1580	2880	197.50	360.00	8333	16000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m5ad.4xlarge [2]	2880		360.0		16000	
m5ad.8xlarge [2]	4750		593,75		20000	
m5ad.12xlarge [2]	6780		847.5		30000	
m5ad.16xlarge [2]	9500		1187,5		40000	
m5ad.24xlarge [2]	13750		1718.75		60000	
m5d.large [1]	650	4750	81,25	593,75	3600	18750
m5d.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5d.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
m5d.4xlarge [2]	4750		593,75		18750	
m5d.8xlarge [2]	6800		850.0		30000	
m5d.12xlarge [2]	9500		1187,5		40000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m5d.16xlarge [2]	13600		1700.0		60000	
m5d.24xlarge [2]	19000		2375.0		80000	
m5d.metal [2]	19000		2375.0		80000	
m5dn.large [1]	650	4750	81,25	593,75	3600	18750
m5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5dn.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
m5dn.4xlarge [2]	4750		593,75		18750	
m5dn.8xlarge [2]	6800		850.0		30000	
m5dn.12xlarge [2]	9500		1187,5		40000	
m5dn.16xlarge [2]	13600		1700.0		60000	
m5dn.24xlarge [2]	19000		2375.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m5dn.metal [2]	19000		2375.0		80000	
m5n.large [1]	650	4750	81,25	593,75	3600	18750
m5n.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5n.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
m5n.4xlarge [2]	4750		593,75		18750	
m5n.8xlarge [2]	6800		850.0		30000	
m5n.12xlarge [2]	9500		1187,5		40000	
m5n.16xlarge [2]	13600		1700.0		60000	
m5n.24xlarge [2]	19000		2375.0		80000	
m5n.metal [2]	19000		2375.0		80000	
m5zn.large [1]	800	3170	100.00	396.25	3333	13333

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m5zn.xlarge [1]	1564	3170	195,50	396.25	6667	13333
m5zn.2xlarge [2]	3170		396.25		13333	
m5zn.3xlarge [2]	4750		593,75		20000	
m5zn.6xlarge [2]	9500		1187,5		40000	
m5zn.12xlarge [2]	19000		2375.0		80000	
m5zn.metal [2]	19000		2375.0		80000	
m6a.large [1]	650	10000	81,25	1250,00	3600	40000
m6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6a.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
m6a.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m6a.8xlarge [2]	10000		1250.0		40000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m6a.12xlarge [2]	15000		1875.0		60000	
m6a.16xlarge [2]	20000		2500.0		80000	
m6a.24xlarge [2]	30000		3750.0		120000	
m6a.32xlarge [2]	40000		5000.0		160000	
m6a.48xlarge [2]	40000		5000.0		240000	
m6a.metal [2]	40000		5000.0		240000	
m6g.medium [1]	315	4750	39,38	593,75	2500	20000
m6g.large [1]	630	4750	78.75	593,75	3600	20000
m6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
m6g.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
m6g.4xlarge [2]	4750		593,75		20000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m6g.8xlarge [2]	9500		1187,5		40000	
m6g.12xlarge [2]	14250		1781.25		50000	
m6g.16xlarge [2]	19000		2375.0		80000	
m6g.metal [2]	19000		2375.0		80000	
m6gd.medium [1]	315	4750	39,38	593,75	2500	20000
m6gd.large [1]	630	4750	78.75	593,75	3600	20000
m6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
m6gd.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
m6gd.4xlarge [2]	4750		593,75		20000	
m6gd.8xlarge [2]	9500		1187,5		40000	
m6gd.12xlarge [2]	14250		1781.25		50000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m6gd.16xlarge [2]	19000		2375.0		80000	
m6gd.metal [2]	19000		2375.0		80000	
m6i.large [1]	650	10000	81,25	1250,00	3600	40000
m6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6i.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
m6i.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m6i.8xlarge [2]	10000		1250.0		40000	
m6i.12xlarge [2]	15000		1875.0		60000	
m6i.16xlarge [2]	20000		2500.0		80000	
m6i.24xlarge [2]	30000		3750.0		120000	
m6i.32xlarge [2]	40000		5000.0		160000	
m6i.metal [2]	40000		5000.0		160000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m6id.large [1]	650	10000	81,25	1250,00	3600	40000
m6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6id.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
m6id.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m6id.8xlarge [2]	10000		1250.0		40000	
m6id.12xlarge [2]	15000		1875.0		60000	
m6id.16xlarge [2]	20000		2500.0		80000	
m6id.24xlarge [2]	30000		3750.0		120000	
m6id.32xlarge [2]	40000		5000.0		160000	
m6id.metal [2]	40000		5000.0		160000	
m6idn.large [1]	1562	25000	195.31	3125.00	6250	100000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m6idn.xlarge [1]	3125	25000	390.62	3125.00	12500	100000
m6idn.2xlarge [1]	6250	25000	781,25	3125.00	25000	100000
m6idn.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
m6idn.8xlarge [2]	25000		3125.0		100000	
m6idn.12xlarge [2]	37500		4687.5		150000	
m6idn.16xlarge [2]	50000		6250.0		200000	
m6idn.24xlarge [2]	75000		9375.0		300000	
m6idn.32xlarge [2]	100000		12500.0		400000	
m6idn.metal [2]	100000		12500.0		400000	
m6in.large [1]	1562	25000	195.31	3125.00	6250	100000
m6in.xlarge [1]	3125	25000	390.62	3125.00	12500	100000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m6in.2xlarge [1]	6250	25000	781,25	3125.00	25000	100000
m6in.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
m6in.8xlarge [2]	25000		3125.0		100000	
m6in.12xlarge [2]	37500		4687.5		150000	
m6in.16xlarge [2]	50000		6250.0		200000	
m6in.24xlarge [2]	75000		9375.0		300000	
m6in.32xlarge [2]	100000		12500.0		400000	
m6in.metal [2]	100000		12500.0		400000	
m7a.medium [1]	325	10000	40,62	1250,00	2500	40000
m7a.large [1]	650	10000	81,25	1250,00	3600	40000
m7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m7a.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
m7a.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m7a.8xlarge [2]	10000		1250.0		40000	
m7a.12xlarge [2]	15000		1875.0		60000	
m7a.16xlarge [2]	20000		2500.0		80000	
m7a.24xlarge [2]	30000		3750.0		120000	
m7a.32xlarge [2]	40000		5000.0		160000	
m7a.48xlarge [2]	40000		5000.0		240000	
m7a.metal-48xl [2]	40000		5000.0		240000	
m7g.medium [1]	315	10000	39,38	1250,00	2500	40000
m7g.large [1]	630	10000	78.75	1250,00	3600	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7g.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
m7g.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m7g.8xlarge [2]	10000		1250.0		40000	
m7g.12xlarge [2]	15000		1875.0		60000	
m7g.16xlarge [2]	20000		2500.0		80000	
m7g.metal [2]	20000		2500.0		80000	
m7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
m7gd.large [1]	630	10000	78.75	1250,00	3600	40000
m7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7gd.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m7gd.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m7gd.8xlarge [2]	10000		1250.0		40000	
m7gd.12xlarge [2]	15000		1875.0		60000	
m7gd.16xlarge [2]	20000		2500.0		80000	
m7gd.logam 2	20000		2500.0		80000	
m7i.large [1]	650	10000	81,25	1250,00	3600	40000
m7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7i.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
m7i.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m7i.8xlarge [2]	10000		1250.0		40000	
m7i.12xlarge [2]	15000		1875.0		60000	
m7i.16xlarge [2]	20000		2500.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m7i.24xlarge [2]	30000		3750.0		120000	
m7i.48xlarge [2]	40000		5000.0		240000	
m7i.metal-24xl [2]	30000		3750.0		120000	
m7i.metal-48xl [2]	40000		5000.0		240000	
m7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
m7i-flex.xlarge [1]	625	10000	78.12	1250,00	3600	40000
m7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7i-flex.4xlarge [1]	2500	10000	312.50	1250,00	12000	40000
m7i-flex.8xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m7i-flex.12xlarge 1	7500	15000	937,50	1875.00	30000	60000
m7i-flex.16xlarge 1	10000	20000	1250,00	2500.00	40000	80000
m8a.medium 1	325	10000	40,62	1250,00	2500	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m8a.large 1	650	10000	81,25	1250,00	3600	40000
m8a.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8a.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
m8a.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
m8a.8xlarge 2	10000		1250.0		40000	
m8a.12xlarge 2	15000		1875.0		60000	
m8a.16xlarge 2	20000		2500.0		80000	
m8a.24xlarge 2	30000		3750.0		120000	
m8a.48xlarge 2	60000		7500.0		240000	
m8a.logam -24xl 2	30000		3750.0		120000	
m8a.logam -48xl 2	60000		7500.0		240000	
m8azn.medium 1	625	15000	78.12	1875.00	2500	60000
m8azn.large 1	1250	15000	156,25	1875.00	5000	60000
m8azn.xlarge 1	2500	15000	312.50	1875.00	10000	60000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m8azn.3xlarge 1	7500	15000	937,50	1875.00	30000	60000
m8azn.6xlarge 2	15000		1875.0		60000	
m8azn.12x large 2	30000		3750.0		120000	
m8azn.24x large 2	60000		7500.0		240000	
m8azn.met al-12xl 2	30000		3750.0		120000	
m8azn.met al-24xl 2	60000		7500.0		240000	
m8g.medium 1	315	10000	39,38	1250,00	2500	40000
m8g.large 1	630	10000	78.75	1250,00	3600	40000
m8g.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8g.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
m8g.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
m8g.8xlarge 2	10000		1250.0		40000	
m8g.12xlarge 2	15000		1875.0		60000	
m8g.16xlarge 2	20000		2500.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m8g.24xlarge 2	30000		3750.0		120000	
m8g.48xlarge 2	40000		5000.0		240000	
m8g.logam -24xl 2	30000		3750.0		120000	
m8g.logam -48xl 2	40000		5000.0		240000	
m8gb.sedang 1	1562	25000	195.31	3125.00	7500	120000
m8gb.large 1	3125	25000	390.62	3125.00	15000	120000
m8gb.xlarge 1	6250	25000	781,25	3125.00	30000	120000
m8gb.2xlarge 1	12500	25000	1562.50	3125.00	60000	120000
m8gb.4xlarge 2	25000		3125.0		120000	
m8gb.8xlarge 2	50000		6250.0		240000	
m8gb.12xlarge 2	75000		9375.0		360000	
m8gb.16xlarge 2	100000		12500.0		480000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m8gb.24xlarge 2	150000		18750,0		720000	
m8gb.48xlarge 2	300000		37500.0		1440000	
m8gb.logam-24xl 2	150000		18750,0		720000	
m8gb.logam-48xl 2	300000		37500.0		1440000	
m8gd.medium 1	315	10000	39,38	1250,00	2500	40000
m8gd.large 1	630	10000	78.75	1250,00	3600	40000
m8gd.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8gd.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
m8gd.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
m8gd.8xlarge 2	10000		1250.0		40000	
m8gd.12xlarge 2	15000		1875.0		60000	
m8gd.16xlarge 2	20000		2500.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m8gd.24xlarge 2	30000		3750.0		120000	
m8gd.48xlarge 2	40000		5000.0		240000	
m8gd.metal-24xl 2	30000		3750.0		120000	
m8gd.metal-48xl 2	40000		5000.0		240000	
m8gn.sedang 1	760	10000	95.00	1250,00	2500	40000
m8gn.large 1	1250	10000	156,25	1250,00	5000	40000
m8gn.xlarge 1	2500	10000	312.50	1250,00	10000	40000
m8gn.2xlarge 1	5000	10000	625.00	1250,00	20000	40000
m8gn.4xlarge 2	10000		1250.0		40000	
m8gn.8xlarge 2	20000		2500.0		80000	
m8gn.12xlarge 2	30000		3750.0		120000	
m8gn.16xlarge 2	40000		5000.0		160000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m8gn.24xlarge 2	60000		7500.0		240000	
m8gn.48xlarge 2	60000		7500.0		240000	
m8gn.metal-24xl 2	60000		7500.0		240000	
m8gn.metal-48xl 2	60000		7500.0		240000	
m8i.large 1	650	10000	81,25	1250,00	3600	40000
m8i.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8i.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
m8i.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
m8i.8xlarge 2	10000		1250.0		40000	
m8i.12xlarge 2	15000		1875.0		60000	
m8i.16xlarge 2	20000		2500.0		80000	
m8i.24xlarge 2	30000		3750.0		120000	
m8i.32xlarge 2	40000		5000.0		160000	
m8i.48xlarge 2	60000		7500.0		240000	
m8i.96xlarge 2	80000		10000.0		480000	
m8i.logam-48xl 2	60000		7500.0		240000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m8i.logam-96xl 2	80000		10000.0		480000	
m8id.large 1	650	10000	81,25	1250,00	3600	40000
m8id.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8id.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
m8id.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
m8id.8xlarge 2	10000		1250.0		40000	
m8id.12xlarge 2	15000		1875.0		60000	
m8id.16xlarge 2	20000		2500.0		80000	
m8id.24xlarge 2	30000		3750.0		120000	
m8id.32xlarge 2	40000		5000.0		160000	
m8id.48xlarge 2	60000		7500.0		240000	
m8id.96xlarge 2	80000		10000.0		480000	
m8id.metal-48xl 2	60000		7500.0		240000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
m8id.metal-96xl [2]	80000		10000.0		480000	
m8i-flex.large [1]	315	10000	39,38	1250,00	2500	40000
m8i-flex.xlarge [1]	630	10000	78.75	1250,00	3600	40000
m8i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m8i-flex.4xlarge [1]	2500	10000	312.50	1250,00	12000	40000
m8i-flex.8xlarge [1]	5000	10000	625.00	1250,00	20000	40000
m8i-flex.12xlarge [1]	7500	15000	937,50	1875.00	30000	60000
m8i-flex.16xlarge [1]	10000	20000	1250,00	2500.00	40000	80000
mac1.metal [2]	14000		1750.0		80000	
mac2.metal [2]	10000		1250.0		55000	
mac2-m1ultra.metal [2]	10000		1250.0		55000	
mac2-m2.metal [2]	8000		1000,0		55000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
mac2-m2pro.metal [2]	8000		1000,0		55000	
mac-m4.logam 2	8000		1000,0		55000	
mac-m4pro .logam 2	8000		1000,0		55000	
mac-m4max .logam 2	10000		1250.0		55000	
t3.nano [1]	43	2085	5.38	260.62	250	11800
t3.micro [1]	87	2085	10.88	260.62	500	11800
t3.small [1]	174	2085	21.75	260.62	1000	11800
t3.medium [1]	347	2085	43.38	260.62	2000	11800
t3.large [1]	695	2780	86.88	347,50	4000	15700
t3.xlarge [1]	695	2780	86.88	347,50	4000	15700
t3.2xlarge [1]	695	2780	86.88	347,50	4000	15700
t3a.nano [1]	45	2085	5.62	260.62	250	11800
t3a.micro [1]	90	2085	11.25	260.62	500	11800
t3a.small [1]	175	2085	21.88	260.62	1000	11800
t3a.medium [1]	350	2085	43,75	260.62	2000	11800

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
t3a.large [1]	695	2780	86.88	347,50	4000	15700
t3a.xlarge [1]	695	2780	86.88	347,50	4000	15700
t3a.2xlarge [1]	695	2780	86.88	347,50	4000	15700
t4g.nano [1]	43	2085	5.38	260.62	250	11800
t4g.micro [1]	87	2085	10.88	260.62	500	11800
t4g.small [1]	174	2085	21.75	260.62	1000	11800
t4g.medium [1]	347	2085	43.38	260.62	2000	11800
t4g.large [1]	695	2780	86.88	347,50	4000	15700
t4g.xlarge [1]	695	2780	86.88	347,50	4000	15700
t4g.2xlarge [1]	695	2780	86.88	347,50	4000	15700

[1] Contoh ini dapat mempertahankan kinerja maksimum selama 30 menit setidaknya sekali setiap 24 jam, setelah itu mereka kembali ke kinerja dasar mereka.

[2] Instans ini dapat mempertahankan performa yang dinyatakan tanpa batas waktu. Jika beban kerja Anda memerlukan performa maksimum yang berkelanjutan selama lebih dari 30 menit, gunakan salah satu instans ini.

Komputasi yang dioptimalkan

> **Note**
>
> Jenis instans C8a, C8g, C8gd, C8i, C8id, C8i-flex mendukung pembobotan bandwidth yang dapat dikonfigurasi. Dengan jenis instans ini, Anda dapat mengoptimalkan bandwidth instans untuk kinerja jaringan atau kinerja Amazon EBS. Tabel berikut menunjukkan kinerja bandwidth Amazon EBS default untuk jenis instans ini. Untuk informasi selengkapnya, lihat EC2 konfigurasi pembobotan bandwidth contoh.

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c4.large [2]	500		62.5		4000	
c4.xlarge [2]	750		93,75		6000	
c4.2xlarge [2]	1000		125,0		8000	
c4.4xlarge [2]	2000		250.0		16000	
c4.8xlarge [2]	4000		500,0		32000	
c5.large [1]	650	4750	81,25	593,75	4000	20000
c5.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5.2xlarge [1]	2300	4750	287.50	593,75	10000	20000
c5.4xlarge [2]	4750		593,75		20000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c5.9xlarge [2]	9500		1187,5		40000	
c5.12xlarge [2]	9500		1187,5		40000	
c5.18xlarge [2]	19000		2375.0		80000	
c5.24xlarge [2]	19000		2375.0		80000	
c5.metal [2]	19000		2375.0		80000	
c5a.large [1]	200	3170	25.00	396.25	800	13300
c5a.xlarge [1]	400	3170	50,00	396.25	1600	13300
c5a.2xlarge [1]	800	3170	100.00	396.25	3200	13300
c5a.4xlarge [1]	1580	3170	197.50	396.25	6600	13300
c5a.8xlarge [2]	3170		396.25		13300	
c5a.12xlarge [2]	4750		593,75		20000	
c5a.16xlarge [2]	6300		787.5		26700	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c5a.24xlarge [2]	9500		1187,5		40000	
c5ad.large [1]	200	3170	25.00	396.25	800	13300
c5ad.xlarge [1]	400	3170	50,00	396.25	1600	13300
c5ad.2xlarge [1]	800	3170	100.00	396.25	3200	13300
c5ad.4xlarge [1]	1580	3170	197.50	396.25	6600	13300
c5ad.8xlarge [2]	3170		396.25		13300	
c5ad.12xlarge [2]	4750		593,75		20000	
c5ad.16xlarge [2]	6300		787.5		26700	
c5ad.24xlarge [2]	9500		1187,5		40000	
c5d.large [1]	650	4750	81,25	593,75	4000	20000
c5d.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5d.2xlarge [1]	2300	4750	287.50	593,75	10000	20000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c5d.4xlarge [2]	4750		593,75		20000	
c5d.9xlarge [2]	9500		1187,5		40000	
c5d.12xlarge [2]	9500		1187,5		40000	
c5d.18xlarge [2]	19000		2375.0		80000	
c5d.24xlarge [2]	19000		2375.0		80000	
c5d.metal [2]	19000		2375.0		80000	
c5n.large [1]	650	4750	81,25	593,75	4000	20000
c5n.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5n.2xlarge [1]	2300	4750	287.50	593,75	10000	20000
c5n.4xlarge [2]	4750		593,75		20000	
c5n.9xlarge [2]	9500		1187,5		40000	
c5n.18xlarge [2]	19000		2375.0		80000	
c5n.metal [2]	19000		2375.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c6a.large [1]	650	10000	81,25	1250,00	3600	40000
c6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6a.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
c6a.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
c6a.8xlarge [2]	10000		1250.0		40000	
c6a.12xlarge [2]	15000		1875.0		60000	
c6a.16xlarge [2]	20000		2500.0		80000	
c6a.24xlarge [2]	30000		3750.0		120000	
c6a.32xlarge [2]	40000		5000.0		160000	
c6a.48xlarge [2]	40000		5000.0		240000	
c6a.metal [2]	40000		5000.0		240000	
c6g.medium [1]	315	4750	39,38	593,75	2500	20000
c6g.large [1]	630	4750	78.75	593,75	3600	20000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
c6g.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
c6g.4xlarge [2]	4750		593,75		20000	
c6g.8xlarge [2]	9500		1187,5		40000	
c6g.12xlarge [2]	14250		1781.25		50000	
c6g.16xlarge [2]	19000		2375.0		80000	
c6g.metal [2]	19000		2375.0		80000	
c6gd.medium [1]	315	4750	39,38	593,75	2500	20000
c6gd.large [1]	630	4750	78.75	593,75	3600	20000
c6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
c6gd.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
c6gd.4xlarge [2]	4750		593,75		20000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c6gd.8xlarge [2]	9500		1187,5		40000	
c6gd.12xlarge [2]	14250		1781.25		50000	
c6gd.16xlarge [2]	19000		2375.0		80000	
c6gd.metal [2]	19000		2375.0		80000	
c6gn.medium [1]	760	9500	95.00	1187,50	2500	40000
c6gn.large [1]	1235	9500	154,38	1187,50	5000	40000
c6gn.xlarge [1]	2375	9500	296.88	1187,50	10000	40000
c6gn.2xlarge [1]	4750	9500	593,75	1187,50	20000	40000
c6gn.4xlarge [2]	9500		1187,5		40000	
c6gn.8xlarge [2]	19000		2375.0		80000	
c6gn.12xlarge [2]	28500		3562.5		120000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c6gn.16xlarge [2]	38000		4750,0		160000	
c6i.large [1]	650	10000	81,25	1250,00	3600	40000
c6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6i.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
c6i.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
c6i.8xlarge [2]	10000		1250.0		40000	
c6i.12xlarge [2]	15000		1875.0		60000	
c6i.16xlarge [2]	20000		2500.0		80000	
c6i.24xlarge [2]	30000		3750.0		120000	
c6i.32xlarge [2]	40000		5000.0		160000	
c6i.metal [2]	40000		5000.0		160000	
c6id.large [1]	650	10000	81,25	1250,00	3600	40000
c6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c6id.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
c6id.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
c6id.8xlarge [2]	10000		1250.0		40000	
c6id.12xlarge [2]	15000		1875.0		60000	
c6id.16xlarge [2]	20000		2500.0		80000	
c6id.24xlarge [2]	30000		3750.0		120000	
c6id.32xlarge [2]	40000		5000.0		160000	
c6id.metal [2]	40000		5000.0		160000	
c6in.large [1]	1562	25000	195.31	3125.00	6250	100000
c6in.xlarge [1]	3125	25000	390.62	3125.00	12500	100000
c6in.2xlarge [1]	6250	25000	781,25	3125.00	25000	100000
c6in.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c6in.8xlarge [2]	25000		3125.0		100000	
c6in.12xlarge [2]	37500		4687.5		150000	
c6in.16xlarge [2]	50000		6250.0		200000	
c6in.24xlarge [2]	75000		9375.0		300000	
c6in.32xlarge [2]	100000		12500.0		400000	
c6in.metal [2]	100000		12500.0		400000	
c7a.medium [1]	325	10000	40,62	1250,00	2500	40000
c7a.large [1]	650	10000	81,25	1250,00	3600	40000
c7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7a.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
c7a.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
c7a.8xlarge [2]	10000		1250.0		40000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c7a.12xlarge [2]	15000		1875.0		60000	
c7a.16xlarge [2]	20000		2500.0		80000	
c7a.24xlarge [2]	30000		3750.0		120000	
c7a.32xlarge [2]	40000		5000.0		160000	
c7a.48xlarge [2]	40000		5000.0		240000	
c7a.metal-48xl [2]	40000		5000.0		240000	
c7g.medium [1]	315	10000	39,38	1250,00	2500	40000
c7g.large [1]	630	10000	78.75	1250,00	3600	40000
c7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7g.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
c7g.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
c7g.8xlarge [2]	10000		1250.0		40000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c7g.12xlarge [2]	15000		1875.0		60000	
c7g.16xlarge [2]	20000		2500.0		80000	
c7g.metal [2]	20000		2500.0		80000	
c7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
c7gd.large [1]	630	10000	78.75	1250,00	3600	40000
c7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7gd.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
c7gd.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
c7gd.8xlarge [2]	10000		1250.0		40000	
c7gd.12xlarge [2]	15000		1875.0		60000	
c7gd.16xlarge [2]	20000		2500.0		80000	
c7gd.metal 2	20000		2500.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c7gn.medium [1]	521	10000	65.12	1250,00	2083	40000
c7gn.large [1]	1042	10000	130,25	1250,00	4167	40000
c7gn.xlarge [1]	2083	10000	260.38	1250,00	8333	40000
c7gn.2xlarge [1]	4167	10000	520.88	1250,00	16667	40000
c7gn.4xlarge [1]	8333	10000	1041.62	1250,00	33333	40000
c7gn.8xlarge [1]	16667	20000	2083.38	2500.00	66667	80000
c7gn.12xlarge [1]	25000	30000	3125.00	3750.00	100000	120000
c7gn.16xlarge [1]	33333	40000	4166.62	5000.00	133333	160000
c7gn.logam 1	33333	40000	4166.62	5000.00	133333	160000
c7i.large [1]	650	10000	81,25	1250,00	3600	40000
c7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7i.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
c7i.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c7i.8xlarge [2]	10000		1250.0		40000	
c7i.12xlarge [2]	15000		1875.0		60000	
c7i.16xlarge [2]	20000		2500.0		80000	
c7i.24xlarge [2]	30000		3750.0		120000	
c7i.48xlarge [2]	40000		5000.0		240000	
c7i.metal-24xl [2]	30000		3750.0		120000	
c7i.metal-48xl [2]	40000		5000.0		240000	
c7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
c7i-flex.xlarge [1]	625	10000	78.12	1250,00	3600	40000
c7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7i-flex.4xlarge [1]	2500	10000	312.50	1250,00	12000	40000
c7i-flex.8xlarge [1]	5000	10000	625.00	1250,00	20000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c7i-flex.12xlarge 1	7500	15000	937,50	1875.00	30000	60000
c7i-flex.16xlarge 1	10000	20000	1250,00	2500.00	40000	80000
c8a.medium 1	325	10000	40,62	1250,00	2500	40000
c8a.large 1	650	10000	81,25	1250,00	3600	40000
c8a.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8a.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
c8a.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
c8a.8xlarge 2	10000		1250.0		40000	
c8a.12xlarge 2	15000		1875.0		60000	
c8a.16xlarge 2	20000		2500.0		80000	
c8a.24xlarge 2	30000		3750.0		120000	
c8a.48xlarge 2	60000		7500.0		240000	
c8a.metal-24xl 2	30000		3750.0		120000	
c8a.metal-48xl 2	60000		7500.0		240000	
c8g.medium 1	315	10000	39,38	1250,00	2500	40000
c8g.large 1	630	10000	78.75	1250,00	3600	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c8g.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8g.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
c8g.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
c8g.8xlarge 2	10000		1250.0		40000	
c8g.12xlarge 2	15000		1875.0		60000	
c8g.16xlarge 2	20000		2500.0		80000	
c8g.24xlarge 2	30000		3750.0		120000	
c8g.48xlarge 2	40000		5000.0		240000	
c8g.logam-24xl 2	30000		3750.0		120000	
c8g.logam-48xl 2	40000		5000.0		240000	
c8gb.medium 1	1562	25000	195.31	3125.00	7500	120000
c8gb.large 1	3125	25000	390.62	3125.00	15000	120000
c8gb.xlarge 1	6250	25000	781,25	3125.00	30000	120000
c8gb.2xlarge 1	12500	25000	1562.50	3125.00	60000	120000
c8gb.4xlarge 2	25000		3125.0		120000	
c8gb.8xlarge 2	50000		6250.0		240000	
c8gb.12xlarge 2	75000		9375.0		360000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c8gb.16xlarge 2	100000		12500.0		480000	
c8gb.24xlarge 2	150000		18750,0		720000	
c8gb.48xlarge 2	300000		37500.0		1440000	
c8gb.metal-24xl 2	150000		18750,0		720000	
c8gb.metal-48xl 2	300000		37500.0		1440000	
c8gd.medium 1	315	10000	39,38	1250,00	2500	40000
c8gd.large 1	630	10000	78.75	1250,00	3600	40000
c8gd.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8gd.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
c8gd.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
c8gd.8xlarge 2	10000		1250.0		40000	
c8gd.12xlarge 2	15000		1875.0		60000	
c8gd.16xlarge 2	20000		2500.0		80000	
c8gd.24xlarge 2	30000		3750.0		120000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c8gd.48xlarge 2	40000		5000.0		240000	
c8gd.metal-24xl 2	30000		3750.0		120000	
c8gd.metal-48xl 2	40000		5000.0		240000	
c8gn.medium 1	760	10000	95.00	1250,00	2500	40000
c8gn.large 1	1250	10000	156,25	1250,00	5000	40000
c8gn.xlarge 1	2500	10000	312.50	1250,00	10000	40000
c8gn.2xlarge 1	5000	10000	625.00	1250,00	20000	40000
c8gn.4xlarge 2	10000		1250.0		40000	
c8gn.8xlarge 2	20000		2500.0		80000	
c8gn.12xlarge 2	30000		3750.0		120000	
c8gn.16xlarge 2	40000		5000.0		160000	
c8gn.24xlarge 2	60000		7500.0		240000	
c8gn.48xlarge 2	60000		7500.0		240000	
c8gn.metal-24xl 2	60000		7500.0		240000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c8gn.metal-48xl 2	60000		7500.0		240000	
c8i.large 1	650	10000	81,25	1250,00	3600	40000
c8i.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8i.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
c8i.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
c8i.8xlarge 2	10000		1250.0		40000	
c8i.12xlarge 2	15000		1875.0		60000	
c8i.16xlarge 2	20000		2500.0		80000	
c8i.24xlarge 2	30000		3750.0		120000	
c8i.32xlarge 2	40000		5000.0		160000	
c8i.48xlarge 2	60000		7500.0		240000	
c8i.96xlarge 2	80000		10000.0		480000	
c8i.logam-48xl 2	60000		7500.0		240000	
c8i.logam-96xl 2	80000		10000.0		480000	
c8id.large 1	650	10000	81,25	1250,00	3600	40000
c8id.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8id.2xlarge 1	2500	10000	312.50	1250,00	12000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c8id.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
c8id.8xlarge 2	10000		1250.0		40000	
c8id.12xlarge 2	15000		1875.0		60000	
c8id.16xlarge 2	20000		2500.0		80000	
c8id.24xlarge 2	30000		3750.0		120000	
c8id.32xlarge 2	40000		5000.0		160000	
c8id.48xlarge 2	60000		7500.0		240000	
c8id.96xlarge 2	80000		10000.0		480000	
c8id.metal-48xl 2	60000		7500.0		240000	
c8id.metal-96xl 2	80000		10000.0		480000	
c8i-flex.large 1	315	10000	39,38	1250,00	2500	40000
c8i-flex.xlarge 1	630	10000	78.75	1250,00	3600	40000
c8i-flex.2xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8i-flex.4xlarge 1	2500	10000	312.50	1250,00	12000	40000
c8i-flex.8xlarge 1	5000	10000	625.00	1250,00	20000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
c8i-flex.12xlarge 1	7500	15000	937,50	1875.00	30000	60000
c8i-flex.16xlarge 1	10000	20000	1250,00	2500.00	40000	80000

[1] Contoh ini dapat mempertahankan kinerja maksimum selama 30 menit setidaknya sekali setiap 24 jam, setelah itu mereka kembali ke kinerja dasar mereka.

[2] Instans ini dapat mempertahankan performa yang dinyatakan tanpa batas waktu. Jika beban kerja Anda memerlukan performa maksimum yang berkelanjutan selama lebih dari 30 menit, gunakan salah satu instans ini.

Memori yang dioptimalkan

> **Note**
>
> - Jenis instans R8a, R8g, R8gd, R8i, R8iD, R8i-flex, X8g, X8AEDZ, X8i mendukung bobot bandwidth yang dapat dikonfigurasi. Dengan jenis instans ini, Anda dapat mengoptimalkan bandwidth instans untuk kinerja jaringan atau kinerja Amazon EBS. Tabel berikut menunjukkan kinerja bandwidth Amazon EBS default untuk jenis instans ini. Untuk informasi selengkapnya, lihat EC2 konfigurasi pembobotan bandwidth contoh.
> - Untuk performa IOPS maksimum dengan instans U7i, sebaiknya gunakan volume io2. BlockExpress

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r4.large [2]	425		53.125		3000	
r4.xlarge [2]	850		106,25		6000	
r4.2xlarge [2]	1700		212.5		12000	
r4.4xlarge [2]	3500		437.5		18750	
r4.8xlarge [2]	7000		875.0		37500	
r4.16xlarge [2]	14000		1750.0		75000	
r5.large [1]	650	4750	81,25	593,75	3600	18750
r5.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
r5.4xlarge [2]	4750		593,75		18750	
r5.8xlarge [2]	6800		850.0		30000	
r5.12xlarge [2]	9500		1187,5		40000	
r5.16xlarge [2]	13600		1700.0		60000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r5.24xlarge [2]	19000		2375.0		80000	
r5.metal [2]	19000		2375.0		80000	
r5a.large [1]	650	2880	81,25	360.00	3600	16000
r5a.xlarge [1]	1085	2880	135.62	360.00	6000	16000
r5a.2xlarge [1]	1580	2880	197.50	360.00	8333	16000
r5a.4xlarge [2]	2880		360.0		16000	
r5a.8xlarge [2]	4750		593,75		20000	
r5a.12xlarge [2]	6780		847.5		30000	
r5a.16xlarge [2]	9500		1187,5		40000	
r5a.24xlarge [2]	13570		1696.25		60000	
r5ad.large [1]	650	2880	81,25	360.00	3600	16000
r5ad.xlarge [1]	1085	2880	135.62	360.00	6000	16000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r5ad.2xlarge [1]	1580	2880	197.50	360.00	8333	16000
r5ad.4xlarge [2]	2880		360.0		16000	
r5ad.8xlarge [2]	4750		593,75		20000	
r5ad.12xlarge [2]	6780		847.5		30000	
r5ad.16xlarge [2]	9500		1187,5		40000	
r5ad.24xlarge [2]	13570		1696.25		60000	
r5b.large [1]	1250	10000	156,25	1250,00	5417	43333
r5b.xlarge [1]	2500	10000	312.50	1250,00	10833	43333
r5b.2xlarge [1]	5000	10000	625.00	1250,00	21667	43333
r5b.4xlarge [2]	10000		1250.0		43333	
r5b.8xlarge [2]	20000		2500.0		86667	
r5b.12xlarge [2]	30000		3750.0		130000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r5b.16xlarge [2]	40000		5000.0		173333	
r5b.24xlarge [2]	60000		7500.0		260000	
r5b.metal [2]	60000		7500.0		260000	
r5d.large [1]	650	4750	81,25	593,75	3600	18750
r5d.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5d.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
r5d.4xlarge [2]	4750		593,75		18750	
r5d.8xlarge [2]	6800		850.0		30000	
r5d.12xlarge [2]	9500		1187,5		40000	
r5d.16xlarge [2]	13600		1700.0		60000	
r5d.24xlarge [2]	19000		2375.0		80000	
r5d.metal [2]	19000		2375.0		80000	
r5dn.large [1]	650	4750	81,25	593,75	3600	18750

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5dn.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
r5dn.4xlarge [2]	4750		593,75		18750	
r5dn.8xlarge [2]	6800		850.0		30000	
r5dn.12xlarge [2]	9500		1187,5		40000	
r5dn.16xlarge [2]	13600		1700.0		60000	
r5dn.24xlarge [2]	19000		2375.0		80000	
r5dn.metal [2]	19000		2375.0		80000	
r5n.large [1]	650	4750	81,25	593,75	3600	18750
r5n.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5n.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
r5n.4xlarge [2]	4750		593,75		18750	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r5n.8xlarge [2]	6800		850.0		30000	
r5n.12xlarge [2]	9500		1187,5		40000	
r5n.16xlarge [2]	13600		1700.0		60000	
r5n.24xlarge [2]	19000		2375.0		80000	
r5n.metal [2]	19000		2375.0		80000	
r6a.large [1]	650	10000	81,25	1250,00	3600	40000
r6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6a.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
r6a.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
r6a.8xlarge [2]	10000		1250.0		40000	
r6a.12xlarge [2]	15000		1875.0		60000	
r6a.16xlarge [2]	20000		2500.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r6a.24xlarge [2]	30000		3750.0		120000	
r6a.32xlarge [2]	40000		5000.0		160000	
r6a.48xlarge [2]	40000		5000.0		240000	
r6a.metal [2]	40000		5000.0		240000	
r6g.medium [1]	315	4750	39,38	593,75	2500	20000
r6g.large [1]	630	4750	78.75	593,75	3600	20000
r6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
r6g.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
r6g.4xlarge [2]	4750		593,75		20000	
r6g.8xlarge [2]	9500		1187,5		40000	
r6g.12xlarge [2]	14250		1781.25		50000	
r6g.16xlarge [2]	19000		2375.0		80000	
r6g.metal [2]	19000		2375.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r6gd.medium [1]	315	4750	39,38	593,75	2500	20000
r6gd.large [1]	630	4750	78.75	593,75	3600	20000
r6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
r6gd.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
r6gd.4xlarge [2]	4750		593,75		20000	
r6gd.8xlarge [2]	9500		1187,5		40000	
r6gd.12xlarge [2]	14250		1781.25		50000	
r6gd.16xlarge [2]	19000		2375.0		80000	
r6gd.metal [2]	19000		2375.0		80000	
r6i.large [1]	650	10000	81,25	1250,00	3600	40000
r6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6i.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r6i.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
r6i.8xlarge [2]	10000		1250.0		40000	
r6i.12xlarge [2]	15000		1875.0		60000	
r6i.16xlarge [2]	20000		2500.0		80000	
r6i.24xlarge [2]	30000		3750.0		120000	
r6i.32xlarge [2]	40000		5000.0		160000	
r6i.metal [2]	40000		5000.0		160000	
r6id.large [1]	650	10000	81,25	1250,00	3600	40000
r6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6id.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
r6id.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
r6id.8xlarge [2]	10000		1250.0		40000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r6id.12xlarge [2]	15000		1875.0		60000	
r6id.16xlarge [2]	20000		2500.0		80000	
r6id.24xlarge [2]	30000		3750.0		120000	
r6id.32xlarge [2]	40000		5000.0		160000	
r6id.metal [2]	40000		5000.0		160000	
r6idn.large [1]	1562	25000	195.31	3125.00	6250	100000
r6idn.xlarge [1]	3125	25000	390.62	3125.00	12500	100000
r6idn.2xlarge [1]	6250	25000	781,25	3125.00	25000	100000
r6idn.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
r6idn.8xlarge [2]	25000		3125.0		100000	
r6idn.12xlarge [2]	37500		4687.5		150000	
r6idn.16xlarge [2]	50000		6250.0		200000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r6idn.24xlarge [2]	75000		9375.0		300000	
r6idn.32xlarge [2]	100000		12500.0		400000	
r6idn.metal [2]	100000		12500.0		400000	
r6in.large [1]	1562	25000	195.31	3125.00	6250	100000
r6in.xlarge [1]	3125	25000	390.62	3125.00	12500	100000
r6in.2xlarge [1]	6250	25000	781,25	3125.00	25000	100000
r6in.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
r6in.8xlarge [2]	25000		3125.0		100000	
r6in.12xlarge [2]	37500		4687.5		150000	
r6in.16xlarge [2]	50000		6250.0		200000	
r6in.24xlarge [2]	75000		9375.0		300000	
r6in.32xlarge [2]	100000		12500.0		400000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r6in.metal [2]	100000		12500.0		400000	
r7a.medium [1]	325	10000	40,62	1250,00	2500	40000
r7a.large [1]	650	10000	81,25	1250,00	3600	40000
r7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7a.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
r7a.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
r7a.8xlarge [2]	10000		1250.0		40000	
r7a.12xlarge [2]	15000		1875.0		60000	
r7a.16xlarge [2]	20000		2500.0		80000	
r7a.24xlarge [2]	30000		3750.0		120000	
r7a.32xlarge [2]	40000		5000.0		160000	
r7a.48xlarge [2]	40000		5000.0		240000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r7a.metal-48xl [2]	40000		5000.0		240000	
r7g.medium [1]	315	10000	39,38	1250,00	2500	40000
r7g.large [1]	630	10000	78.75	1250,00	3600	40000
r7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7g.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
r7g.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
r7g.8xlarge [2]	10000		1250.0		40000	
r7g.12xlarge [2]	15000		1875.0		60000	
r7g.16xlarge [2]	20000		2500.0		80000	
r7g.metal [2]	20000		2500.0		80000	
r7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
r7gd.large [1]	630	10000	78.75	1250,00	3600	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7gd.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
r7gd.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
r7gd.8xlarge [2]	10000		1250.0		40000	
r7gd.12xlarge [2]	15000		1875.0		60000	
r7gd.16xlarge [2]	20000		2500.0		80000	
r7gd.logam 2	20000		2500.0		80000	
r7i.large [1]	650	10000	81,25	1250,00	3600	40000
r7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7i.2xlarge [1]	2500	10000	312.50	1250,00	12000	40000
r7i.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
r7i.8xlarge [2]	10000		1250.0		40000	
r7i.12xlarge [2]	15000		1875.0		60000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r7i.16xlarge [2]	20000		2500.0		80000	
r7i.24xlarge [2]	30000		3750.0		120000	
r7i.48xlarge [2]	40000		5000.0		240000	
r7i.metal-24xl [2]	30000		3750.0		120000	
r7i.metal-48xl [2]	40000		5000.0		240000	
r7iz.large [1]	792	10000	99.00	1250,00	3600	40000
r7iz.xlarge [1]	1584	10000	198.00	1250,00	6667	40000
r7iz.2xlarge [1]	3168	10000	396.00	1250,00	13333	40000
r7iz.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
r7iz.8xlarge [2]	10000		1250.0		40000	
r7iz.12xlarge [2]	19000		2375.0		76000	
r7iz.16xlarge [2]	20000		2500.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r7iz.32xlarge [2]	40000		5000.0		160000	
r7iz.metal-16xl [2]	20000		2500.0		80000	
r7iz.metal-32xl [2]	40000		5000.0		160000	
r8a.medium 1	325	10000	40,62	1250,00	2500	40000
r8a.large 1	650	10000	81,25	1250,00	3600	40000
r8a.xlarge 1	1250	10000	156,25	1250,00	6000	40000
r8a.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
r8a.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
r8a.8xlarge 2	10000		1250.0		40000	
r8a.12xlarge 2	15000		1875.0		60000	
r8a.16xlarge 2	20000		2500.0		80000	
r8a.24xlarge 2	30000		3750.0		120000	
r8a.48xlarge 2	60000		7500.0		240000	
r8a.metal-24xl 2	30000		3750.0		120000	
r8a.metal-48xl 2	60000		7500.0		240000	
r8g.sedang 1	315	10000	39,38	1250,00	2500	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r8g.large 1	630	10000	78.75	1250,00	3600	40000
r8g.xlarge 1	1250	10000	156,25	1250,00	6000	40000
r8g.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
r8g.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
r8g.8xlarge 2	10000		1250.0		40000	
r8g.12xlarge 2	15000		1875.0		60000	
r8g.16xlarge 2	20000		2500.0		80000	
r8g.24xlarge 2	30000		3750.0		120000	
r8g.48xlarge 2	40000		5000.0		240000	
r8g.logam-24xl 2	30000		3750.0		120000	
r8g.logam-48xl 2	40000		5000.0		240000	
r8gb.sedang 1	1562	25000	195.31	3125.00	7500	120000
r8gb.large 1	3125	25000	390.62	3125.00	15000	120000
r8gb.xlarge 1	6250	25000	781,25	3125.00	30000	120000
r8gb.2xbesar 1	12500	25000	1562.50	3125.00	60000	120000
r8gb.4xbesar 2	25000		3125.0		120000	
r8gb.8xlarge 2	50000		6250.0		240000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r8gb.12xlarge 2	75000		9375.0		360000	
r8gb.16xlarge 2	100000		12500.0		480000	
r8gb.24xbesar 2	150000		18750,0		720000	
r8gb.48xlarge 2	300000		37500.0		1440000	
r8gb.metal-24xl 2	150000		18750,0		720000	
r8gb.metal-48xl 2	300000		37500.0		1440000	
r8gd.sedang 1	315	10000	39,38	1250,00	2500	40000
r8gd.large 1	630	10000	78.75	1250,00	3600	40000
r8gd.xlarge 1	1250	10000	156,25	1250,00	6000	40000
r8gd.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
r8gd.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
r8gd.8xlarge 2	10000		1250.0		40000	
r8gd.12xlarge 2	15000		1875.0		60000	
r8gd.16xlarge 2	20000		2500.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r8gd.24xlarge 2	30000		3750.0		120000	
r8gd.48xlarge 2	40000		5000.0		240000	
r8gd.metal-24xl 2	30000		3750.0		120000	
r8gd.metal-48xl 2	40000		5000.0		240000	
r8gn.sedang 1	760	10000	95.00	1250,00	2500	40000
r8gn.large 1	1250	10000	156,25	1250,00	5000	40000
r8gn.xlarge 1	2500	10000	312.50	1250,00	10000	40000
r8gn.2xlarge 1	5000	10000	625.00	1250,00	20000	40000
r8gn.4xlarge 2	10000		1250.0		40000	
r8gn.8xlarge 2	20000		2500.0		80000	
r8gn.12xlarge 2	30000		3750.0		120000	
r8gn.16xlarge 2	40000		5000.0		160000	
r8gn.24xlarge 2	60000		7500.0		240000	
r8gn.48xlarge 2	60000		7500.0		240000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r8gn.metal-24xl 2	60000		7500.0		240000	
r8gn.metal-48xl 2	60000		7500.0		240000	
r8i.large 1	650	10000	81,25	1250,00	3600	40000
r8i.xlarge 1	1250	10000	156,25	1250,00	6000	40000
r8i.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
r8i.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
r8i.8xlarge 2	10000		1250.0		40000	
r8i.12xlarge 2	15000		1875.0		60000	
r8i.16xlarge 2	20000		2500.0		80000	
r8i.24xlarge 2	30000		3750.0		120000	
r8i.32xlarge 2	40000		5000.0		160000	
r8i.48xlarge 2	60000		7500.0		240000	
r8i.96xlarge 2	80000		10000.0		480000	
r8i.logam-48xl 2	60000		7500.0		240000	
r8i.logam-96xl 2	80000		10000.0		480000	
r8id.large 1	650	10000	81,25	1250,00	3600	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r8id.xlarge 1	1250	10000	156,25	1250,00	6000	40000
r8id.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
r8id.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
r8id.8xlarge 2	10000		1250.0		40000	
r8id.12xlarge 2	15000		1875.0		60000	
r8id.16xlarge 2	20000		2500.0		80000	
r8id.24xlarge 2	30000		3750.0		120000	
r8id.32xlarge 2	40000		5000.0		160000	
r8id.48xlarge 2	60000		7500.0		240000	
r8id.96xlarge 2	80000		10000.0		480000	
r8id.metal-48xl 2	60000		7500.0		240000	
r8id.metal-96xl 2	80000		10000.0		480000	
r8i-flex.large 1	315	10000	39,38	1250,00	2500	40000
r8i-flex.xlarge 1	630	10000	78.75	1250,00	3600	40000
r8i-flex.2xlarge 1	1250	10000	156,25	1250,00	6000	40000
r8i-flex.4xlarge 1	2500	10000	312.50	1250,00	12000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
r8i-flex.8xlarge 1	5000	10000	625.00	1250,00	20000	40000
r8i-flex. 12xlarge 1	7500	15000	937,50	1875.00	30000	60000
r8i-flex. 16xlarge 1	10000	20000	1250,00	2500.00	40000	80000
u-3tb1.56 xlarge [2]	19000		2375.0		80000	
u-6tb1.56 xlarge [2]	38000		4750,0		160000	
u-6tb1.11 2xlarge [2]	38000		4750,0		160000	
u-6tb1.me tal [2]	38000		4750,0		160000	
u-9tb1.11 2xlarge [2]	38000		4750,0		160000	
u-9tb1.me tal [2]	38000		4750,0		160000	
u-12tb1.1 12xlarge [2]	38000		4750,0		160000	
u-12tb1.m etal [2]	38000		4750,0		160000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
u-18tb1.112xlarge [2]	38000		4750,0		160000	
u-18tb1.metal [2]	38000		4750,0		160000	
u-24tb1.112xlarge [2]	38000		4750,0		160000	
u-24tb1.metal [2]	38000		4750,0		160000	
u7i-6tb.112xlarge 2	100000		12500.0		560000	
u7i-8tb.112xlarge 2	100000		12500.0		560000	
u7i-12tb.224xbesar 2	100000		12500.0		560000	
u7in-16tb.224xlarge 2	100000		12500.0		560000	
u7in-24tb.224xlarge 2	100000		12500.0		560000	
u7in-32tb.224xlarge 2	100000		12500.0		560000	
u7inh-32tb.480xlarge 2	160000		20000.0		840000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
x1.16xlarge [2]	7000		875.0		40000	
x1.32xlarge [2]	14000		1750.0		80000	
x1e.xlarge [2]	500		62.5		3700	
x1e.2xlarge [2]	1000		125,0		7400	
x1e.4xlarge [2]	1750		218.75		10000	
x1e.8xlarge [2]	3500		437.5		20000	
x1e.16xlarge [2]	7000		875.0		40000	
x1e.32xlarge [2]	14000		1750.0		80000	
x2gd.medium [1]	315	4750	39,38	593,75	2500	20000
x2gd.large [1]	630	4750	78.75	593,75	3600	20000
x2gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
x2gd.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
x2gd.4xlarge [2]	4750		593,75		20000	
x2gd.8xlarge [2]	9500		1187,5		40000	
x2gd.12xlarge [2]	14250		1781.25		60000	
x2gd.16xlarge [2]	19000		2375.0		80000	
x2gd.metal [2]	19000		2375.0		80000	
x2idn.16xlarge [2]	40000		5000.0		173333	
x2idn.24xlarge [2]	60000		7500.0		260000	
x2idn.32xlarge [2]	80000		10000.0		260000	
x2idn.metal [2]	80000		10000.0		260000	
x2iedn.xlarge [1]	2500	20000	312.50	2500.00	8125	65000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
x2iedn.2xlarge [1]	5000	20000	625.00	2500.00	16250	65000
x2iedn.4xlarge [1]	10000	20000	1250,00	2500.00	32500	65000
x2iedn.8xlarge [2]	20000		2500.0		65000	
x2iedn.16xlarge [2]	40000		5000.0		130000	
x2iedn.24xlarge [2]	60000		7500.0		195000	
x2iedn.32xlarge [2]	80000		10000.0		260000	
x2iedn.metal [2]	80000		10000.0		260000	
x2iezn.2xlarge [2]	3170		396.25		13333	
x2iezn.4xlarge [2]	4750		593,75		20000	
x2iezn.6xlarge [2]	9500		1187,5		40000	
x2iezn.8xlarge [2]	12000		1500.0		55000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
x2iezn.12xlarge [2]	19000		2375.0		80000	
x2iezn.metal [2]	19000		2375.0		80000	
x8g.medium 1	315	10000	39,38	1250,00	2500	40000
x8g.large 1	630	10000	78.75	1250,00	3600	40000
x8g.xlarge 1	1250	10000	156,25	1250,00	6000	40000
x8g.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
x8g.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
x8g.8xlarge 2	10000		1250.0		40000	
x8g.12xlarge 2	15000		1875.0		60000	
x8g.16xlarge 2	20000		2500.0		80000	
x8g.24xlarge 2	30000		3750.0		120000	
x8g.48xlarge 2	40000		5000.0		240000	
x8g.logam-24xl 2	30000		3750.0		120000	
x8g.logam-48xl 2	40000		5000.0		240000	
x8aedz.large 1	1250	15000	156,25	1875.00	5000	60000
x8aedz.xlarge 1	2500	15000	312.50	1875.00	10000	60000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
x8aedz.3xlarge 1	7500	15000	937,50	1875.00	30000	60000
x8aedz.6xlarge 2	15000		1875.0		60000	
x8aedz.12xlarge 2	30000		3750.0		120000	
x8aedz.24xlarge 2	60000		7500.0		240000	
x8aedz.metal-12xl 2	30000		3750.0		120000	
x8aedz.metal-24xl 2	60000		7500.0		240000	
x8i.large 1	650	10000	81,25	1250,00	3600	40000
x8i.xlarge 1	1250	10000	156,25	1250,00	6000	40000
x8i.2xlarge 1	2500	10000	312.50	1250,00	12000	40000
x8i.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
x8i.8xlarge 2	10000		1250.0		40000	
x8i.12xlarge 2	15000		1875.0		60000	
x8i.16xlarge 2	20000		2500.0		80000	
x8i.24xlarge 2	30000		3750.0		120000	
x8i.32xlarge 2	40000		5000.0		160000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
x8i.48xlarge 2	60000		7500.0		240000	
x8i.64xlarge 2	70000		8750,0		320000	
x8i.96xlarge 2	80000		10000.0		480000	
x8i.logam-48xl 2	60000		7500.0		240000	
x8i.logam-96xl 2	80000		10000.0		480000	
z1d.large [1]	800	3170	100.00	396.25	3333	13333
z1d.xlarge [1]	1580	3170	197.50	396.25	6667	13333
z1d.2xlarge [2]	3170		396.25		13333	
z1d.3xlarge [2]	4750		593,75		20000	
z1d.6xlarge [2]	9500		1187,5		40000	
z1d.12xlarge [2]	19000		2375.0		80000	
z1d.metal [2]	19000		2375.0		80000	

[1] Contoh ini dapat mempertahankan kinerja maksimum selama 30 menit setidaknya sekali setiap 24 jam, setelah itu mereka kembali ke kinerja dasar mereka.

[2] Instans ini dapat mempertahankan performa yang dinyatakan tanpa batas waktu. Jika beban kerja Anda memerlukan performa maksimum yang berkelanjutan selama lebih dari 30 menit, gunakan salah satu instans ini.

Penyimpanan yang dioptimalkan

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
d2.xlarge [2]	750		93,75		6000	
d2.2xlarge [2]	1000		125,0		8000	
d2.4xlarge [2]	2000		250.0		16000	
d2.8xlarge [2]	4000		500,0		32000	
d3.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3.2xlarge [1]	1700	2800	212.50	350,00	10000	15000
d3.4xlarge [2]	2800		350.0		15000	
d3.8xlarge [2]	5000		625.0		30000	
d3en.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3en.2xlarge [1]	1700	2800	212.50	350,00	10000	15000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
d3en.4xlarge [2]	2800		350.0		15000	
d3en.6xlarge [2]	4000		500,0		25000	
d3en.8xlarge [2]	5000		625.0		30000	
d3en.12xlarge [2]	7000		875.0		40000	
h1.2xlarge [2]	1750		218.75		12000	
h1.4xlarge [2]	3500		437.5		20000	
h1.8xlarge [2]	7000		875.0		40000	
h1.16xlarge [2]	14000		1750.0		80000	
i3.large [2]	425		53.125		3000	
i3.xlarge [2]	850		106,25		6000	
i3.2xlarge [2]	1700		212.5		12000	
i3.4xlarge [2]	3500		437.5		16000	
i3.8xlarge [2]	7000		875.0		32500	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
i3.16xlarge [2]	14000		1750.0		65000	
i3.metal [2]	19000		2375.0		80000	
i3en.large [1]	576	4750	72.10	593,75	3000	20000
i3en.xlarge [1]	1153	4750	144,20	593,75	6000	20000
i3en.2xlarge [1]	2307	4750	288.39	593,75	12000	20000
i3en.3xlarge [1]	3800	4750	475.00	593,75	15000	20000
i3en.6xlarge [2]	4750		593,75		20000	
i3en.12xlarge [2]	9500		1187,5		40000	
i3en.24xlarge [2]	19000		2375.0		80000	
i3en.metal [2]	19000		2375.0		80000	
i4g.large [1]	625	10000	78.12	1250,00	2500	40000
i4g.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4g.2xlarge [1]	2500	10000	312.50	1250,00	10000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
i4g.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
i4g.8xlarge [2]	10000		1250.0		40000	
i4g.16xlarge [2]	20000		2500.0		80000	
i4i.large [1]	625	10000	78.12	1250,00	2500	40000
i4i.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4i.2xlarge [1]	2500	10000	312.50	1250,00	10000	40000
i4i.4xlarge [1]	5000	10000	625.00	1250,00	20000	40000
i4i.8xlarge [2]	10000		1250.0		40000	
i4i.12xlarge [2]	15000		1875.0		60000	
i4i.16xlarge [2]	20000		2500.0		80000	
i4i.24xlarge [2]	30000		3750.0		120000	
i4i.32xlarge [2]	40000		5000.0		160000	
i4i.metal [2]	40000		5000.0		160000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
i7i.large 1	625	10000	78.12	1250,00	2500	40000
i7i.xlarge 1	1250	10000	156,25	1250,00	5000	40000
i7i.2xlarge 1	2500	10000	312.50	1250,00	10000	40000
i7i.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
i7i.8xlarge 2	10000		1250.0		40000	
i7i.12xlarge 2	15000		1875.0		60000	
i7i.16xlarge 2	20000		2500.0		80000	
i7i.24xlarge 2	30000		3750.0		120000	
i7i.48xlarge 2	60000		7500.0		240000	
i7i.logam-24xl 2	30000		3750.0		120000	
i7i.logam-48xl 2	60000		7500.0		240000	
i7ie.large 1	625	10000	78.12	1250,00	2500	40000
i7ie.xlarge 1	1250	10000	156,25	1250,00	5000	40000
i7ie.2xlarge 1	2500	10000	312.50	1250,00	10000	40000
i7ie.3xlarge 1	3750	10000	468,75	1250,00	15000	40000
i7ie.6xlarge 1	7500	10000	937,50	1250,00	30000	40000
i7ie.12xlarge 2	15000		1875.0		60000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
i7ie.18xlarge 2	22500		2812.5		90000	
i7ie.24xlarge 2	30000		3750.0		120000	
i7ie.48xlarge 2	60000		7500.0		240000	
i7ie.logam-24xl 2	30000		3750.0		120000	
i7ie.logam-48xl 2	60000		7500.0		240000	
i8g.large 1	625	10000	78.12	1250,00	2500	40000
i8g.xlarge 1	1250	10000	156,25	1250,00	5000	40000
i8g.2xlarge 1	2500	10000	312.50	1250,00	10000	40000
i8g.4xlarge 1	5000	10000	625.00	1250,00	20000	40000
i8g.8xlarge 2	10000		1250.0		40000	
i8g.12xlarge 2	15000		1875.0		60000	
i8g.16xlarge 2	20000		2500.0		80000	
i8g.24xlarge 2	30000		3750.0		120000	
i8g.48xlarge 2	60000		7500.0		240000	
i8g.logam-24xl 2	30000		3750.0		120000	
i8g.logam-48xl 2	60000		7500.0		240000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
i8ge.large 1	625	10000	78.12	1250,00	2500	40000
i8ge.xlarge 1	1250	10000	156,25	1250,00	5000	40000
i8ge.2xlarge 1	2500	10000	312.50	1250,00	10000	40000
i8ge.3xlarge 1	3750	10000	468,75	1250,00	15000	40000
i8ge.6xlarge 1	7500	10000	937,50	1250,00	30000	40000
i8ge.12xlarge 2	15000		1875.0		60000	
i8ge.18xlarge 2	22500		2812.5		90000	
i8ge.24xlarge 2	30000		3750.0		120000	
i8ge.48xlarge 2	60000		7500.0		240000	
i8ge.metal-24xl 2	30000		3750.0		120000	
i8ge.metal-48xl 2	60000		7500.0		240000	
im4gn.large [1]	1250	10000	156,25	1250,00	5000	40000
im4gn.xlarge [1]	2500	10000	312.50	1250,00	10000	40000
im4gn.2xlarge [1]	5000	10000	625.00	1250,00	20000	40000
im4gn.4xlarge [2]	10000		1250.0		40000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
im4gn.8xlarge [2]	20000		2500.0		80000	
im4gn.16xlarge [2]	40000		5000.0		160000	
is4gen.medium [1]	625	10000	78.12	1250,00	2500	40000
is4gen.large [1]	1250	10000	156,25	1250,00	5000	40000
is4gen.xlarge [1]	2500	10000	312.50	1250,00	10000	40000
is4gen.2xlarge [1]	5000	10000	625.00	1250,00	20000	40000
is4gen.4xlarge [2]	10000		1250.0		40000	
is4gen.8xlarge [2]	20000		2500.0		80000	

[1] Contoh ini dapat mempertahankan kinerja maksimum selama 30 menit setidaknya sekali setiap 24 jam, setelah itu mereka kembali ke kinerja dasar mereka.

[2] Instans ini dapat mempertahankan performa yang dinyatakan tanpa batas waktu. Jika beban kerja Anda memerlukan performa maksimum yang berkelanjutan selama lebih dari 30 menit, gunakan salah satu instans ini.

Komputasi yang dipercepat

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
dl1.24xlarge [2]	19000		2375.0		80000	
dl2q.24xlarge [2]	19000		2375.0		80000	
f1.2xlarge [2]	1700		212.5		12000	
f1.4xlarge [2]	3500		437.5		44000	
f1.16xlarge [2]	14000		1750.0		75000	
f2.6xbesar 2	7500		937,5		30000	
f2.12xbesar 2	15000		1875.0		60000	
f2.48xbesar 2	60000		7500.0		240000	
g3.4xlarge [2]	3500		437.5		20000	
g3.8xlarge [2]	7000		875.0		40000	
g3.16xlarge [2]	14000		1750.0		80000	
g4ad.xlarge [1]	400	3170	50,00	396.25	1700	13333
g4ad.2xlarge [1]	800	3170	100.00	396.25	3400	13333

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
g4ad.4xlarge [1]	1580	3170	197.50	396.25	6700	13333
g4ad.8xlarge [2]	3170		396.25		13333	
g4ad.16xlarge [2]	6300		787.5		26667	
g4dn.xlarge [1]	950	3500	118.75	437.50	3000	20000
g4dn.2xlarge [1]	1150	3500	143,75	437.50	6000	20000
g4dn.4xlarge [2]	4750		593,75		20000	
g4dn.8xlarge [2]	9500		1187,5		40000	
g4dn.12xlarge [2]	9500		1187,5		40000	
g4dn.16xlarge [2]	9500		1187,5		40000	
g4dn.metal [2]	19000		2375.0		80000	
g5.xlarge [1]	700	3500	87.50	437.50	3000	15000
g5.2xlarge [1]	850	3500	106,25	437.50	3500	15000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
g5.4xlarge [2]	4750		593,75		20000	
g5.8xlarge [2]	16000		2000,0		65000	
g5.12xlarge [2]	16000		2000,0		65000	
g5.16xlarge [2]	16000		2000,0		65000	
g5.24xlarge [2]	19000		2375.0		80000	
g5.48xlarge [2]	19000		2375.0		80000	
g5g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
g5g.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
g5g.4xlarge [2]	4750		593,75		20000	
g5g.8xlarge [2]	9500		1187,5		40000	
g5g.16xlarge [2]	19000		2375.0		80000	
g5g.metal [2]	19000		2375.0		80000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
g6.xlarge 1	1000	5000	125.00	625.00	4000	20000
g6.2xlarge 1	2000	5000	250.00	625.00	8000	20000
g6.4xlarge 2	8000		1000,0		32000	
g6.8xlarge 2	16000		2000,0		64000	
g6.12xlarge 2	20000		2500.0		80000	
g6.16xlarge 2	20000		2500.0		80000	
g6.24xlarge 2	30000		3750.0		120000	
g6.48xlarge 2	60000		7500.0		240000	
g6e.xlarge 1	1000	5000	125.00	625.00	4000	20000
g6e.2xlarge 1	2000	5000	250.00	625.00	8000	20000
g6e.4xlarge 2	8000		1000,0		32000	
g6e.8xlarge 2	16000		2000,0		64000	
g6e.12xlarge 2	20000		2500.0		80000	
g6e.16xlarge 2	20000		2500.0		80000	
g6e.24xlarge 2	30000		3750.0		120000	
g6e.48xlarge 2	60000		7500.0		240000	
g6f.large 1	936	5000	117.00	625.00	3750	20000
g6f.xlarge 1	1000	5000	125.00	625.00	4000	20000
g6f.2xlarge 1	2000	5000	250.00	625.00	8000	20000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
g6f.4xlarge 2	6000		750.0		24000	
gr6.4xbesar 2	8000		1000,0		32000	
gr6.8xbesar 2	16000		2000,0		64000	
gr6f.4xbesar 2	8000		1000,0		32000	
g7e.2xlarge 1	2000	5000	250.00	625.00	8000	20000
g7e.4xlarge 2	8000		1000,0		32000	
g7e.8xlarge 2	16000		2000,0		64000	
g7e.12xlarge 2	25000		3125.0		100000	
g7e.24xlarge 2	50000		6250.0		200000	
g7e.48xlarge 2	100000		12500.0		400000	
inf1.xlarge 1	1190	4750	148,75	593,75	4000	20000
inf1.2xlarge 1	1190	4750	148,75	593,75	6000	20000
inf1.6xlarge 2	4750		593,75		20000	
inf1.24xlarge 2	19000		2375.0		80000	
inf2.xlarge 1	1250	10000	156,25	1250,00	6000	40000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
inf2.8xlarge [2]	10000		1250.0		40000	
inf2.24xlarge [2]	30000		3750.0		120000	
inf2.48xlarge [2]	60000		7500.0		240000	
p3.2xlarge [2]	1750		218.75		10000	
p3.8xlarge [2]	7000		875.0		40000	
p3.16xlarge [2]	14000		1750.0		80000	
p3dn.24xlarge [2]	19000		2375.0		80000	
p4d.24xlarge [2]	19000		2375.0		80000	
p4de.24xlarge [2]	19000		2375.0		80000	
p5.4xbesar 2	10000		1250.0		32500	
p5.48xlarge [2]	80000		10000.0		260000	
p5e.48xlarge 2	80000		10000.0		260000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
p5en.48xlarge 2	100000		12500.0		400000	
p6-b200.48xlarge 2	100000		12500.0		400000	
p6-b300.48xlarge 2	100000		12500.0		400000	
p6e-gb200.36xlarge 2	60000		7500.0		240000	
trn1.2xlarge [1]	5000	20000	625.00	2500.00	16250	65000
trn1.32xlarge [2]	80000		10000.0		260000	
trn1n.32xlarge [2]	80000		10000.0		260000	
trn2.3xlarge 2	5000		625.0		16250	
trn2.48xlarge 2	80000		10000.0		260000	
trn2u.48xlarge 2	80000		10000.0		260000	
vt1.3xlarge 1	2375	4750	296.88	593,75	10000	20000
vt1.6xlarge 2	4750		593,75		20000	

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
vt1.24xlarge [2]	19000		2375.0		80000	

[1] Contoh ini dapat mempertahankan kinerja maksimum selama 30 menit setidaknya sekali setiap 24 jam, setelah itu mereka kembali ke kinerja dasar mereka.

[2] Instans ini dapat mempertahankan performa yang dinyatakan tanpa batas waktu. Jika beban kerja Anda memerlukan performa maksimum yang berkelanjutan selama lebih dari 30 menit, gunakan salah satu instans ini.

Komputasi performa tinggi

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
hpc6a.48xlarge [1]	87	2085	10.88	260.62	500	11000
hpc6id.32xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7a.12xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7a.24xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7a.48xlarge [1]	87	2085	10.88	260.62	500	11000

Ukuran instans	Bandwidth dasar (Mbps)	Bandwidth maksimum (Mbps)	Throughput dasar () MB/s, 128 KiB I/O	Throughput maksimum () MB/s, 128 KiB I/O	IOPS dasar (16 KiB I/O)	IOPS maksimum (16 KiB I/O)
hpc7a.96xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7g.4xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7g.8xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7g.16xlarge [1]	87	2085	10.88	260.62	500	11000
hpc8a.96xlarge 1	87	2085	10.88	260.62	500	11000

[1] Contoh ini dapat mempertahankan kinerja maksimum selama 30 menit setidaknya sekali setiap 24 jam, setelah itu mereka kembali ke kinerja dasar mereka.

[2] Instans ini dapat mempertahankan performa yang dinyatakan tanpa batas waktu. Jika beban kerja Anda memerlukan performa maksimum yang berkelanjutan selama lebih dari 30 menit, gunakan salah satu instans ini.

Optimisasi EBS didukung

Jenis instance berikut mendukung pengoptimalan EBS tetapi pengoptimalan EBS tidak diaktifkan secara default. Anda harus mengaktifkan pengoptimalan EBS, dengan biaya tambahan per jam, selama atau setelah peluncuran untuk mencapai tingkat kinerja EBS yang dijelaskan.

Ukuran instans	Bandwidth maksimum (Mbps)	Throughput maksimum () MB/s, 128 KiB I/O	IOPS maksimum (16 KiB I/O)
c1.xlarge	1000	125,0	8000

Ukuran instans	Bandwidth maksimum (Mbps)	Throughput maksimum () MB/s, 128 KiB I/O	IOPS maksimum (16 KiB I/O)
c3.xlarge	500	62.5	4000
c3.2xlarge	1000	125,0	8000
c3.4xlarge	2000	250.0	16000
i2.xlarge	500	62.5	4000
i2.2xlarge	1000	125,0	8000
i2.4xlarge	2000	250.0	16000
m1.large	500	62.5	4000
m1.xlarge	1000	125,0	8000
m2.2xlarge	500	62.5	4000
m2.4xlarge	1000	125,0	8000
m3.xlarge	500	62.5	4000
m3.2xlarge	1000	125,0	8000
r3.xlarge	500	62.5	4000
r3.2xlarge	1000	125,0	8000
r3.4xlarge	2000	250.0	16000

Note

Instans `i2.8xlarge`, `c3.8xlarge`, dan `r3.8xlarge` tidak memiliki bandwidth EBS khusus dan tidak menawarkan optimisasi EBS. Pada instans ini, lalu lintas jaringan dan lalu lintas Amazon EBS berbagi antarmuka jaringan 10 gigabit yang sama.

Dapatkan performa maksimal Amazon EBS yang dioptimalkan

Kinerja EBS instans dibatasi oleh batas kinerja tipe instans, atau kinerja agregat dari volume terlampirnya, mana yang lebih kecil. Untuk mencapai performa EBS maksimum, instans harus memiliki volume terlampir yang memberikan performa gabungan yang sama atau lebih besar dari performa instans maksimum. Misalnya, untuk mencapai `80,000` IOPS`r6i.16xlarge`, instance harus memiliki setidaknya 5 `gp2` volume yang disediakan dengan `16,000` IOPS masing-masing (5volume x IOPS = `16,000` IOPS), atau volume dapat disediakan dengan `80,000` IOPS. 1 `gp3` `80,000` Kami menyarankan Anda memilih jenis instans yang menyediakan throughput Amazon EBS yang lebih berdedikasi daripada kebutuhan aplikasi Anda; jika tidak, koneksi antara Amazon EBS dan Amazon EC2 dapat menjadi hambatan kinerja.

> **Important**
>
> Saat menggunakan pembobotan bandwidth yang dapat dikonfigurasi, batas bandwidth EBS untuk instans Anda mungkin berubah. Misalnya dengan konfigurasi `VPC-1` pembobotan, yang meningkatkan bandwidth jaringan, Anda mungkin mengalami IOPS yang lebih rendah dari yang diharapkan untuk volume EBS karena mencapai batas bandwidth EBS sebelum batas IOPS. Ini terutama terlihat dengan I/O ukuran yang lebih besar. Selalu uji beban kerja spesifik Anda untuk memastikannya memenuhi persyaratan kinerja Anda dengan pembobotan bandwidth pilihan Anda. Untuk informasi selengkapnya, lihat EC2 konfigurasi pembobotan bandwidth contoh.

Anda dapat menggunakan metrik `EBSIOBalance%` dan `EBSByteBalance%` untuk membantu Anda menentukan apakah instans Anda memiliki ukuran yang tepat. Anda dapat melihat metrik ini di CloudWatch konsol dan menyetel alarm yang dipicu berdasarkan ambang batas yang Anda tentukan. Metrik ini dinyatakan sebagai persentase. Instans dengan persentase keseimbangan yang rendah secara konsisten adalah kandidat yang harus naik ukurannya. Instans yang persentase keseimbangan tidak pernah turun di bawah 100% adalah kandidat untuk penurunan ukuran. Untuk informasi selengkapnya, lihat Pantau instans Anda menggunakan CloudWatch.

Instans memori yang tinggi dirancang untuk menjalankan basis data dalam memori yang besar, termasuk deployment produksi dari basis data dalam memori SAP HANA, di cloud. Untuk memaksimalkan performa EBS, gunakan instans memori yang tinggi dengan menerapkan jumlah genap volume `io1` atau `io2` dengan performa identik yang disediakan. Misalnya, untuk beban kerja berat IOPS, gunakan empat volume `io1` atau `io2` dengan 40.000 IOPS yang Tersedia untuk mendapatkan maksimum 160.000 instans IOPS. Demikian pula, untuk throughput beban kerja berat,

gunakan enam `io1` atau `io2` volume dengan 48.000 IOPS yang disediakan untuk mendapatkan throughput maksimum 4.750. MB/s Untuk rekomendasi tambahan, lihat Konfigurasi Penyimpanan untuk SAP HANA.

Pertimbangan-pertimbangan

- Instans G4dn, i3en, Inf1, M5a, M5ad, R5a, R5ad, T3, T3a, dan Z1d yang diluncurkan setelah 26 Februari 2020 memberikan kinerja EBS maksimum yang dioptimalkan. Untuk mendapatkan performa maksimum dari suatu instans yang diluncurkan sebelum 26 Februari 2020, hentikan dan mulai.
- Instans C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn, dan P3dn yang diluncurkan setelah 3 Desember 2019 memberikan kinerja EBS maksimum yang dioptimalkan. Untuk mendapatkan performa maksimum dari instans yang diluncurkan sebelum 3 Desember 2019, hentikan dan mulai.
- `u-6tb1.metal`,`u-9tb1.metal`, dan `u-12tb1.metal` instans yang diluncurkan setelah 12 Maret 2020 memberikan kinerja EBS maksimum yang dioptimalkan. Tipe instans ini diluncurkan sebelum 12 Maret 2020 mungkin memberikan performa yang lebih rendah. Untuk mendapatkan performa maksimum dari suatu instans yang diluncurkan sebelum 12 Maret 2020, hubungi tim akun Anda untuk mempebarui instansnya tanpa biaya tambahan.

Temukan jenis instans EC2 yang dioptimalkan EBS

Anda dapat melihat jenis instans yang mendukung pengoptimalan EBS di setiap Wilayah.

Console

Untuk menemukan jenis instance yang dioptimalkan EBS secara default

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Tipe Instans.
3. Tambahkan filter dukungan optimasi EBS = default.
4. (Opsional) Klik ikon Preferensi dan kemudian nyalakan kolom yang relevan, seperti EBS Maximum IOPS dan EBS Baseline IOPS.
5. (Opsional) Tambahkan filter ke cakupan lebih lanjut ke jenis instans tertentu yang menarik.

AWS CLI

Untuk menemukan jenis instance yang dioptimalkan EBS secara default

Gunakan perintah perintah describe-instance-types berikut ini.

```
aws ec2 describe-instance-types \
--filters Name=ebs-info.ebs-optimized-support,Values=default  \
--query 'InstanceTypes[].{InstanceType:InstanceType,
 "MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,
 MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--output=table
```

Untuk menemukan jenis instans yang secara opsional mendukung pengoptimalan EBS

Gunakan perintah berikut describe-instance-types.

```
aws ec2 describe-instance-types \
--filters Name=ebs-info.ebs-optimized-support,Values=supported \
--query 'InstanceTypes[].{InstanceType:InstanceType,
 "MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,
 MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--output=table
```

Berikut ini adalah contoh output untukeu-west-1.

```
-------------------------------------------------------------------------
|                          DescribeInstanceTypes                        |
+--------------+----------------------+----------+----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+----------------------+----------+----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
```

```
|  c3.xlarge   |  500                 |  4000    |  62.5                |
|  m3.2xlarge  |  1000                |  8000    |  125.0               |
|  r3.xlarge   |  500                 |  4000    |  62.5                |
|  i2.4xlarge  |  2000                |  16000   |  250.0               |
|  c3.4xlarge  |  2000                |  16000   |  250.0               |
|  c3.2xlarge  |  1000                |  8000    |  125.0               |
|  m1.large    |  500                 |  4000    |  62.5                |
+--------------+----------------------+----------+----------------------+
```

PowerShell

Untuk menemukan jenis instance yang dioptimalkan EBS secara default

Gunakan Get-EC2InstanceTypecmdlet.

```
Get-EC2InstanceType `
    -Filter @{Name="ebs-info.ebs-optimized-support"; Values="default"} | `
    Select InstanceType, `
        @{Name="MaxBandwidth(Mb/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps)}}, `
        @{Name="MaxIOPS"; Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumIops)}}, `
        @{Name="MaxThroughput (MB/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps)}}
```

Untuk menemukan jenis instans yang secara opsional mendukung pengoptimalan EBS

Gunakan Get-EC2InstanceTypecmdlet.

```
Get-EC2InstanceType `
    -Filter @{Name="ebs-info.ebs-optimized-support"; Values="supported"} | `
    Select InstanceType, `
        @{Name="MaxBandwidth(Mb/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps)}}, `
        @{Name="MaxIOPS"; Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumIops)}}, `
        @{Name="MaxThroughput (MB/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps)}}
```

Berikut ini adalah contoh output untuk`eu-west-1`.

```
InstanceType MaxBandwidth(Mb/s) MaxIOPS MaxThroughput (MB/s)
------------ ------------------ ------- --------------------
m2.4xlarge                1000    8000              125.000
```

```
i2.2xlarge                1000    8000              125.000
c1.xlarge                 1000    8000              125.000
m2.2xlarge                 500    4000               62.500
r3.2xlarge                1000    8000              125.000
m3.xlarge                  500    4000               62.500
r3.4xlarge                2000   16000              250.000
m1.xlarge                 1000    8000              125.000
i2.xlarge                  500    4000               62.500
c3.xlarge                  500    4000               62.500
c3.4xlarge                2000   16000              250.000
c3.2xlarge                1000    8000              125.000
i2.4xlarge                2000   16000              250.000
r3.xlarge                  500    4000               62.500
m3.2xlarge                1000    8000              125.000
m1.large                   500    4000               62.500
```

Aktifkan pengoptimalan EBS untuk instans Amazon EC2

Anda dapat mengaktifkan pengoptimalan EBS secara manual hanya untuk jenis instans generasi sebelumnya yang secara opsional mendukung pengoptimalan EBS. Jika Anda mengaktifkan pengoptimalan EBS untuk jenis instans ini, ada biaya tambahan per jam

Prasyarat

- Verifikasi bahwa jenis instans mengharuskan Anda mengaktifkan pengoptimalan EBS. Untuk informasi selengkapnya, lihat Optimisasi EBS didukung.
- Untuk mengaktifkan pengoptimalan EBS setelah peluncuran, Anda harus menghentikan instans.

> **Warning**
>
> Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instans akan hilang. Untuk menyimpan data ini, buat cadangan ke penyimpanan persisten.

Console

Untuk mengaktifkan optimasi Amazon EBS selama peluncuran

Di wizard Peluncuran instance, pilih jenis instans yang diperlukan. Perluas bagian Detail lanjutan, lalu untuk instans yang dioptimalkan EBS, pilih Aktifkan.

Jika jenis instans yang dipilih tidak mendukung optimasi Amazon EBS, drop-down akan dinonaktifkan. Jika jenis instans adalah Amazon EBS yang dioptimalkan secara default, Aktifkan sudah dipilih.

Untuk mengaktifkan optimasi Amazon EBS setelah peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, dan pilih instans.
3. Hentikan instans. Pilih Actions, Instance state, Stop instance.
4. Dengan instans yang masih dipilih, klik Tindakan, Pengaturan instans, Ubah tipe instans.
5. Pilih EBS dioptimalkan dan kemudian pilih Terapkan.

   Jika jenis instans adalah Amazon EBS yang dioptimalkan secara default, atau jika tidak mendukung pengoptimalan Amazon EBS, kotak centang akan dinonaktifkan.
6. Mulai ulang instans. Pilih Status instans, Mulai instans.

AWS CLI

Untuk mengaktifkan optimasi Amazon EBS selama peluncuran

Gunakan perintah run-instance dengan opsi. `--ebs-optimized`

Untuk mengaktifkan optimasi Amazon EBS setelah peluncuran

1. Jika instance sedang berjalan, hentikan dengan menggunakan perintah stop-instance.

   ```
   aws ec2 stop-instances --instance-ids i-1234567890abcdef0
   ```
2. Aktifkan optimasi EBS dengan menggunakan modify-instance-attributeperintah dengan `--ebs-optimized` opsi.

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 \
       --ebs-optimized
   ```

PowerShell

Untuk mengaktifkan optimasi Amazon EBS selama peluncuran

Gunakan New-EC2Instancecmdlet dengan opsi. `-EbsOptimized`

Untuk mengaktifkan optimasi Amazon EBS setelah peluncuran

1. Jika instance sedang berjalan, hentikan dengan menggunakan Stop-EC2Instancecmdlet.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

2. Aktifkan optimasi EBS dengan menggunakan Edit-EC2InstanceAttributecmdlet dengan opsi. `-EbsOptimized`

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -EbsOptimized $true
```

Opsi CPU untuk instans Amazon EC2

Banyak instans Amazon EC2 mendukung multithreading simultan (SMT), yang memungkinkan beberapa thread berjalan secara bersamaan pada satu inti CPU. Setiap thread direpresentasikan sebagai CPU virtual (vCPU) pada instans. Sebuah instans memiliki jumlah inti CPU default, yang bervariasi sesuai dengan tipe instans. Misalnya, tipe `m5.xlarge` instance memiliki dua core CPU dan dua thread per core secara default — total empat v. CPUs

Dalam kebanyakan kasus, ada jenis instans Amazon EC2 yang memiliki kombinasi memori dan jumlah v yang sesuai dengan beban CPUs kerja Anda. Namun, untuk mengoptimalkan instans Anda untuk beban kerja atau kebutuhan bisnis tertentu, Anda dapat menentukan opsi CPU berikut selama dan setelah peluncuran instance:

- Jumlah inti CPU: Anda dapat menyesuaikan jumlah inti CPU untuk instans. Anda mungkin akan melakukan ini agar dapat mengoptimalkan biaya lisensi perangkat lunak Anda dengan instans yang memiliki jumlah RAM yang cukup untuk beban kerja yang membutuhkan memori intensif tetapi dengan inti CPU yang lebih sedikit.
- Thread per core: Anda dapat menonaktifkan SMT dengan menentukan satu utas per inti CPU. Anda dapat melakukannya untuk beban kerja tertentu, seperti beban kerja komputasi performa tinggi (HPC).

Pertimbangan-pertimbangan

- Anda tidak dapat mengubah jumlah thread per inti untuk instance T2, C7a, M7a, R7a, dan Apple silicon Mac, dan instance berdasarkan prosesor Graviton. AWS
- Jumlah instance yang dapat Anda jalankan didasarkan pada v default CPUs untuk jenis instance yang digunakan. Bagaimana kami menghitung v yang CPUs dikonsumsi oleh sebuah instance tidak terpengaruh dengan mengubah opsi CPU-nya.

Harga

Tidak ada biaya tambahan untuk menentukan opsi CPU. Untuk instans EC2 yang diluncurkan dari AMI Windows dan SQL Server yang disertakan lisensi, Anda dapat menyesuaikan opsi CPU untuk memanfaatkan fitur EC2 Optimize CPU untuk membayar biaya lisensi berdasarkan jumlah vCPU yang dikonfigurasi untuk instans Anda. Untuk instans EC2 lainnya, Anda dikenakan biaya yang sama seperti instans yang diluncurkan dengan opsi CPU default.

Daftar Isi

- Aturan untuk menentukan opsi CPU untuk instans Amazon EC2
- Opsi CPU yang didukung untuk jenis instans Amazon EC2
- Tentukan opsi CPU untuk instans Amazon EC2
- Melihat utas dan inti CPU untuk instans Amazon EC2
- Optimalkan CPUs untuk instance yang Termasuk Lisensi

Aturan untuk menentukan opsi CPU untuk instans Amazon EC2

Untuk menentukan opsi CPU untuk instans Anda, perhatikan aturan berikut:

- Anda tidak dapat menentukan opsi CPU untuk instans bare metal.
- Anda dapat menentukan opsi CPU selama dan setelah peluncuran instance.
- Untuk mengonfigurasi opsi CPU, Anda harus menentukan jumlah inti CPU dan utas per inti dalam permintaan. Untuk contoh permintaan, lihat Tentukan opsi CPU untuk instans Amazon EC2.
- Jumlah v CPUs untuk contoh adalah jumlah core CPU dikalikan dengan thread per core. Untuk menentukan jumlah kustom vCPUs, Anda harus menentukan jumlah inti CPU dan utas per inti yang valid untuk jenis instance. Anda tidak dapat melebihi jumlah default v CPUs untuk instance. Untuk informasi selengkapnya, lihat Opsi CPU yang didukung untuk jenis instans Amazon EC2.

- Untuk menonaktifkan multithreading simultan (SMT), juga disebut sebagai hyper-threading, tentukan satu utas per inti.
- Di konsol, saat Anda mengubah jenis instans dari instans yang ada, Amazon EC2 menerapkan pengaturan opsi CPU dari instans yang ada ke instans baru, jika memungkinkan. Jika jenis instans baru tidak mendukung pengaturan tersebut, opsi CPU disetel ulang ke Gunakan opsi CPU default. Opsi ini menggunakan nomor default v CPUs untuk jenis instance baru.

  Untuk memperbarui pengaturan untuk instance baru, pilih Tentukan opsi CPU di bawah Detail lanjutan dalam tampilan Ubah jenis instans.
- Opsi CPU yang ditentukan tidak akan berubah setelah Anda menghentikan, memulai, atau me-reboot sebuah instans.
- Jika Anda menggunakan Instans Cadangan, diskon mungkin tidak diterapkan saat Anda mengonfigurasi Optimalkan CPUs untuk instans yang diluncurkan dari Windows yang disertakan lisensi AMIs di akun pembayar yang sama. Kami menyarankan Anda menggunakan Savings Plans untuk mengurangi biaya lisensi berbasis VCPU dan memberikan penghematan yang sebanding pada biaya komputasi Anda.
- Untuk menghemat biaya lisensi untuk instance yang diluncurkan dari Windows dan SQL Server yang disertakan lisensi AMIs, Anda harus mengonfigurasi minimal empat v. CPUs Jika Anda mengonfigurasi kurang dari empat vCPUs, penagihan default diterapkan.
- Optimalkan CPUs untuk instans Termasuk Lisensi tidak didukung pada jenis instans T3.

Opsi CPU yang didukung untuk jenis instans Amazon EC2

Tabel berikut mencantumkan tipe instans yang mendukung penentuan opsi CPU.

Daftar Isi

- Instans tujuan umum
- Instans komputasi yang dioptimalkan
- Instans memori yang dioptimalkan
- Instans penyimpanan yang dioptimalkan
- Instans komputasi terakselerasi
- Instans komputasi performa tinggi

Instans tujuan umum

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6idn.12x large	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16x large	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24x large	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8a.medium	1	1	1	1	1
m8a.large	2	2	1	1, 2	1
m8a.xlarge	4	4	1	1, 2, 3, 4	1
m8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
m8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m8azn.medium	1	1	1	1	1
m8azn.large	2	2	1	1, 2	1
m8azn.xlarge	4	4	1	1, 2, 3, 4	1
m8azn.3xlarge	12	12	1	1, 2, 4, 6, 8, 10, 12	1
m8azn.6xlarge	24	24	1	1, 2, 3, 4, 8, 12, 16, 20, 24	1
m8azn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48	1
m8azn.24xlarge	96	96	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96	1
m8g.large	2	2	1	1, 2	1
m8g.xlarge	4	4	1	1, 2, 3, 4	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gb.large	2	2	1	1, 2	1
m8gb.xlarge	4	4	1	1, 2, 3, 4	1
m8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gd.large	2	2	1	1, 2	1
m8gd.xlarge	4	4	1	1, 2, 3, 4	1
m8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gn.large	2	2	1	1, 2	1
m8gn.xlarge	4	4	1	1, 2, 3, 4	1
m8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8i.large	2	1	2	1	1, 2
m8i.xlarge	4	2	2	1, 2	1, 2
m8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
m8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8id.large	2	1	2	1	1, 2
m8id.xlarge	4	2	2	1, 2	1, 2
m8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8i-flex.large	2	1	2	1	1, 2
m8i-flex.xlarge	4	2	2	1, 2	1, 2
m8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
m8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
t3.nano	2	1	2	1	1, 2
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
t3a.micro	2	1	2	1	1, 2
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instans komputasi yang dioptimalkan

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8a.medium	1	1	1	1	1
c8a.large	2	2	1	1, 2	1
c8a.xlarge	4	4	1	1, 2, 3, 4	1
c8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
c8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c8g.large	2	2	1	1, 2	1
c8g.xlarge	4	4	1	1, 2, 3, 4	1
c8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gb.large	2	2	1	1, 2	1
c8gb.xlarge	4	4	1	1, 2, 3, 4	1
c8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gd.large	2	2	1	1, 2	1
c8gd.xlarge	4	4	1	1, 2, 3, 4	1
c8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gn.large	2	2	1	1, 2	1
c8gn.xlarge	4	4	1	1, 2, 3, 4	1
c8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8i.large	2	1	2	1	1, 2
c8i.xlarge	4	2	2	1, 2	1, 2
c8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
c8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c8id.large	2	1	2	1	1, 2
c8id.xlarge	4	2	2	1, 2	1, 2
c8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c8i-flex.large	2	1	2	1	1, 2
c8i-flex.xlarge	4	2	2	1, 2	1, 2
c8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
c8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instans memori yang dioptimalkan

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6idn.12x large	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16x large	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6idn.24x large	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8a.medium	1	1	1	1	1
r8a.large	2	2	1	1, 2	1
r8a.xlarge	4	4	1	1, 2, 3, 4	1
r8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r8g.large	2	2	1	1, 2	1
r8g.xlarge	4	4	1	1, 2, 3, 4	1
r8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gb.large	2	2	1	1, 2	1
r8gb.xlarge	4	4	1	1, 2, 3, 4	1
r8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gd.large	2	2	1	1, 2	1
r8gd.xlarge	4	4	1	1, 2, 3, 4	1
r8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gn.large	2	2	1	1, 2	1
r8gn.xlarge	4	4	1	1, 2, 3, 4	1
r8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8i.large	2	1	2	1	1, 2
r8i.xlarge	4	2	2	1, 2	1, 2
r8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
r8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8id.large	2	1	2	1	1, 2
r8id.xlarge	4	2	2	1, 2	1, 2
r8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8i-flex.large	2	1	2	1	1, 2
r8i-flex.xlarge	4	2	2	1, 2	1, 2
r8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
r8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
u-3tb1.56xlarge	224	112	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u-6tb1.56xlarge	224	224	1	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1
u-6tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u-9tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-12tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u-18tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-24tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u7i-6tb.112xlarge	448	224	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u7i-8tb.112xlarge	448	224	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
u7inh-32tb.480xlarge	1920	960	2	32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, 256, 272, 288, 304, 320, 336, 352, 368, 384, 400, 416, 432, 448, 464, 480, 496, 512, 528, 544, 560, 576, 576, 592, 608, 624, 640, 656, 672, 688, 704, 720, 736, 752, 768, 784, 800, 816, 832, 848, 864, 880, 896, 912, 928, 944, 960	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x8g.large	2	2	1	1, 2	1
x8g.xlarge	4	4	1	1, 2, 3, 4	1
x8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
x8aedz.large	2	2	1	1, 2	1
x8aedz.xlarge	4	4	1	1, 2, 3, 4	1
x8aedz.3xlarge	12	12	1	1, 2, 4, 6, 8, 10, 12	1
x8aedz.6xlarge	24	24	1	1, 2, 3, 4, 8, 12, 16, 20, 24	1
x8aedz.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48	1
x8aedz.24xlarge	96	96	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96	1
x8i.large	2	1	2	1	1, 2
x8i.xlarge	4	2	2	1, 2	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
x8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
x8i.64xlarge	256	128	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128	1, 2
x8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
z1d.large	2	1	2	1	1, 2
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Instans penyimpanan yang dioptimalkan

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
i7i.large	2	1	2	1	1, 2
i7i.xlarge	4	2	2	1, 2	1, 2
i7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
i7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
i7ie.large	2	1	2	1	1, 2
i7ie.xlarge	4	2	2	1, 2	1, 2
i7ie.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i7ie.3xlarge	12	6	2	1, 2, 3, 4, 5, 6	1, 2
i7ie.6xlarge	24	12	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i7ie.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i7ie.18xlarge	72	36	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i7ie.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
i7ie.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
i8g.large	2	2	1	1, 2	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8g.xlarge	4	4	1	1, 2, 3, 4	1
i8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
i8ge.large	2	2	1	1, 2	1
i8ge.xlarge	4	4	1	1, 2, 3, 4	1
i8ge.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i8ge.3xlarge	12	12	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1
i8ge.6xlarge	24	24	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8ge.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8ge.18xlarge	72	72	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8ge.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
i8ge.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instans komputasi terakselerasi

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
f2.6xlarge	24	12	2	1, 2, 3, 6, 9, 12	1, 2
f2.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
f2.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6e.xlarge	4	2	2	1, 2	1, 2
g6e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6e.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g6e.12xlarge	48	24	2	3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6e.16xlarge	64	32	2	4, 8, 12, 16, 20, 24, 28, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
g6e.24xlarge	96	48	2	6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6f.large	2	1	2	1	1, 2
g6f.xlarge	4	2	2	1, 2	1, 2
g6f.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6f.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
gr6f.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g7e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g7e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
g7e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g7e.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
g7e.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
g7e.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
p5e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
p5en.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
p6-b200.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
p6-b300.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
p6e-gb200.36xlarge	144	144	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98,	1

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
				99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136 , 137, 138, 139, 140, 141, 142, 143, 144	
`trn1.2xlarge`	8	4	2	2, 4	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn2.3xlarge	12	6	2	1, 2, 3, 4, 5, 6	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
trn2.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
trn2u.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

Instans komputasi performa tinggi

Tipe instans	Default v CPUs	Inti CPU default	Thread default per inti	Inti CPU yang valid	Thread valid per inti
hpc6id.32xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1
hpc8a.96xlarge	192	192	1	24, 48, 72, 96, 120, 144, 168, 192	1

Tentukan opsi CPU untuk instans Amazon EC2

Anda dapat menentukan opsi CPU selama atau setelah peluncuran instance.

Tugas

- Nonaktifkan multithreading simultan
- Tentukan nomor kustom v CPUs saat peluncuran
- Tentukan nomor kustom v CPUs dalam template peluncuran
- Ubah opsi CPU untuk instans EC2 Anda

Nonaktifkan multithreading simultan

Untuk menonaktifkan multithreading simultan (SMT), juga dikenal sebagai hyper-threading, tentukan 1 utas per inti.

Console

Untuk menonaktifkan SMT selama peluncuran instans

1. Ikuti prosedur Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol dan konfigurasikan instans Anda sesuai kebutuhan.
2. Perluas Detail lanjutan, dan pilih kotak centang Tentukan opsi CPU.
3. Untuk Jumlah inti, pilih jumlah inti CPU yang diperlukan. Dalam contoh ini, untuk menentukan jumlah inti CPU default untuk instans `r5.4xlarge`, pilih 8.
4. Untuk menonaktifkan SMT, untuk Threads per core, pilih 1.
5. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

AWS CLI

Untuk menonaktifkan SMT selama peluncuran instans

Gunakan AWS CLI perintah run-instance dan tentukan nilai 1 for `ThreadsPerCore` untuk parameter. `--cpu-options` Untuk `CoreCount`, tentukan jumlah inti CPU. Dalam contoh ini, untuk menentukan jumlah inti CPU default untuk instans `r7i.4xlarge`, tentukan nilai 8.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name my-key-pair
```

PowerShell

Untuk menonaktifkan SMT selama peluncuran instans

Gunakan New-EC2Instanceperintah dan tentukan nilai 1 for `ThreadsPerCore` untuk `-CpuOptions` parameter. Untuk `CoreCount`, tentukan jumlah inti CPU. Dalam contoh ini, untuk menentukan jumlah inti CPU default untuk instans `r7i.4xlarge`, tentukan nilai 8.

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=8; ThreadsPerCore=1} `
    -KeyName 'my-key-pair'
```

> **Note**
>
> Untuk menonaktifkan SMT untuk instance yang ada, ikuti proses yang ditunjukkanUbah opsi CPU untuk instans EC2 Anda, dan ubah jumlah utas yang dijalankan per inti menjadi1.

Tentukan nomor kustom v CPUs saat peluncuran

Anda dapat menyesuaikan jumlah inti CPU dan utas per inti saat meluncurkan instance dari konsol EC2 atau AWS CLI. Contoh di bagian ini menggunakan tipe `r5.4xlarge` instance, yang memiliki pengaturan default berikut:

- Inti CPU: 8
- Utas per inti: 2

Instans diluncurkan dengan jumlah maksimum v yang CPUs tersedia untuk jenis instans secara default. Untuk jenis instance ini, yaitu 16 total v CPUs (masing-masing 8 core menjalankan 2 thread). Untuk informasi selengkapnya tentang jenis instance ini, lihatInstans memori yang dioptimalkan.

Contoh berikut meluncurkan sebuah `r5.4xlarge` instance dengan 4 vCPUs.

Console

Untuk menentukan nomor kustom v CPUs selama peluncuran instance

1. Ikuti prosedur Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol dan konfigurasikan instans Anda sesuai kebutuhan.
2. Perluas Detail lanjutan, dan pilih kotak centang Tentukan opsi CPU.
3. Untuk mendapatkan 4 vCPUs, tentukan 2 core CPU dan 2 thread per core, sebagai berikut:
   - Untuk jumlah inti, pilih 2.
   - Untuk Thread per inti, pilih 2.
4. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

AWS CLI

Untuk menentukan nomor kustom v CPUs selama peluncuran instance

Gunakan AWS CLI perintah run-instance dan tentukan jumlah core CPU dan jumlah thread dalam parameter. `--cpu-options` Anda dapat menentukan 2 core CPU dan 2 thread per core untuk mendapatkan 4 vCPUs.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name my-key-pair
```

Atau, tentukan 4 core CPU dan 1 thread per core (nonaktifkan SMT) untuk mendapatkan 4 vCPUs:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name my-key-pair
```

PowerShell

Untuk menentukan nomor kustom v CPUs selama peluncuran instance

Gunakan New-EC2Instanceperintah dan tentukan jumlah inti CPU dan jumlah utas dalam `-CpuOptions` parameter. Anda dapat menentukan 2 core CPU dan 2 thread per core untuk mendapatkan 4 vCPUs.

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=2; ThreadsPerCore=2} `
    -KeyName 'my-key-pair'
```

Atau, tentukan 4 core CPU dan 1 thread per core (nonaktifkan SMT) untuk mendapatkan 4 vCPUs:

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=4; ThreadsPerCore=1} `
    -KeyName 'my-key-pair'
```

Tentukan nomor kustom v CPUs dalam template peluncuran

Anda dapat menyesuaikan jumlah inti CPU dan thread per inti untuk instans dalam templat peluncuran. Contoh di bagian ini menggunakan tipe `r5.4xlarge` instance, yang memiliki pengaturan default berikut:

- Inti CPU: 8
- Utas per inti: 2

Instans diluncurkan dengan jumlah maksimum v yang CPUs tersedia untuk jenis instans secara default. Untuk jenis instance ini, yaitu 16 total v CPUs (masing-masing 8 core menjalankan 2 thread). Untuk informasi selengkapnya tentang jenis instance ini, lihatInstans memori yang dioptimalkan.

Contoh berikut membuat template peluncuran yang menentukan konfigurasi untuk sebuah `r5.4xlarge` instance dengan 4 vCPUs.

Console

Untuk menentukan nomor kustom v CPUs dalam template peluncuran

1. Ikuti prosedur Buat template peluncuran dengan menentukan parameter dan konfigurasikan templat peluncuran Anda sesuai kebutuhan.
2. Perluas Detail lanjutan, dan pilih kotak centang Tentukan opsi CPU.
3. Untuk mendapatkan 4 vCPUs, tentukan 2 core CPU dan 2 thread per core, sebagai berikut:
   - Untuk jumlah inti, pilih 2.
   - Untuk Thread per inti, pilih 2.
4. Di panel Ringkasan, tinjau konfigurasi instans Anda dan pilih Buat templat peluncuran. Untuk informasi selengkapnya, lihat Simpan parameter peluncuran instans di templat peluncuran Amazon EC2.

AWS CLI

Untuk menentukan nomor kustom v CPUs dalam template peluncuran

Gunakan create-launch-template AWS CLI perintah dan tentukan jumlah inti CPU dan jumlah utas dalam `CpuOptions` parameter. Anda dapat menentukan 2 core CPU dan 2 thread per core untuk mendapatkan 4 vCPUs.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
    --launch-template-data file://template-data.json
```

Berikut ini adalah contoh file JSON yang berisi data templat peluncuran, yang mencakup opsi CPU, untuk konfigurasi instans untuk contoh ini.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
```

```
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

Atau, tentukan 4 core CPU dan 1 thread per core (nonaktifkan SMT) untuk mendapatkan 4 vCPUs:

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":1
    }
}
```

PowerShell

Untuk menentukan nomor kustom v CPUs dalam template peluncuran

Gunakan New-EC2LaunchTemplate.

```
New-EC2LaunchTemplate `
    -LaunchTemplateName 'TemplateForCPUOptions' `
    -VersionDescription 'CPUOptionsVersion1' `
    -LaunchTemplateData (Get-Content -Path 'template-data.json' | ConvertFrom-Json)
```

Ubah opsi CPU untuk instans EC2 Anda

Karena kebutuhan Anda berubah seiring waktu, Anda mungkin ingin mengubah konfigurasi opsi CPU untuk instance yang ada. Setiap thread yang berjalan pada instance Anda dikenal sebagai CPU virtual (vCPU). Anda dapat mengubah jumlah vCPU yang berjalan untuk instans yang ada di konsol AWS CLI Amazon EC2, API, atau. SDKs Status instance harus `Stopped` sebelum Anda dapat membuat perubahan ini.

Untuk melihat langkah konsol atau baris perintah, pilih tab yang cocok dengan lingkungan Anda. Untuk informasi permintaan dan respons API, lihat ModifyInstanceCpuOptionsdi Referensi API Amazon EC2.

Console

Ikuti prosedur ini untuk mengubah jumlah v aktif CPUs untuk instance Anda dari Konsol Manajemen AWS.

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans. Ini membuka daftar instance yang ditentukan untuk saat ini AWS Region.
3. Pilih instance dari daftar Instances. Atau, Anda dapat memilih link instance untuk membuka halaman detail instance.
4. Jika instance berjalan, Anda harus menghentikannya sebelum melanjutkan. Pilih Stop instance dari menu status Instance.
5. Untuk mengubah konfigurasi vCPU, pilih Ubah opsi CPU dari Pengaturan instans di menu Tindakan. Ini membuka halaman opsi Ubah CPU.
6. Pilih salah satu opsi CPU berikut untuk mengubah konfigurasi instans Anda.

   Gunakan opsi CPU default

   Opsi ini me-reset instance Anda ke nomor default v CPUs untuk jenis instance. Defaultnya adalah menjalankan semua utas untuk semua inti CPU.

Tentukan opsi CPU

Opsi ini memungkinkan konfigurasi jumlah v CPUs yang berjalan pada instance Anda.

7. Jika Anda memilih Tentukan opsi CPU, CPUs bidang Aktif v akan ditampilkan.

   - Gunakan pemilih pertama untuk mengonfigurasi jumlah utas untuk setiap inti CPU. Untuk menonaktifkan multithreading simultan, pilih. 1
   - Gunakan pemilih kedua untuk mengonfigurasi jumlah CPUs yang dijalankan pada instance Anda.

   Bidang berikut diperbarui secara dinamis saat Anda membuat perubahan pada pemilih opsi CPU.

   - Aktif v CPUs: Jumlah inti CPU dikalikan dengan utas per inti, berdasarkan pilihan yang Anda buat. Misalnya, jika Anda memilih 2 utas dan 4 inti, itu akan sama dengan 8 vCPUs.
   - Total v CPUs: Jumlah maksimum v CPUs untuk tipe instance. Misalnya, untuk tipe `m6i.4xlarge` instance, ini adalah 16 v CPUs (8 core masing-masing menjalankan 2 thread).
8. Untuk menerapkan pembaruan Anda, pilih Ubah.

AWS CLI

Ikuti prosedur ini untuk mengubah jumlah v aktif CPUs untuk instance Anda dari AWS CLI.

Gunakan modify-instance-cpu-optionsperintah dan tentukan jumlah inti CPU yang berjalan di `--core-count` parameter, dan jumlah utas yang berjalan per inti dalam `--threads-per-core` parameter.

Contoh berikut menunjukkan dua kemungkinan konfigurasi pada tipe `m6i.4xlarge` instance untuk menjalankan 8 v CPUs pada instance yang ditentukan. Default untuk jenis instance ini adalah 16 v CPUs (masing-masing 8 core menjalankan 2 thread).

Contoh 1: Jalankan 4 core CPU dengan 2 thread per core, dengan total 8 vCPU.

```
aws ec2 modify-instance-cpu-options \
    --instance-id i-1234567890abcdef0 \

    --core-count=4 \
```

```
    --threads-per-core=2
```

Contoh 2: Nonaktifkan multi-threading simultan dengan mengubah jumlah utas yang dijalankan per inti menjadi. 1 Konfigurasi yang dihasilkan juga menjalankan total 8 v CPUs (8 core CPU dengan 1 thread per core).

```
aws ec2 modify-instance-cpu-options \
    --instance-id 1234567890abcdef0 \
    --core-count=8 \
    --threads-per-core=1
```

PowerShell

Untuk mengubah jumlah v aktif CPUs untuk sebuah instance

Gunakan Edit-EC2InstanceCpuOptioncmdlet dan tentukan jumlah inti CPU yang berjalan di `-CoreCount` parameter, dan jumlah utas yang dijalankan per inti dalam parameter. `ThreadsPerCore`

Contoh 1: Jalankan 4 core CPU dengan 2 thread per core, dengan total 8 vCPU.

```
Edit-EC2InstanceCpuOption `
    -InstanceId 'i-1234567890abcdef0' `
    -CoreCount 4 `
    -ThreadsPerCore 2
```

Contoh 2: Nonaktifkan multi-threading simultan dengan mengubah jumlah utas yang dijalankan per inti menjadi. 1 Konfigurasi yang dihasilkan juga menjalankan total 8 v CPUs (8 core CPU dengan 1 thread per core).

```
Edit-EC2InstanceCpuOption `
    -InstanceId 'i-1234567890abcdef0' `
    -CoreCount 8 `
    -ThreadsPerCore 1
```

Melihat utas dan inti CPU untuk instans Amazon EC2

Anda dapat melihat opsi CPU untuk instance yang ada dengan menjelaskan instance.

Console

Untuk melihat opsi CPU untuk sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi kiri, pilih Instans, kemudian pilih instans.
3. Pada tab Detail, di bawah Host dan grup penempatan, temukan Jumlah v CPUs.

AWS CLI

Untuk melihat opsi CPU untuk sebuah instance

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].CpuOptions
```

Berikut ini adalah output contoh. `CoreCount`Bidang menunjukkan jumlah inti untuk instance. Bidang `ThreadsPerCore` menunjukkan jumlah thread per inti.

```
[
    {
        "CoreCount": 24,
        "ThreadsPerCore": 2
    },
]
```

PowerShell

Untuk melihat opsi CPU untuk sebuah instance

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -InstanceId 'i-1234567890abcdef0').Instances.CpuOptions
```

Berikut ini adalah output contoh.

```
AmdSevSnp CoreCount ThreadsPerCore
```

```
--------- --------- --------------
          24        2
```

Atau, untuk melihat informasi CPU, Anda dapat terhubung ke instans Anda dan menggunakan salah satu alat sistem berikut:

- Windows `Task Manager` pada instance Windows Anda
- lscpuPerintah pada instance Linux Anda

Anda dapat menggunakan AWS Config untuk merekam, menilai, mengaudit, dan mengevaluasi perubahan konfigurasi untuk instance, termasuk instance yang dihentikan. Untuk informasi selengkapnya, lihat Memulai AWS Config di Panduan Pengguna AWS Config .

Optimalkan CPUs untuk instance yang Termasuk Lisensi

Beban kerja seperti Microsoft SQL Server sering membutuhkan tingkat memori dan IOPS yang tinggi tetapi jumlah vCPU yang rendah. AWS menyediakan serangkaian jenis instans yang luas yang dapat mencakup sebagian besar kebutuhan infrastruktur Anda. Namun, untuk mengurangi biaya lisensi berbasis VCPU untuk Windows dan Microsoft SQL Server, Anda dapat menyesuaikan jumlah vCPU yang berjalan pada instans EC2 Anda sambil mempertahankan memori, penyimpanan, dan spesifikasi jaringan yang sama. Pendekatan ini dapat menghemat biaya lisensi berbasis VCPU untuk beban kerja yang termasuk lisensi dan (BYOL). Bring-Your-Own-License Anda dapat menentukan opsi CPU saat meluncurkan atau memodifikasi instans menggunakan konsol atau Amazon EC2 API. Untuk petunjuk, lihat Tentukan opsi CPU untuk instans Amazon EC2.

Untuk informasi selengkapnya, lihat posting blog ini tentang praktik terbaik CPUs untuk mengoptimalkan beban kerja SQL Server.

Jenis lisensi yang didukung

Optimize CPUs mendukung penagihan berdasarkan jumlah aktif CPUs untuk jenis konfigurasi lisensi berikut untuk instance yang diluncurkan dari AMI yang disertakan lisensi. Untuk informasi selengkapnya tentang jenis lisensi, lihatBidang informasi penagihan AMI.

Penagihan instans AMI yang disertakan lisensi

Lisensi disertakan	Operasi penggunaan	Harga per jam vCPU

Lisensi disertakan	Operasi penggunaan	Harga per jam vCPU
Windows Server	RunInstances:0002	$0,046
Windows Server dengan SQL Server Enterprise	RunInstances:0102	$0,421
Windows Server dengan Standar SQL Server	RunInstances:0006	$0,166
Windows Server dengan SQL Server Web	RunInstances:0202	$0,063

Opsi pembelian yang didukung

Optimize CPUs mendukung opsi pembelian berikut untuk instance yang disertakan lisensi:

- Sesuai Permintaan
- Savings Plans

> **Warning**
>
> Jika Anda menggunakan Instans Cadangan, diskon mungkin tidak diterapkan saat Anda mengonfigurasi Optimalkan CPUs untuk instans yang disertakan lisensi di akun pembayar yang sama. Kami menyarankan Anda menggunakan Savings Plans untuk mengurangi biaya lisensi berbasis VCPU dan memberikan penghematan yang sebanding pada biaya komputasi Anda.
>
> Akun yang menggunakan Instans Optimalkan CPUs dan Cadangan untuk Windows dan SQL Server pada jenis instans yang sama sebelum 15 Oktober 2025, ditambahkan ke daftar opt-out untuk mempertahankan pengalaman penagihan mereka saat ini. Untuk memanfaatkan penghematan lisensi CPU Optimalkan, hubungi AWS Dukungan Pusat untuk dihapus dari daftar opt-out.

Bagaimana Optimize CPUs bekerja untuk menghemat biaya lisensi

Contoh berikut membantu menggambarkan penghematan biaya yang dimungkinkan saat Anda mengonfigurasi penggunaan CPU Anda.

Contoh 1: Penagihan default Contoh ini menunjukkan instance r7i.8xlarge yang diluncurkan dari Windows dan SQL Server Enterprise AMI yang disertakan lisensi yang berjalan selama 100 jam dengan konfigurasi CPU default 32 v CPUs untuk jenis instans (3200 jam vCPU).

Tagihan menunjukkan satu item baris dengan tarif gabungan yang mencakup biaya penggunaan dan lisensi.

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 1** **Description**	**Usage Quantity**	**Total charges** **$1,558.88** **Amount in USD**
Elastic Compute Cloud		$1,558.88
|- US East (N. Virginia)		$1,558.88
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$1,558.88
| |- $15.5888 per On Demand Windows with SQL Server Enterprise r7i.8xlarge Instance Hour	100 Hrs	$1,558.88

Contoh 2: Optimalkan CPUs penagihan Contoh ini menunjukkan instance r7i.8xlarge yang diluncurkan dari AMI Windows dan SQL Server Enterprise yang disertakan lisensi. Untuk menghemat biaya lisensi, jumlah CPUs yang aktif dikurangi menjadi 16 vCPUs. Kemudian instance berjalan selama 100 jam dengan konfigurasi baru.

RUU tersebut menunjukkan dua item baris berikut.

Deskripsi penagihan: Elastic Compute Cloud

Item baris pertama menunjukkan biaya dasar instance Windows dan SQL Server yang berjalan selama 100 jam ($211.68).

Deskripsi penagihan: Amazon EC2 Optimalkan Lisensi CPU Termasuk Biaya Pihak Ketiga

Item baris kedua mencakup biaya lisensi berdasarkan jumlah v CPUs yang aktif untuk periode penagihan ($673,60).

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 2** **Description**	**Usage Quantity**	**Total charges** **$885.28** **Amount in USD**
Elastic Compute Cloud		$211.68
|- US East (N. Virginia)		$211.68
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$211.68
| |- $2.1168 per On Demand Windows and SQL Server Enterprise without licenses r7i.8xlarge Instance Hr	100 Hrs	$211.68
Amazon EC2 Optimize CPU License Included Third Party Fees		$673.60
|- US East (N. Virginia)		$673.60
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$673.60
| |- $0.421 per vCPU-Hour of On Demand Windows with SQL Server licenses on r7i Instance	1,600 vCPU-Hrs	$673.60

Contoh 3: Optimalkan CPUs penagihan dengan Savings Plans Contoh ini menunjukkan instans r7i.8xlarge yang diluncurkan dari Windows dan SQL Server Enterprise AMI yang disertakan lisensi. Untuk menghemat biaya lisensi, jumlah CPUs yang aktif dikurangi menjadi 16 vCPUs. Kemudian instance berjalan selama 100 jam dengan konfigurasi baru.

Satu tahun No Upfront Compute Savings Plan dengan komitmen $1,60/jam (bulat) memberikan penghematan biaya lebih lanjut yang mengurangi biaya dasar instans Windows dan SQL Server. Komitmen Savings Plan mencakup penggunaan 100 jam penuh dari instans r7i.8xlarge untuk tarif Savings Plans sebesar $1.53362/jam.

RUU menunjukkan item baris berikut.

Deskripsi penagihan: Savings Plans untuk penggunaan Compute

Item baris pertama menunjukkan komitmen Savings Plan untuk penggunaan 100 jam penuh ($160.00).

Deskripsi penagihan: Elastic Compute Cloud

Item baris kedua berisi dua entri. Entri pertama menunjukkan berapa biaya dasar instance Windows dan SQL Server yang berjalan selama 100 jam tanpa Savings Plan ($211.68). Entri kedua menunjukkan bahwa biaya dasar penuh ditanggung oleh Compute Savings Plan (-$211.68), yang menghasilkan biaya bersih nol untuk item baris ini.

Deskripsi penagihan: Amazon EC2 Optimalkan Lisensi CPU Termasuk Biaya Pihak Ketiga

Item baris ketiga mencakup biaya lisensi berdasarkan jumlah v CPUs yang aktif untuk periode penagihan ($673,60).

For illustration purposes only

Amazon Web Services, Inc. charges by service		**Total charges**
Total services: 3		**$833.60**
Description	**Usage Quantity**	**Amount in USD**
Savings Plans for Compute usage		$160.00
|- Any		$160.00
|- Compute Savings Plans		$160.00
| |- 1 year No Upfront Compute Savings Plan	100 Hrs	$160.00
Elastic Compute Cloud		$0.00
|- US East (N. Virginia)		$0.00
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$0.00
| |- $2.1168 per On Demand Windows and SQL Server Enterprise without licenses r7i.8xlarge Instance Hr	100 Hrs	$211.68
| |- r7i.8xlarge Windows with SQL Server Enterprise without licenses instance usage covered by CSP	100 Hrs	($211.68)
Amazon EC2 Optimize CPU License Included Third Party Fees		$673.60
|- US East (N. Virginia)		$673.60
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$673.60
| |- $0.421 per vCPU-Hour of On Demand Windows with SQL Server licenses on r7i Instance	1,600 vCPU-Hrs	$673.60

AMD SEV-SNP untuk instans Amazon EC2

AMD Secure Encrypted Virtualization-Secure Nested Paging (AMD SEV-SNP) adalah fitur CPU yang menyediakan properti berikut:

- Pengesahan — AMD SEV-SNP memungkinkan Anda untuk mengambil laporan pengesahan yang ditandatangani yang berisi ukuran kriptografi yang dapat digunakan untuk memvalidasi status dan identitas instans, dan bahwa instans tersebut berjalan pada perangkat keras AMD asli. Untuk informasi selengkapnya, lihat Membuktikan EC2 instans Amazon dengan AMD SEV-SNP.
- Enkripsi memori — Dimulai dengan prosesor AMD EPYC (Milan), AWS Graviton2, dan Intel Xeon Scalable (Ice Lake), memori instance selalu dienkripsi. Instans yang diaktifkan untuk AMD SEV-SNP menggunakan kunci khusus instans untuk enkripsi memori mereka.

Daftar Isi

- Konsep dan terminologi
- Persyaratan
- Pertimbangan-pertimbangan
- Harga
- Temukan jenis EC2 instans yang mendukung AMD SEV-SNP
- Aktifkan AMD SEV-SNP untuk sebuah instance EC2
- Membuktikan EC2 instans Amazon dengan AMD SEV-SNP

Konsep dan terminologi

Sebelum Anda mulai menggunakan AMD SEV-SNP, pastikan Anda terbiasa dengan konsep dan terminologi berikut.

Laporan pengesahan AMD SEV-SNP

Laporan pengesahan AMD SEV-SNP adalah dokumen yang dapat diminta oleh instans dari CPU. Laporan pengesahan AMD SEV-SNP dapat digunakan untuk memvalidasi status dan identitas suatu instans, dan untuk memverifikasi bahwa itu berjalan di lingkungan AMD yang disetujui. Laporan tersebut mencakup pengukuran peluncuran, yang merupakan hash kriptografi dari status boot awal sebuah instance, termasuk isi memori instance awal dan status awal v. CPUs Laporan pengesahan AMD SEV-SNP ditandatangani dengan tanda tangan VLEK yang kembali ke akar kepercayaan AMD.

VLEK

Versioned Loaded Endorsement Key (VLEK) adalah kunci penandatanganan berversi yang disertifikasi oleh AMD dan digunakan oleh CPU AMD untuk menandatangani laporan pengesahan AMD SEV-SNP. Tanda tangan VLEK dapat divalidasi menggunakan sertifikat yang disediakan oleh AMD.

Biner OVMF

Open Virtual Machine Firmware (OVMF) adalah kode boot awal yang digunakan untuk menyediakan lingkungan UEFI untuk instans. Kode boot awal dijalankan sebelum kode di AMI di-boot. OVMF juga menemukan dan menjalankan boot loader yang disediakan di AMI. Untuk informasi selengkapnya, lihat Repositori OVMF.

Persyaratan

Untuk menggunakan AMD SEV-SNP, Anda harus melakukan hal berikut:

- Gunakan salah satu dari tipe instans yang didukung berikut:
  - Tujuan umum: `m6a.large` `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Komputasi yang dioptimalkan: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Memori dioptimalkan: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Luncurkan instans Anda di didukung AWS Region. Saat ini, hanya AS Timur (Ohio) dan Eropa (Irlandia) yang didukung.

- Gunakan AMI dengan mode boot `uefi` atau `uefi-preferred` dan sistem operasi yang mendukung AMD SEV-SNP. Untuk informasi lebih lanjut tentang dukungan AMD SEV-SNP pada sistem operasi Anda, lihat dokumentasi sistem operasi masing-masing. Untuk AWS, AMD SEV-SNP didukung pada AL2 023, RHEL 9.3, SLES 15 SP4, dan Ubuntu 23.04 dan yang lebih baru.

Pertimbangan-pertimbangan

Anda hanya dapat mengaktifkan AMD SEV-SNP saat meluncurkan instans. Ketika AMD SEV-SNP diaktifkan untuk peluncuran instans Anda, aturan berikut berlaku.

- Setelah diaktifkan, AMD SEV-SNP tidak dapat dinonaktifkan. Itu tetap diaktifkan sepanjang siklus hidup instance.
- Anda hanya dapat mengubah jenis instans ke jenis instans lain yang mendukung AMD SEV-SNP.
- Hibernasi dan Nitro Enklave tidak didukung.
- Host Khusus tidak didukung.
- Jika host yang mendasari instans Anda dijadwalkan untuk pemeliharaan, Anda akan menerima pemberitahuan acara terjadwal 14 hari sebelum acara. Anda harus menghentikan atau memulai ulang instans secara manual untuk memindahkannya ke host baru.

Harga

Saat meluncurkan EC2 instans Amazon dengan AMD SEV-SNP diaktifkan, Anda akan dikenakan biaya penggunaan tambahan per jam yang setara dengan 10 persen tarif per jam Sesuai Permintaan dari jenis instans yang dipilih.

Biaya penggunaan AMD SEV-SNP ini merupakan biaya terpisah untuk penggunaan instans Amazon EC2 Anda. Instans Terpesan, Savings Plans, dan penggunaan sistem operasi tidak memengaruhi biaya ini.

Jika Anda mengonfigurasi Instans Spot untuk diluncurkan dengan AMD SEV-SNP diaktifkan, Anda akan dikenakan biaya penggunaan tambahan per jam yang setara dengan 10 persen tarif per jam Sesuai Permintaan dari jenis instans yang dipilih. Jika strategi alokasi menggunakan harga sebagai masukan, Armada Spot tidak termasuk biaya tambahan ini; hanya harga Spot yang digunakan.

Temukan jenis EC2 instans yang mendukung AMD SEV-SNP

Anda dapat menemukan jenis instance yang mendukung AMD SEV-SNP. EC2 Konsol Amazon tidak menampilkan informasi ini untuk jenis instans.

AWS CLI

Untuk menemukan jenis instance yang mendukung AMD SEV-SNP

Gunakan perintah describe-instance-types berikut ini.

```
aws ec2 describe-instance-types \
    --filters Name=processor-info.supported-features,Values=amd-sev-snp \
    --query 'InstanceTypes[*].[InstanceType]' \
    --output text | sort
```

Berikut ini adalah output contoh.

```
c6a.12xlarge
c6a.16xlarge
c6a.2xlarge
c6a.4xlarge
c6a.8xlarge
c6a.large
c6a.xlarge
m6a.2xlarge
m6a.4xlarge
m6a.8xlarge
m6a.large
m6a.xlarge
r6a.2xlarge
r6a.4xlarge
r6a.large
r6a.xlarge
```

PowerShell

Untuk menemukan jenis instance yang mendukung AMD SEV-SNP

Gunakan Get-EC2InstanceTypecmdlet.

```
(Get-EC2InstanceType `
    -Filter @{Name="processor-info.supported-features"; Values="amd-sev-
snp"}).InstanceType.Value | Sort-Object
```

Berikut ini adalah output contoh.

```
c6a.12xlarge
c6a.16xlarge
c6a.2xlarge
c6a.4xlarge
c6a.8xlarge
c6a.large
c6a.xlarge
m6a.2xlarge
m6a.4xlarge
m6a.8xlarge
m6a.large
m6a.xlarge
r6a.2xlarge
r6a.4xlarge
r6a.large
r6a.xlarge
```

Aktifkan AMD SEV-SNP untuk sebuah instance EC2

Anda dapat meluncurkan instance dengan AMD SEV-SNP diaktifkan. Anda tidak dapat mengaktifkan AMD SEV-SNP setelah peluncuran.

Luncurkan instance dengan AMD SEV-SNP diaktifkan

Anda tidak dapat mengaktifkan AMD SEV-SNP menggunakan konsol Amazon. EC2

AWS CLI

Untuk meluncurkan instance dengan AMD SEV-SNP diaktifkan

Gunakan perintah run-instances dengan opsi `--cpu-options`. Untuk persyaratan tambahan, lihat persyaratan AMD SEV-SNP.

```
--cpu-options AmdSevSnp=enabled
```

PowerShell

Untuk meluncurkan instance dengan AMD SEV-SNP diaktifkan

Gunakan New-EC2Instancecmdlet dengan parameter. `-CpuOption`

```
-CpuOption @{AmdSevSnp="enabled"}
```

Periksa apakah sebuah EC2 instance diaktifkan untuk AMD SEV-SNP

Anda dapat menemukan instance yang diaktifkan untuk AMD SEV-SNP. EC2 Konsol Amazon tidak menampilkan informasi ini.

AWS CLI

Untuk memeriksa apakah AMD SEV-SNP diaktifkan untuk sebuah instance

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].CpuOptions
```

Berikut ini adalah output contoh. Jika tidak `AmdSevSnp` ada`CpuOptions`, maka AMD SEV-SNP dinonaktifkan.

```
[
    {
        "AmdSevSnp": "enabled",
        "CoreCount": 1,
        "ThreadsPerCore": 2
    }
]
```

PowerShell

Untuk memeriksa apakah AMD SEV-SNP diaktifkan untuk sebuah instance

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.CpuOptions
```

Berikut ini adalah output contoh. Jika nilai tidak `AmdSevSnp` ada, maka AMD SEV-SNP dinonaktifkan.

```
AmdSevSnp CoreCount ThreadsPerCore
--------- --------- --------------
enabled   1         2
```

AWS CloudTrail

Dalam AWS CloudTrail hal permintaan peluncuran instance, properti berikut menunjukkan bahwa AMD SEV-SNP diaktifkan untuk instance.

```
"cpuOptions": {"AmdSevSnp": "enabled"}
```

Membuktikan EC2 instans Amazon dengan AMD SEV-SNP

Pengesahan adalah proses yang memungkinkan instans Anda membuktikan status dan identitasnya. Setelah Anda mengaktifkan AMD SEV-SNP untuk instans Anda, Anda dapat meminta laporan pengesahan AMD SEV-SNP dari prosesor yang mendasarinya. Laporan pengesahan AMD SEV-SNP berisi hash kriptografi, yang disebut pengukuran peluncuran, dari konten memori tamu awal dan status vCPU awal. Laporan pengesahan ditandatangani dengan tanda tangan VLEK yang berantai kembali ke root kepercayaan AMD. Anda dapat menggunakan pengukuran peluncuran yang disertakan dalam laporan pengesahan untuk memvalidasi bahwa instans berjalan di lingkungan AMD asli dan untuk memvalidasi kode boot awal yang digunakan untuk meluncurkan instans.

Prasyarat

Luncurkan instance yang diaktifkan untuk AMD SEV-SNP. Untuk informasi selengkapnya, lihat Aktifkan AMD SEV-SNP untuk sebuah instance EC2.

Langkah-langkah

- Langkah 1: Dapatkan laporan pengesahan
- Langkah 2: Validasi tanda tangan laporan pengesahan

Langkah 1: Dapatkan laporan pengesahan

Pada langkah ini, Anda menginstal dan membangun `snpguest` utilitas, dan kemudian menggunakannya untuk meminta laporan pengesahan AMD SEV-SNP dan sertifikat.

1. Terhubung ke instans Anda.

2. Jalankan perintah berikut untuk membangun `snpguest` utilitas dari file snpguest repository.

```
$ git clone https://github.com/virtee/snpguest.git
$ cd snpguest
$ cargo build -r
$ cd target/release
```

3. Hasilkan permintaan untuk laporan pengesahan. Utilitas meminta laporan pengesahan dari host, dan menuliskannya ke file biner dengan data permintaan yang disediakan.

   Contoh berikut membuat string permintaan acak, dan menggunakannya sebagai file permintaan (`request-file.txt`). Ketika perintah mengembalikan laporan pengesahan itu disimpan di jalur file yang Anda tentukan ()`report.bin`. Dalam hal ini, utilitas menyimpan laporan di direktori saat ini.

```
$ ./snpguest report report.bin request-file.txt --random
```

4. Minta sertifikat dari memori host, dan simpan sebagai file PEM. Contoh berikut menyimpan file dalam direktori yang sama dengan `snpguest` utilitas. Jika sertifikat sudah ada di direktori yang ditentukan, sertifikat tersebut akan ditimpa.

```
$ ./snpguest certificates PEM ./
```

Langkah 2: Validasi tanda tangan laporan pengesahan

Laporan pengesahan ditandatangani dengan sertifikat, yang disebut Versioned Loaded Endorsement Key (VLEK), yang dikeluarkan oleh AMD untuk. AWS Pada langkah ini, Anda dapat memvalidasi bahwa sertifikat VLEK dikeluarkan oleh AMD, dan bahwa laporan pengesahan ditandatangani oleh sertifikat VLEK itu.

1. Unduh root sertifikat kepercayaan VLEK dari situs web resmi AMD ke direktori saat ini.

```
$ sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/Milan/
cert_chain -o ./cert_chain.pem
```

2. Gunakan `openssl` untuk memvalidasi bahwa sertifikat VLEK ditandatangani oleh root sertifikat kepercayaan AMD.

```
$ sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
```

Berikut ini adalah output contoh.

```
vlek.pem: OK
```

3. Gunakan pemanfaatan `snpguest` untuk memvalidasi bahwa laporan pengesahan ditandatangi oleh sertifikat VLEK.

```
$ ./snpguest verify attestation ./ report.bin
```

Berikut ini adalah output contoh.

```
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
VEK signed the Attestation Report!
```

Kontrol status prosesor untuk instans Amazon EC2 Linux

C-state mengontrol tingkat tidur yang dapat dimasuki inti saat menganggur. Status-C diberi nomor mulai dengan C0 (status paling dangkal di mana inti benar-benar terjaga dan menjalankan instruksi) hingga C6 (keadaan idle terdalam di mana inti dimatikan).

P-state mengontrol kinerja yang diinginkan (dalam frekuensi CPU) dari inti. Status-P diberi nomor mulai dari P0 (pengaturan performa tertinggi di mana inti diizinkan untuk menggunakan Intel Turbo Boost Technology untuk meningkatkan frekuensi jika memungkinkan), dan mereka beralih dari P1 (status-P yang meminta frekuensi acuan maksimum) ke P15 (frekuensi serendah mungkin).

> **Note**
>
> AWS Prosesor Graviton memiliki mode hemat daya bawaan dan beroperasi pada frekuensi tetap. Oleh karena itu, mereka tidak menyediakan kemampuan untuk sistem operasi untuk mengontrol status-C dan status-P.

Status-C dan Status-P

Jenis contoh berikut memberikan kemampuan untuk sistem operasi untuk mengontrol C-state dan P-state:

- Tujuan umum: `m4.10xlarge` | `m4.16xlarge`
- Komputasi dioptimalkan: `c4.8xlarge`
- Memori dioptimalkan: `r4.8xlarge` `r4.16xlarge` `x1.16xlarge` | `x1.32xlarge` | | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge`
- Penyimpanan yang dioptimalkan: `d2.8xlarge` | `i3.8xlarge` | `i3.16xlarge` | `h1.8xlarge` | `h1.16xlarge`
- Komputasi yang dipercepat: `f1.16xlarge` `g3.16xlarge` | | `p2.16xlarge` | `p3.16xlarge`
- Bare metal: Semua instans bare metal dengan prosesor Intel dan AMD

Status-C saja

Jenis contoh berikut memberikan kemampuan untuk sistem operasi untuk mengontrol C-state:

- Tujuan umum: `m5.12xlarge` `m5.24xlarge` | `m5d.12xlarge` | `m5d.24xlarge` `m5n.12xlarge` | `m5n.24xlarge` | `m5dn.12xlarge` | `m5dn.24xlarge` | `m5zn.6xlarge` `m5zn.12xlarge` | `m6a.24xlarge` | `m6a.48xlarge` | `m6i.16xlarge` | `m6i.32xlarge` `m6id.16xlarge` | `m6id.32xlarge` | `m6idn.16xlarge` | `m6in.16xlarge` `m6in.32xlarge` | `m7a.medium` | `m7a.large` | `m7a.xlarge` | `m7a.2xlarge` `m7a.4xlarge` | `m7a.8xlarge` | `m7a.12xlarge` | `m7a.16xlarge` | `m7a.24xlarge` `m7a.32xlarge` | `m7a.48xlarge` | `m7i.large` | `m7i.xlarge` | `m7i.2xlarge` `m7i.4xlarge` | `m7i.8xlarge` | `m7i.12xlarge` | `m7i.16xlarge`| `m7i.24xlarge` | `m7i.48xlarge` | `m8a.medium` | `m8a.large` | `m8a.xlarge` | `m8a.2xlarge` | `m8a.4xlarge` | `m8a.8xlarge` `m8a.12xlarge` | `m8a.16xlarge` | `m8a.24xlarge` | `m8a.48xlarge` | `m8azn.medium` | `m8azn.large` | `m8azn.xlarge` | `m8azn.3xlarge` | `m8azn.6xlarge` | `m8azn.12xlarge` | `m8azn.24xlarge` | `m8i.large` | `m8i.xlarge` | `m8i.2xlarge` | `m8i.4xlarge` | `m8i.8xlarge` | `m8i.12xlarge` | `m8i.16xlarge` | `m8i.24xlarge` `m8i.32xlarge` | `m8i.48xlarge` | `m8i.96xlarge` | `m8id.large` | `m8id.xlarge` | `m8id.2xlarge` | `m8id.4xlarge` | `m8id.8xlarge` | `m8id.12xlarge` | `m8id.16xlarge` | `m8id.24xlarge`| `m8id.32xlarge` | `m8id.48xlarge` | `m8id.96xlarge`
- Komputasi dioptimalkan: `c5.9xlarge` `c5.12xlarge` `c5.18xlarge` `c5.24xlarge` | `c5a.24xlarge` | `c5ad.24xlarge` | `c5d.9xlarge` | `c5d.12xlarge` | `c5d.18xlarge` | `c5d.24xlarge` | `c5n.9xlarge` | `c5n.18xlarge` | `c6a.24xlarge` | `c6a.32xlarge` |

c6a.48xlarge | c6i.16xlarge | c6i.32xlarge | c6id.24xlarge | c6id.32xlarge | c6in.32xlarge | c7a.medium | c7a.large | c7a.xlarge | c7a.2xlarge | c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge | c7a.24xlarge | c7a.32xlarge | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge | c7i.4xlarge | c7i.8xlarge c7i.12xlarge| c7i.16xlarge | c7i.24xlarge | c7i.48xlarge | c8a.medium | c8a.large | c8a.xlarge | c8a.2xlarge | c8a.4xlarge c8a.8xlarge | c8a.12xlarge | c8a.16xlarge | c8a.24xlarge | c8a.48xlarge | c8i.large | c8i.xlarge | c8i.2xlarge | c8i.4xlarge | c8i.8xlarge | c8i.12xlarge | c8i.16xlarge | c8i.24xlarge | c8i.32xlarge | c8i.48xlarge | c8i.96xlarge | c8id.large | c8id.xlarge c8id.2xlarge | c8id.4xlarge | c8id.8xlarge | c8id.12xlarge | c8id.16xlarge | c8id.24xlarge | c8id.32xlarge | c8id.48xlarge | c8id.96xlarge x8i.large | x8i.xlarge | x8i.2xlarge| x8i.4xlarge | x8i.8xlarge | x8i.12xlarge x8i.16xlarge | x8i.24xlarge | x8i.32xlarge | x8i.48xlarge | x8i.48xlarge | x8i.96xlarge

- Memori dioptimalkan: r5.12xlarge r5.24xlarge r5b.12xlarge r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | r6id.16xlarge | r6id.32xlarge | r6in.16xlarge | r6in.32xlarge | r7a.medium | r7a.large | r7a.xlarge | r7a.2xlarge | r7a.4xlarge | r7a.8xlarge | r7a.12xlarge | r7a.16xlarge | r7a.24xlarge | r7a.32xlarge | r7a.48xlarge | r7i.large | r7i.xlarge | r7i.2xlarge | r7i.4xlarge | r7i.8xlarge | r7i.12xlarge | r7i.16xlarge | r7i.24xlarge | r7i.48xlarge| r7iz.large | r7iz.xlarge | r7iz.2xlarge | r7iz.4xlarge | r7iz.8xlarge | r7iz.12xlarge | r7iz.16xlarge | r7iz.32xlarge r8a.medium | r8a.large | r8a.xlarge | r8a.2xlarge | r8a.4xlarge | r8a.8xlarge | r8a.12xlarge | r8a.16xlarge | r8a.24xlarge | r8a.48xlarge | r8i.large | r8i.xlarge | r8i.2xlarge | r8i.4xlarge | r8i.8xlarge | r8i.12xlarge | r8i.16xlarge | r8i.24xlarge | r8i.32xlarge r8i.48xlarge | r8i.96xlarge | r8id.large | r8id.xlarge | r8id.2xlarge | r8id.4xlarge | r8id.8xlarge | r8id.12xlarge | r8id.16xlarge | r8id.24xlarge | r8id.32xlarge| r8id.48xlarge | r8id.96xlarge | u-3tb1.56xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge | u-9tb1.112xlarge | u-12tb1.112xlarge | u-18tb1.112xlarge | u-24tb1.112xlarge | u7i-6tb.112xlarge | u7i-8tb.112xlarge | u7i-12tb.224xlarge | u7in-16tb.224xlarge u7in-24tb.224xlarge | u7in-32tb.224xlarge | u7inh-32tb.480xlarge | x2idn.32xlarge | x2iedn.16xlarge | x2iedn.32xlarge | x2iezn.12xlarge | x8aedz.large | x8aedz.xlarge | x8aedz.3xlarge | x8aedz.6xlarge | x8aedz.12xlarge | x8aedz.24xlarge | z1d.6xlarge | z1d.12xlarge

- Penyimpanan dioptimalkan: d3en.12xlarge dl1.24xlarge i3en.12xlarge | i3en.24xlarge | i4i.16xlarge | i7i.large | i7i.xlarge | i7i.2xlarge | i7i.4xlarge | i7i.8xlarge i7i.12xlarge | i7i.16xlarge | i7i.24xlarge | i7i.48xlarge | i7ie.large | i7ie.xlarge | i7ie.2xlarge | i7ie.3xlarge | i7ie.6xlarge | i7ie.12xlarge | i7ie.18xlarge | i7ie.24xlarge | i7ie.48xlarge | r5b.12xlarge | r5b.24xlarge
- Komputasi dipercepat: dl1.24xlarge f2.6xlarge f2.12xlarge f2.48xlarge g5.24xlarge | g5.48xlarge | g6.24xlarge | g6.48xlarge | g6e.12xlarge | g6e.24xlarge | g6e.48xlarge g7e.2xlarge | g7e.4xlarge | g7e.8xlarge | g7e.12xlarge | g7e.24xlarge | g7e.48xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge p4de.24xlarge | p5.48xlarge | p5e.48xlarge | p5en.48xlarge | p6-b200.48xlarge | p6-b300.48xlarge | trn1.32xlarge | trn2.3xlarge | trn2.48xlarge | trn2a.3xlarge trn2a.48xlarge | trn2n.3xlarge | trn2n.48xlarge | trn2p.48xlarge | trn2u.48xlarge | vt1.24xlarge
- Komputasi berkinerja tinggi: hpc7a.12xlarge | hpc7a.24xlarge | hpc7a.48xlarge | hpc7a.96xlarge hpc8a.96xlarge

Anda mungkin harus mengubah pengaturan status-C atau status-P untuk meningkatkan konsistensi performa prosesor, mengurangi latensi, atau menyelaraskan instans Anda dengan beban kerja tertentu. Pengaturan status-C dan status-P default memberikan kinerja maksimum, yang optimal untuk sebagian besar beban kerja. Namun, jika aplikasi Anda akan mendapatkan keuntungan dari pengurangan latensi dengan biaya frekuensi ssatu inti atau dua inti yang lebih tinggi, atau dari performa yang konsisten pada frekuensi yang lebih rendah, dibandingkan dengan frekuensi Turbo Boost yang melonjak, pertimbangkan untuk bereksperimen dengan pengaturan status-C atau status-P yang tersedia untuk instans ini.

Untuk informasi tentang konfigurasi prosesor yang berbeda dan cara memantau efek konfigurasi Anda untuk Amazon Linux, lihat Kontrol status prosesor untuk instans Amazon EC2 Amazon Linux di Panduan Pengguna Amazon Linux 2. Prosedur ini ditulis untuk, dan berlaku untuk Amazon Linux; Namun, mereka mungkin juga bekerja untuk distribusi Linux lainnya dengan kernel Linux 3.9 atau yang lebih baru. Untuk informasi lebih lanjut tentang distribusi Linux dan kontrol status prosesor lainnya, lihat dokumentasi khusus sistem Anda.

Instans terkelola Amazon EC2

Instans terkelola Amazon EC2 adalah instans EC2 yang disediakan dan dikelola oleh penyedia layanan yang ditunjuk, seperti Amazon EKS melalui Mode Otomatis EKS. Instans terkelola menyediakan cara yang disederhanakan untuk menjalankan beban kerja komputasi di Amazon EC2 dengan memungkinkan Anda mendelegasikan kontrol operasional instans ke penyedia layanan.

Kontrol yang didelegasikan adalah satu-satunya perubahan yang diperkenalkan untuk instance terkelola. Spesifikasi teknis dan penagihan tetap sama dengan instans EC2 yang tidak dikelola. Karena instans terkelola memungkinkan Anda mendelegasikan kontrol ke penyedia layanan, Anda bisa mendapatkan keuntungan dari keahlian operasional dan praktik terbaik penyedia layanan. Ketika sebuah instans dikelola, penyedia layanan bertanggung jawab atas tugas-tugas seperti menyediakan instance, mengonfigurasi perangkat lunak, menskalakan kapasitas, menangani kegagalan dan penggantian instans, dan menghentikan instance.

Anda tidak dapat langsung mengubah pengaturan instance terkelola atau menghentikannya. Layanan dan operasi spesifik ditentukan oleh perjanjian antara Anda dan penyedia layanan. Namun, Anda dapat menambahkan, memodifikasi, atau menghapus tag dari instans terkelola, memungkinkan Anda untuk mengkategorikannya dalam lingkungan Anda. AWS

Daftar Isi

- Penagihan untuk instans terkelola
- Identifikasi instance terkelola
- Memulai instans terkelola

Penagihan untuk instans terkelola

Instans terkelola Amazon EC2 dikenakan biaya dasar yang sama dengan instans Amazon EC2 yang tidak dikelola, ditambah biaya terpisah untuk penyedia layanan. Biaya tambahan ini dibebankan oleh penyedia layanan yang mengelola instans Anda dan ditagih secara terpisah. Ini mencakup biaya layanan yang disediakan untuk mengoperasikan dan memelihara instans terkelola Anda.

Semua opsi pembelian Amazon EC2 tersedia untuk instans terkelola, termasuk Instans Sesuai Permintaan, Instans Cadangan, Instans Spot, dan Savings Plans. Dengan sumber komputasi Anda langsung dari EC2 dan kemudian memberikannya kepada penyedia layanan Anda, Anda mendapatkan keuntungan dari Instans Cadangan atau Savings Plans yang ada yang diterapkan ke

akun Anda, memastikan bahwa Anda menggunakan kapasitas komputasi paling hemat biaya yang tersedia.

Misalnya, saat menggunakan Mode Otomatis Amazon EKS, Anda membayar tarif instans EC2 standar untuk instans yang mendasarinya, ditambah biaya tambahan dari Amazon EKS untuk mengelola instans atas nama Anda. Jika Anda kemudian memutuskan untuk mendaftar ke Savings Plans, tarif instans EC2 dikurangi oleh Savings Plans, sementara biaya tambahan dari Amazon EKS tetap tidak berubah.

Identifikasi instance terkelola

Instans terkelola diidentifikasi oleh nilai sebenarnya di bidang Dikelola. Penyedia layanan diidentifikasi di bidang Operator (di konsol) atau `Principal` bidang (di CLI).

Gunakan prosedur berikut untuk mengidentifikasi instans terkelola.

Console

Untuk mengidentifikasi instance terkelola

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih contoh yang ingin Anda periksa.
4. Pada tab Detail (jika Anda memilih kotak centang) atau di area ringkasan (jika Anda memilih ID instance), cari bidang Dikelola.
   - Nilai true menunjukkan instance terkelola.
   - Nilai false menunjukkan instance yang tidak dikelola.
5. Jika Dikelola disetel ke true, bidang Operator menampilkan nilai yang mengidentifikasi penyedia layanan yang bertanggung jawab untuk mengelola instance. Misalnya, nilai eks.amazonaws.com mengidentifikasi Amazon EKS sebagai penyedia layanan.

AWS CLI

Untuk mengidentifikasi instance terkelola

Gunakan perintah describe-instances dan tentukan ID instans.

```
aws ec2 describe-instances \
```

```
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].Operator
```

Berikut ini adalah output contoh. Jika `Managed` ya`true`, instance adalah instance terkelola dan a `Principal` disertakan. Prinsipnya adalah penyedia layanan yang mengelola instance. Misalnya, nilai `eks.amazonaws.com` mengidentifikasi Amazon EKS sebagai penyedia layanan.

```
[
    {
        "Managed": true,
        "Principal": "eks.amazonaws.com"
    }
]
```

Untuk menemukan instans terkelola

Gunakan perintah describe-instance dan tentukan `operator.managed` filter dengan nilai. `true` `--query`Opsi ini hanya menampilkan contoh IDs terkelola.

```
aws ec2 describe-instances \
    --filters "Name=operator.managed,Values=true" \
    --query Reservations[*].Instances[].InstanceId
```

PowerShell

Untuk mengidentifikasi instance terkelola

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.Operator
```

Berikut ini adalah output contoh.

```
Managed Principal
------- ---------
True    eks.amazonaws.com
```

Untuk menemukan instans terkelola

Gunakan Get-EC2Instancecmdlet. Contoh ini hanya menampilkan contoh yang dikelola. IDs

```
(Get-EC2Instance -Filter @{Name="operator.managed";
 Values="true"}).Instances.InstanceId
```

Memulai instans terkelola

Untuk panduan tentang penggunaan instans terkelola, lihat Mengotomatiskan infrastruktur klaster dengan Mode Otomatis EKS di Panduan Pengguna Amazon EKS.

Gunakan virtualisasi bersarang untuk menjalankan hypervisor di instans Amazon EC2

Virtualisasi bersarang memungkinkan Anda menjalankan hypervisor seperti Hyper-V dan KVM di dalam instans Amazon EC2 virtual. Instans EC2 virtual adalah instans logam non-telanjang. Kemampuan ini memperluas fleksibilitas virtualisasi dengan menambahkan dukungan virtualisasi tingkat prosesor ke instans EC2 virtual, memungkinkan hypervisor yang berjalan di instans Anda untuk membuat dan mengelola mesin virtual.

Virtualisasi bersarang dapat membantu saat Anda menjalankan alat pengembangan seperti Docker Desktop, Windows Subsystem for Linux 2 (WSL2), emulator Android Studio, atau QEMU dalam alur kerja pengembangan Anda, karena memungkinkan Anda memilih dari berbagai jenis instans Amazon EC2 virtual standar yang memenuhi persyaratan kinerja dan harga spesifik Anda.

Tidak ada biaya tambahan untuk menggunakan virtualisasi bersarang.

Daftar Isi

- Cara kerjanya
- Pertimbangan-pertimbangan
- Luncurkan instance baru dengan virtualisasi bersarang diaktifkan
- Konfigurasikan instance yang ada untuk menggunakan virtualisasi bersarang

Cara kerjanya

Instans EC2 virtual berjalan pada host fisik yang memiliki hypervisor Nitro. Untuk mendukung virtualisasi bersarang, Sistem Nitro meneruskan ekstensi prosesor, seperti Intel VT-x, ke instance untuk memfasilitasi menjalankan mesin virtual bersarang. Arsitektur virtualisasi bersarang terdiri

dari tiga lapisan: AWS infrastruktur fisik dan Nitro hypervisor (L0), instans EC2 Anda menjalankan hypervisor (L1), dan satu atau lebih mesin virtual yang dibuat dalam instance itu (L2).

Pertimbangan-pertimbangan

Sebelum Anda mulai menggunakan virtualisasi bersarang, pertimbangkan hal berikut:

- Jenis instans yang didukung - Virtualisasi bersarang saat ini didukung pada instance C8i, M8i, dan R8i.
- Hypervisor yang didukung — Saat ini, KVM dan Hyper-V adalah hypervisor L1 yang didukung.
- Instans Windows - Ketika virtualisasi bersarang diaktifkan pada instance Windows:
  - Credential Guard — Virtual Secure Mode (VSM) dinonaktifkan secara otomatis.
  - Hibernasi - Hibernasi dan resume instans tidak didukung.
  - Batas CPU - Tidak didukung pada instance Windows dengan lebih dari 192 CPUs, seperti. `m8i.96xl`
- Tanggung jawab keamanan — Saat menggunakan virtualisasi bersarang pada instans EC2, AWS bertanggung jawab atas “keamanan cloud,” melindungi infrastruktur yang mendasarinya dan mempertahankan batas isolasi yang kuat antara instans EC2 yang disediakan oleh Sistem Nitro. AWS Pelanggan bertanggung jawab atas “keamanan di cloud,” yang mencakup pengamanan sistem operasi, hypervisor, mesin virtual bersarang, sistem operasi tamu, aplikasi, dan data dalam instans EC2.
- Kinerja — AWS merekomendasikan agar pelanggan yang ingin menjalankan beban kerja yang memerlukan akses ke ekstensi virtualisasi perangkat keras, dan sensitif terhadap kinerja atau memiliki persyaratan latensi yang ketat, untuk mengevaluasi instance bare metal.

Luncurkan instance baru dengan virtualisasi bersarang diaktifkan

Saat meluncurkan instance baru, Anda dapat mengaktifkan virtualisasi bersarang untuk menjalankan hypervisor dan mesin virtual di dalamnya.

Prasyarat

Anda harus memiliki izin IAM yang diperlukan untuk meluncurkan instans Amazon EC2.

Console

Untuk mengaktifkan virtualisasi bersarang selama peluncuran instance

1. Ikuti prosedur the section called “Luncurkan menggunakan wizard peluncuran instans” dan konfigurasikan instans Anda sesuai kebutuhan.
2. Pastikan jenis instans yang didukung dipilih.
3. Perluas Detail lanjutan, dan untuk virtualisasi bersarang, pilih Aktifkan.
4. Di panel Ringkasan, tinjau konfigurasi instans Anda, lalu pilih Luncurkan instans.

AWS CLI

Untuk meluncurkan instance dengan virtualisasi bersarang diaktifkan

Gunakan perintah run-instans.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r8i.4xlarge \
    --cpu-options "NestedVirtualization=enabled" \
    --key-name my-key-pair
```

PowerShell

Untuk meluncurkan instance dengan virtualisasi bersarang diaktifkan

Gunakan perintah New-EC2Instance.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType r8i.4xlarge `
    -CpuOption @{NestedVirtualization='enabled'} `
    -KeyName my-key-pair
```

Konfigurasikan instance yang ada untuk menggunakan virtualisasi bersarang

Anda dapat mengaktifkan virtualisasi bersarang pada instans Amazon EC2 yang ada.

Prasyarat

- Contoh harus dalam `stopped` keadaan.
- Jenis instance harus mendukung virtualisasi bersarang.

Console

Untuk mengaktifkan virtualisasi bersarang pada instance yang ada

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih contoh yang ingin Anda modifikasi dari tabel instance.
4. Pilih Tindakan, Pengaturan instans, Ubah opsi CPU.
5. Pada halaman Ubah opsi CPU, untuk virtualisasi Nested, pilih salah satu opsi berikut:
   - Aktifkan - Mengaktifkan virtualisasi bersarang untuk instance
   - Nonaktifkan - Mematikan virtualisasi bersarang untuk contoh
6. Tinjau perubahan Anda, lalu pilih Ubah untuk menerapkan opsi CPU baru.

AWS CLI

Untuk mengaktifkan virtualisasi bersarang pada instance yang ada

Pertama hentikan instance, dan kemudian gunakan modify-instance-cpu-optionsperintah.

```
aws ec2 modify-instance-cpu-options \
    --instance-id i-1234567890abcdef0 \
    --core-count 4 \
    --threads-per-core 2 \
    --nested-virtualization enabled
```

PowerShell

Untuk mengaktifkan virtualisasi bersarang pada instance yang ada

Pertama hentikan instance, dan kemudian gunakan Edit-EC2InstanceCpuOptionperintah.

```
Edit-EC2InstanceCpuOption `
```

```
    -InstanceId i-1234567890abcdef0 `
    -CoreCount 4 `
    -ThreadsPerCore 2 `
    -NestedVirtualization enabled
```

Opsi penagihan dan pembelian Amazon EC2

Anda dapat menggunakan opsi berikut untuk mengoptimalkan biaya Anda untuk Amazon EC2:

- Instans Sesuai Permintaan – Bayar, per detik, untuk instans yang Anda luncurkan.
- Savings Plans – Kurangi biaya Amazon EC2 dengan membuat komitmen pada jumlah penggunaan yang konsisten, dalam USD per jam, untuk jangka waktu 1 atau 3 tahun.
- Instans Terpesan – Kurangi biaya Amazon EC2 Anda dengan membuat komitmen pada konfigurasi instans yang konsisten, termasuk tipe instans dan Wilayah, untuk jangka waktu 1 atau 3 tahun.
- Instans Spot – Minta instans EC2 yang tidak digunakan, yang dapat mengurangi biaya Amazon EC2 Anda secara signifikan.
- Host Khusus - Bayar untuk host fisik yang sepenuhnya didedikasikan untuk menjalankan instans Anda, dan bawa lisensi perangkat lunak per soket, per inti, atau per VM yang ada untuk mengurangi biaya.
- Instans Khusus - Bayar, per jam, untuk instans yang berjalan pada perangkat keras penghuni tunggal.
- Reservasi Kapasitas — Kapasitas cadangan untuk instans EC2 Anda di Availability Zone tertentu.

Jika Anda tidak dapat membuat komitmen terhadap konfigurasi instans tertentu, tetapi Anda dapat berkomitmen pada jumlah penggunaan, belilah Savings Plans untuk mengurangi biaya Instans Sesuai Permintaan.Jika Anda memerlukan reservasi kapasitas, belilah Instans Terpesan atau Reservasi Kapasitas untuk Zona Ketersediaan tertentu. Blok Kapasitas dapat digunakan untuk memesan klaster instans GPU. Instans Spot adalah pilihan hemat biaya jika Anda dapat bersikap fleksibel tentang kapan aplikasi Anda berjalan dan apakah aplikasi tersebut dapat diinterupsi. Host Khusus atau Instans Khusus dapat membantu Anda memenuhi persyaratan kepatuhan dan mengurangi biaya dengan menggunakan lisensi perangkat lunak terikat server yang ada.

Untuk informasi selengkapnya, lihat Harga Amazon EC2 dan. Instans terkelola Amazon EC2

Membeli Instans Sesuai Permintaan untuk Amazon EC2

Dengan Instans Sesuai Permintaan, Anda membayar kapasitas komputasi per detik tanpa komitmen jangka panjang. Anda memiliki kendali penuh atas siklus hidup instans—Anda memutuskan kapan akan meluncurkan, menghentikan, hibernasi, memulai, melakukan reboot, atau mengakhirinya.

Tidak ada komitmen jangka panjang yang diperlukan saat Anda membeli Instans Sesuai Permintaan. Anda hanya membayar untuk detik saat Instans Sesuai Permintaan Anda berada pada status `running`, dengan minimum 60 detik. Harga per detik untuk Instans Sesuai Permintaan yang berjalan ditetapkan, dan tercantum di halaman EC2 Harga Amazon, Harga Sesuai Permintaan, halaman .

Kami menyarankan agar Anda menggunakan Instans Sesuai Permintaan untuk aplikasi dengan beban kerja tidak teratur jangka pendek yang tidak dapat diganggu.

Untuk penghematan Instans Sesuai Permintaan yang signifikan, gunakan AWS Savings Plans, Instans Spot, atau Instans Cadangan untuk ikhtisar Amazon EC2.

Daftar Isi

- Kuota Instans Sesuai Permintaan
  - Memantau kuota dan penggunaan Instans Sesuai Permintaan
  - Meminta peningkatan kuota
- Membuat kueri harga Instans Sesuai Permintaan

Kuota Instans Sesuai Permintaan

Ada kuota untuk jumlah Instans Sesuai Permintaan yang berjalan per Akun AWS Wilayah. Kuota Instans Sesuai Permintaan dikelola berdasarkan jumlah unit pemrosesan pusat virtual (vCPUs) yang digunakan Instans Sesuai Permintaan Anda, apa pun jenis instancenya. Setiap jenis kuota menentukan jumlah maksimum v CPUs untuk satu atau lebih keluarga instance.

Akun Anda menyertakan kuota berikut untuk Instans Sesuai Permintaan. Instans yang berada dalam status tertunda, berhenti, berhenti, dan hibernasi tidak dihitung dalam kuota Instans Sesuai Permintaan Anda. Reservasi Kapasitas dihitung dalam kuota Instans Sesuai Permintaan Anda, meskipun tidak digunakan.

Nama	Default	Dapat disesuaikan
Instans DL Sesuai Permintaan yang Berjalan	0	Ya

Nama	Default	Dapat disesuaikan
Instans F Sesuai Permintaan yang Berjalan	0	Ya
Instans DL Sesuai Permintaan yang Berjalan dan instans VT	0	Ya
Instans HPC Sesuai Permintaan yang Berjalan	0	Ya
Instans Memori Tinggi Sesuai Permintaan yang Berjalan	0	Ya
Instans Inf Sesuai Permintaan yang Berjalan	0	Ya
Instans P Sesuai Permintaan yang Berjalan	0	Ya
Instans Standar (A, C, D, H, I, M, R, T, Z) Sesuai Permintaan yang Berjalan	5	Ya
Instans Trn Sesuai Permintaan yang Berjalan	0	Ya
Instans X Sesuai Permintaan yang Berjalan	0	Ya

Untuk informasi tentang keluarga, generasi, dan ukuran instans yang berbeda, lihat Panduan Jenis EC2 Instans Amazon.

Anda dapat meluncurkan kombinasi jenis instans yang memenuhi kebutuhan aplikasi yang berubah, selama jumlah v CPUs tidak melebihi kuota akun Anda. Misalnya, dengan kuota instans Standar 256 vCPUs, Anda dapat meluncurkan 32 `m5.2xlarge` instance (32 x 8 vCPUs) atau 16 `c5.4xlarge` instance (16 x 16 v). CPUs Untuk informasi selengkapnya, lihat Batas Instans EC2 Sesuai Permintaan.

Tugas

- Memantau kuota dan penggunaan Instans Sesuai Permintaan
- Meminta peningkatan kuota

Memantau kuota dan penggunaan Instans Sesuai Permintaan

Anda dapat melihat dan mengelola kuota Instans Sesuai Permintaan untuk setiap Wilayah menggunakan metode berikut.

Untuk melihat kuota saat ini menggunakan konsol Kuota Layanan

1. Buka konsol Service Quotas di https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Dari bilah navigasi, pilih Wilayah.
3. Di bidang filter, masukkan **`On-Demand`**.
4. Kolom Nilai kuota Terapan menampilkan jumlah maksimum v CPUs untuk setiap jenis kuota Instans Sesuai Permintaan untuk akun Anda.

Untuk melihat kuota Anda saat ini menggunakan konsol AWS Trusted Advisor

Buka halaman batas layanan di AWS Trusted Advisor konsol.

Untuk mengkonfigurasi CloudWatch alarm

Dengan integrasi CloudWatch metrik Amazon, Anda dapat memantau EC2 penggunaan Anda terhadap kuota Anda. Anda juga dapat mengonfigurasi alarm untuk memperingatkan saat sudah mendekati kuota. Untuk informasi selengkapnya, lihat Service Quotas dan CloudWatch alarm Amazon di Panduan Pengguna Service Quotas.

Meminta peningkatan kuota

Meskipun Amazon EC2 secara otomatis meningkatkan kuota Instans Sesuai Permintaan berdasarkan penggunaan, Anda dapat meminta peningkatan kuota jika perlu. Misalnya, jika Anda bermaksud untuk meluncurkan lebih banyak instans daripada yang diizinkan oleh kuota saat ini, Anda dapat meminta peningkatan kuota dengan menggunakan Konsol Kuota Layanan yang dijelaskan di Kuota EC2 layanan Amazon.

Membuat kueri harga Instans Sesuai Permintaan

Anda dapat menggunakan API Layanan Daftar Harga atau API Daftar AWS Harga untuk menanyakan harga Instans Sesuai Permintaan. Untuk informasi selengkapnya, lihat Menggunakan API Daftar AWS Harga di Panduan AWS Billing Pengguna.

Instans Cadangan untuk ikhtisar Amazon EC2

> **Important**
>
> Kami merekomendasikan Savings Plans atas Instans Cadangan. Paket Tabungan adalah cara termudah dan paling fleksibel untuk menghemat uang pada biaya AWS komputasi Anda dan menawarkan harga yang lebih rendah (diskon hingga 72% dari harga On-Demand), seperti Instans Cadangan. Namun, Savings Plans berbeda dengan Instans Cadangan. Dengan Instans Cadangan, Anda berkomitmen pada konfigurasi instans tertentu, sedangkan dengan Savings Plans, Anda memiliki fleksibilitas untuk menggunakan konfigurasi instans yang paling sesuai dengan kebutuhan Anda. Untuk menggunakan Savings Plans, Anda membuat komitmen terhadap jumlah penggunaan yang konsisten, diukur dalam USD per jam. Untuk informasi selengkapnya, lihat AWS Panduan Pengguna Savings Plans.

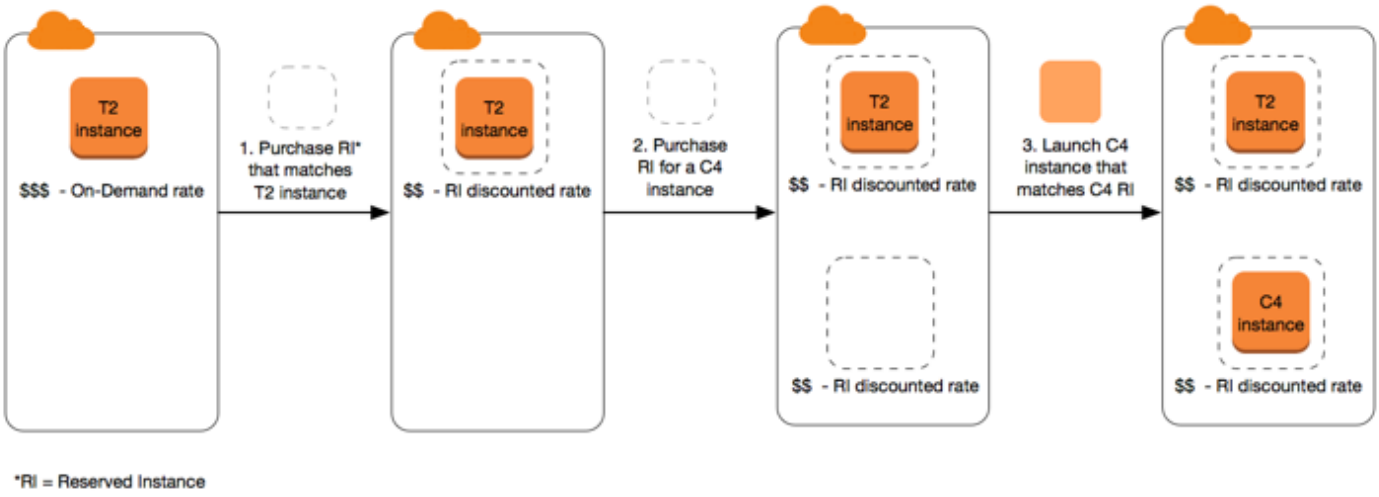
Instans Terpesan memberi Anda penghematan yang signifikan pada biaya Amazon EC2 Anda dibandingkan dengan harga Instans Sesuai Permintaan. Instans Terpesan bukanlah instans fisik, melainkan diskon penagihan yang diterapkan untuk penggunaan Instans Sesuai Permintaan di akun Anda. Instans Sesuai Permintaan ini harus cocok dengan atribut tertentu, seperti tipe instans dan Wilayah, untuk mendapatkan keuntungan dari diskon penagihan.

Topik Instans Terpesan

- Contoh skenario Instans Cadangan
- Variabel utama yang menentukan harga Instans Terpesan
- Instans Terpesan Regional dan zonal (cakupan)
- Tipe Instans Terpesan (kelas penawaran)
- Bagaimana diskon Instans Cadangan diterapkan
- Menggunakan Instans Terpesan Anda
- Cara kerja penagihan dengan Instans Cadangan
- Beli Instans Cadangan untuk Amazon EC2
- Jual Instans Cadangan untuk Amazon EC2 di Marketplace Instans Cadangan
- Memodifikasi Instans Terpesan
- Menukar Instans Terpesan Konvertibel
- Kuota Instans Terpesan

Contoh skenario Instans Cadangan

Diagram berikut menunjukkan skenario dasar pembelian dan penggunaan Instans Cadangan.



Dalam skenario ini, Anda memiliki Instans Sesuai Permintaan (T2) yang berjalan di akun Anda, yang saat ini Anda bayar dengan tarif Sesuai Permintaan. Anda membeli Instans Terpesan yang cocok dengan atribut instans Anda yang sedang berjalan, dan manfaat penagihan segera diterapkan. Selanjutnya, Anda membeli Instans Terpesan untuk instans C4. Anda tidak memiliki instans yang sedang berjalan di akun Anda yang cocok dengan atribut Instans Terpesan ini. Pada langkah terakhir, Anda meluncurkan instans yang cocok dengan atribut Instans Terpesan C4, dan manfaat penagihan segera diterapkan.

Variabel utama yang menentukan harga Instans Terpesan

Harga Instans Terpesan ditentukan oleh variabel kunci berikut.

Atribut instans

Instans Terpesan memiliki empat atribut instans yang menentukan harganya.

- Tipe instans: Contohnya, `m4.large`. Ini terdiri dari keluarga instans (sebagai contoh, `m4`) dan ukuran instans (misalnya, `large`).
- Wilayah: Wilayah tempat Instans Terpesan dibeli.
- Penghunian: Apakah instans Anda berjalan pada perangkat keras bersama (default) atau penghuni tunggal (khusus). Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.
- Platform: Sistem operasi; misalnya, Windows atau Linux/Unix. Untuk informasi selengkapnya, lihat Memilih platform.

Komitmen jangka waktu

Anda dapat membeli Instans Terpesan untuk komitmen satu tahun atau tiga tahun, di mana komitmen tiga tahun menawarkan diskon yang lebih besar.

- Satu tahun: Satu tahun didefinisikan sebagai 31.536.000 detik (365 hari).
- Tiga tahun: Tiga tahun didefinisikan sebagai 94.608.000 detik (1.095 hari).

Instans Terpesan tidak diperpanjang secara otomatis; saat kedaluwarsa, Anda dapat terus menggunakan instans EC2 tanpa gangguan, tetapi Anda dikenai tarif Sesuai Permintaan. Dalam contoh di atas, ketika Instans Terpesan yang mencakup instans T2 dan C4 telah kedaluwarsa, Anda kembali membayar tarif Sesuai Permintaan hingga Anda mengakhiri instans atau membeli Instans Terpesan baru yang cocok dengan atribut instans.

> **Important**
>
> Setelah Anda membeli Instans Terpesan, Anda tidak dapat membatalkan pembelian tersebut. Namun, Anda mungkin dapat mengubah, menukar, atau menjual Instans Terpesan itu jika kebutuhan Anda berubah.

Opsi pembayaran

Opsi pembayaran berikut tersedia untuk Instans Terpesan:

- Lunas di Depan: Pembayaran penuh dilakukan di awal jangka waktu, tanpa biaya lain atau biaya per jam tambahan yang timbul untuk sisa jangka waktu, berapa pun jam yang digunakan.
- Dengan Uang Muka: Sebagian dari biaya harus dibayar di muka dan sisa jam dalam jangka waktu tersebut ditagih dengan tarif per jam yang didiskon, terlepas dari apakah Instans Terpesan tersebut sedang digunakan.
- Tanpa Uang Muka: Anda akan dikenai tarif per jam dengan diskon untuk setiap jam dalam jangka waktu tersebut, terlepas dari apakah Instans Terpesan sedang digunakan. Tidak perlu uang muka.

> **Note**
>
> Tidak ada Instans Terpesan Tanpa Uang Muka yang didasarkan pada kewajiban kontraktual untuk membayar bulanan untuk seluruh jangka waktu reservasi. Untuk alasan

ini, riwayat penagihan yang berhasil diperlukan sebelum Anda dapat membeli Instans Terpesan Tanpa Uang Muka.

Secara umum, Anda dapat menghemat lebih banyak uang dengan membayar uang muka yang lebih tinggi untuk Instans Terpesan. Anda juga dapat menemukan Instans Terpesan yang ditawarkan oleh penjual pihak ketiga dengan harga lebih rendah dan jangka waktu lebih pendek di Pasar Instans Terpesan. Untuk informasi selengkapnya, lihat Jual Instans Cadangan untuk Amazon EC2 di Marketplace Instans Cadangan.

Kelas penawaran

Jika kebutuhan komputasi Anda berubah, Anda mungkin dapat mengubah atau menukar Instans Cadangan Anda, bergantung pada kelas penawaran.

- Standar: Kelas ini memberikan diskon paling signifikan, tetapi hanya dapat dimodifikasi. Instans Terpesan Standar tidak dapat ditukar.
- Konvertibel: Kelas ini memberikan diskon yang lebih rendah daripada Instans Terpesan Standar, tetapi dapat ditukar dengan Instans Terpesan Konvertibel lainnya dengan atribut instans yang berbeda. Instans Terpesan Konvertibel juga dapat dimodifikasi.

Untuk informasi selengkapnya, lihat Tipe Instans Terpesan (kelas penawaran).

Important

Setelah Anda membeli Instans Terpesan, Anda tidak dapat membatalkan pembelian tersebut. Namun, Anda mungkin dapat mengubah, menukar, atau menjual Instans Terpesan itu jika kebutuhan Anda berubah.

Untuk informasi selengkapnya, lihat halaman Harga Instans Terpesan Amazon EC2.

Instans Terpesan Regional dan zonal (cakupan)

Saat Anda membeli Instans Terpesan, Anda menentukan cakupan Instans Terpesan tersebut. Cakupan itu bisa regional atau zonal.

- Regional: Saat Anda membeli Instans Terpesan untuk suatu Wilayah, maka instans itu disebut sebagai Instans Terpesan regional.

- Zonal: Saat Anda membeli Instans Terpesan untuk Zona Ketersediaan tertentu, instans itu disebut sebagai Instans Terpesan zonal.

Cakupan tidak memengaruhi harga. Anda membayar harga yang sama untuk Instans Terpesan regional maupun zonal. Untuk informasi selengkapnya tentang harga Instans Terpesan, lihat Variabel utama yang menentukan harga Instans Terpesan dan Harga Instans Terpesan Amazon EC2.

Untuk informasi selengkapnya tentang cara menentukan cakupan Instans Terpesan, lihat Atribut RI, khususnya bullet Zona Ketersediaan.

Perbedaan antara Instans Terpesan regional dan zonal

Tabel berikut menyoroti beberapa perbedaan utama antara Instans Terpesan regional dan Instans Terpesan zonal:

	Instans Terpesan Regional	Instans Terpesan Zonal
Kemampuan untuk memesan kapasitas	Instans Terpesan regional tidak memesan kapasitas.	Instans Terpesan zonal memesan kapasitas di Zona Ketersediaan yang ditentukan.
Fleksibilitas Zona Ketersediaan	Diskon Instans Terpesan berlaku untuk penggunaan instans di Zona Ketersediaan mana pun di Wilayah yang ditentukan.	Tidak ada fleksibilitas Zona Ketersediaan — diskon Instans Terpesan berlaku untuk penggunaan instans di Zona Ketersediaan yang ditentukan saja.
Fleksibilitas ukuran instans	Diskon Instans Terpesan berlaku untuk penggunaan instans dalam keluarga instans, berapa pun ukurannya. Hanya didukung di Instans Linux/Unix Cadangan Amazon	Tidak ada fleksibilitas ukuran instans — diskon Instans Terpesan berlaku untuk penggunaan instans dengan tipe dan ukuran instans yang ditentukan.

	Instans Terpesan Regional	Instans Terpesan Zonal
	dengan penyewaan default. Untuk informasi selengkap nya, lihat Fleksibilitas ukuran instans ditentukan oleh faktor normalisasi.	
Mengantrekan pembelian	Anda dapat mengantrekan pembelian untuk Instans Terpesan regional.	Anda dapat mengantrekan pembelian untuk Instans Terpesan zonal.

Untuk informasi dan contoh selengkapnya, lihat Bagaimana diskon Instans Cadangan diterapkan.

Tipe Instans Terpesan (kelas penawaran)

Kelas penawaran Instans Terpesan adalah Standar atau Konvertibel. Instans Terpesan Standar memberikan diskon yang lebih signifikan daripada Instans Terpesan Konvertibel, tetapi Anda tidak dapat menukarkan Instans Terpesan Standar. Anda dapat menukar Instans Terpesan Konvertibel. Anda dapat memodifikasi Instans Terpesan Standar dan Konvertibel.

Konfigurasi Instans Terpesan terdiri dari satu tipe instans, platform, cakupan, dan penghunian selama jangka waktu tertentu. Jika kebutuhan komputasi Anda berubah, Anda mungkin dapat mengubah atau menukar Instans Terpesan Anda.

Perbedaaan antara Instans Terpesan Standar dan Konvertibel

Berikut adalah perbedaaan antara Instans Terpesan Standar dan Konvertibel.

	Instans Terpesan Standar	Instans Terpesan Konvertibel
Memodifikasi Instans Terpesan	Beberapa atribut dapat dimodifikasi. Untuk informasi selengkapnya, lihat Memodifik asi Instans Terpesan.	Beberapa atribut dapat dimodifikasi. Untuk informasi selengkapnya, lihat Memodifik asi Instans Terpesan.
Menukar Instans Terpesan	Tidak bisa ditukar.	Dapat ditukar selama jangka waktu dengan Instans

	Instans Terpesan Standar	Instans Terpesan Konvertibel
		Terpesan Konvertibel lainnya dengan atribut baru, termasuk keluarga instans, tipe instans, platform, cakupan, atau penghunian. Untuk informasi selengkapnya, lihat Menukar Instans Terpesan Konvertibel.
Menjual di Marketplace Instans Terpesan	Dapat dijual di Marketplace Instans Terpesan.	Tidak dapat dijual di Marketplace Instans Terpesan.
Membeli dari Marketplace Instans Terpesan	Dapat dibeli di Marketplace Instans Terpesan.	Tidak dapat dibeli di Marketplace Instans Terpesan.

Bagaimana diskon Instans Cadangan diterapkan

Instans Terpesan bukanlah instans fisik, melainkan diskon penagihan yang diterapkan untuk Instans Sesuai Permintaan yang berjalan di akun Anda. Instans Sesuai Permintaan harus cocok dengan spesifikasi Instans Terpesan tertentu untuk mendapatkan keuntungan dari diskon penagihan.

Jika Anda membeli Instans Terpesan dan sudah memiliki Instans Sesuai Permintaan yang berjalan yang sesuai dengan spesifikasi Instans Terpesan, diskon penagihan langsung diterapkan secara otomatis. Anda tidak perlu memulai ulang instans Anda. Jika Anda tidak memiliki Instans Sesuai Permintaan yang memenuhi syarat, luncurkan Instans Sesuai Permintaan dengan spesifikasi yang sama dengan Instans Terpesan Anda. Untuk informasi selengkapnya, lihat Menggunakan Instans Terpesan Anda.

Kelas penawaran (Standar atau Konvertibel) dari Instans Terpesan tidak memengaruhi bagaimana diskon penagihan diterapkan.

Topik

- Bagaimana Instans Terpesan zonal diterapkan
- Bagaimana Instans Terpesan regional diterapkan
- Fleksibilitas ukuran instans
- Contoh penerapan Instans Terpesan

Bagaimana Instans Terpesan zonal diterapkan

Instans Terpesan yang dibeli untuk memesan kapasitas di Zona Ketersediaan tertentu disebut Instans Terpesan zonal.

- Diskon Instans Terpesan berlaku untuk penggunaan instans yang sesuai di Zona Ketersediaan tersebut.
- Atribut (penghunian, platform, Zona Ketersediaan, tipe instans, dan ukuran instans) dari instans yang sedang berjalan harus cocok dengan Instans Terpesan.

Misalnya, jika Anda membeli dua Instans Cadangan Standar Linux/Unix tenancy `c4.xlarge` default untuk Availability Zone us-east-1a, maka hingga dua instance tenancy `c4.xlarge` default yang berjalan di Availability Zone us-east-1a dapat memanfaatkan diskon Linux/Unix Instans Cadangan.

Bagaimana Instans Terpesan regional diterapkan

Instans Terpesan yang dibeli untuk suatu Wilayah disebut Instans Terpesan regional, dan menyediakan Zona Ketersediaan serta fleksibilitas ukuran instans.

- Diskon Instans Terpesan berlaku untuk penggunaan instans di Zona Ketersediaan mana pun di Wilayah tersebut.
- Diskon Instans Terpesan berlaku untuk penggunaan instans dalam keluarga instans, berapa pun ukurannya—ini dikenal sebagai fleksibilitas ukuran instans.

Fleksibilitas ukuran instans

Dengan fleksibilitas ukuran instans, diskon Instans Cadangan berlaku untuk penggunaan instans untuk instance yang memiliki keluarga yang sama. Instans Terpesan diterapkan dari ukuran instans terkecil hingga terbesar dalam keluarga instans berdasarkan faktor normalisasi. Untuk contoh bagaimana diskon Instans Terpesan diterapkan, lihat Skenario 2: Instans Terpesan dalam satu akun menggunakan faktor normalisasi.

Batasan

- Didukung: Fleksibilitas ukuran instans hanya didukung untuk Instans Terpesan Regional.
- Tidak didukung: Fleksibilitas ukuran instans tidak didukung untuk Instans Terpesan berikut:
  - Instans Terpesan yang dibeli untuk Zona Ketersediaan tertentu (Instans Terpesan zonal)

- Instans Cadangan untuk instans G4ad, G4dn, G5, G5g, G6, G6e, G6f, Gr6, Gr6f, hpc7a, P5, Inf1, Inf2, u7i-6tb, dan u7i-8tb
- Instans Terpesan untuk Windows Server, Windows Server dengan SQL Standard, Windows Server dengan SQL Server Enterprise, Windows Server dengan SQL Server Web, RHEL, dan SUSE Linux Enterprise Server
- Instans Terpesan dengan penghunian khusus

Fleksibilitas ukuran instans ditentukan oleh faktor normalisasi

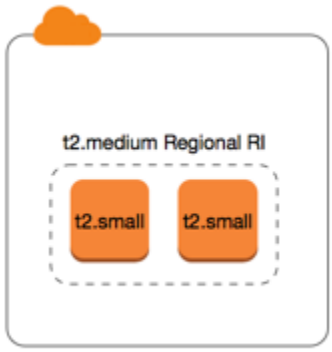
Fleksibilitas ukuran instans ditentukan oleh faktor normalisasi ukuran instans. Diskon berlaku baik sepenuhnya atau sebagian untuk instans yang berjalan dari keluarga instans yang sama, bergantung pada ukuran instans reservasi, di Zona Ketersediaan mana pun di Wilayah itu. Atribut yang harus dicocokkan adalah keluarga instans penghunian, dan platform.

Tabel berikut mencantumkan berbagai ukuran dalam keluarga instans, dan faktor normalisasi yang sesuai. Skala ini digunakan untuk menerapkan tarif diskon dari Instans Terpesan ke penggunaan normal keluarga instans.

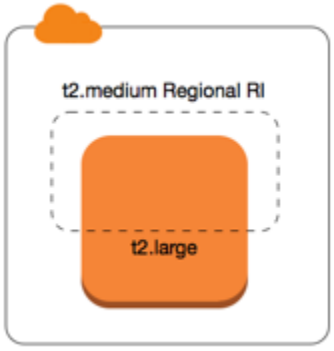
Ukuran instans	Faktor normalisasi
nano	0,25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48

Ukuran instans	Faktor normalisasi
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Misalnya, instans `t2.medium` memiliki faktor normalisasi 2. Jika Anda membeli Instans Terpesan Amazon Linux/Unix penghunian default `t2.medium` di AS Timur (Virginia Utara) dan Anda memiliki dua instans `t2.small` yang sedang berjalan di akun Anda di Wilayah itu, manfaat penagihan diterapkan secara penuh untuk kedua instans.



Atau, jika Anda memiliki satu instans `t2.large` yang berjalan di akun Anda di Wilayah AS Timur (Virginia Utara), manfaat penagihan diterapkan ke 50% penggunaan instans.



Faktor normalisasi juga diterapkan saat memodifikasi Instans Terpesan. Untuk informasi selengkapnya, lihat Memodifikasi Instans Terpesan.

Faktor normalisasi untuk instans bare metal

Fleksibilitas ukuran instans juga berlaku untuk instans bare metal dalam keluarga instans. Jika Anda memiliki Instans Linux/Unix Cadangan Amazon regional dengan penyewaan bersama pada instans logam kosong, Anda dapat memanfaatkan penghematan Instans Cadangan dalam keluarga instans yang sama. Hal sebaliknya juga berlaku: jika Anda memiliki Instans Linux/Unix Cadangan Amazon regional dengan penyewaan bersama pada instans dalam keluarga yang sama dengan instans logam kosong, Anda dapat memanfaatkan penghematan Instans Cadangan pada instans logam kosong.

Ukuran instans `metal` tidak memiliki faktor normalisasi tunggal. Instans bare metal memiliki faktor normalisasi yang sama dengan ukuran instans virtual setara dalam keluarga instans yang sama. Misalnya, instans `i3.metal` memiliki faktor normalisasi yang sama dengan instans `i3.16xlarge`.

Ukuran instans	Faktor normalisasi
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128
`c5n.metal`	144

Ukuran instans	Faktor normalisasi
c5.metal| c5d.metal | i3en.metal | m5.metal| m5d.metal | m5dn.metal | m5n.metal | r5.metal| r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal |c6id.metal |m6i.metal |m6id.metal |r6d.metal |r6id.metal	256
u-18tb1.metal |u-24tb1.metal	448
u-6tb1.metal |u-9tb1.metal |u-12tb1.metal	896

Misalnya, file`i3.metal` Misalnya memiliki faktor normalisasi 128. Jika Anda membeli Instans Terpesan Amazon Linux/Unix penghunian default `i3.metal` di AS Timur (Virginia Utara), manfaat penagihan dapat berlaku sebagai berikut:

- Jika Anda memiliki satu `i3.16xlarge` yang berjalan di akun Anda di Wilayah tersebut, keuntungan penagihan diterapkan secara penuh ke instans `i3.16xlarge` (faktor normalisasi `i3.16xlarge` = 128).
- Atau, jika Anda memiliki dua instans `i3.8xlarge` yang berjalan di akun Anda di Wilayah tersebut, keuntungan penagihan diterapkan secara penuh ke kedua instans `i3.8xlarge` (faktor normalisasi `i3.8xlarge` = 64).
- Atau, jika Anda memiliki empat instans `i3.4xlarge` yang berjalan di akun Anda di Wilayah tersebut, keuntungan penagihan diterapkan secara penuh ke semua empat instans `i3.4xlarge` (faktor normalisasi `i3.4xlarge` = 32).

Kebalikannya juga benar. Misalnya, jika Anda membeli dua Instans Linux/Unix Cadangan Amazon sewaan `i3.8xlarge` default di AS Timur (Virginia N.), dan Anda memiliki satu `i3.metal` instans yang berjalan di Wilayah tersebut, manfaat penagihan diterapkan secara penuh ke instans. `i3.metal`

Contoh penerapan Instans Terpesan

Skenario berikut membahas cara penerapan Instans Terpesan.

- Skenario 1: Instans Terpesan dalam satu akun

- Skenario 2: Instans Terpesan dalam satu akun menggunakan faktor normalisasi
- Skenario 3: Instans Terpesan Regional dalam akun tertaut
- Skenario 4: Instans Terpesan Zonal dalam akun tertaut

Skenario 1: Instans Terpesan dalam satu akun

Anda menjalankan Instans Sesuai Permintaan berikut di akun A:

- 4 x `m3.large` Linux, instans penghunian default di Zona Ketersediaan us-east-1a
- 2 x `m4.xlarge` Amazon Linux, instans penghunian default di Zona Ketersediaan us-east-1b
- 1 x `c4.xlarge` Amazon Linux, instans penghunian default di Zona Ketersediaan us-east-1c

Anda membeli Instans Terpesan berikut di akun A:

- 4 x `m3.large` Linux, Instans Terpesan penghunian default di Zona Ketersediaan us-east-1a (kapasitas dipesan)
- 4 x `m4.large` Amazon Linux, Instans Terpesan penghunian default di Wilayah us-east-1
- 1 x `c4.large` Amazon Linux, Instans Terpesan penghunian default di Wilayah us-east-1

Keuntungan Instans Terpesan diterapkan dengan cara berikut:

- Diskon dan reservasi kapasitas keempat Instans Terpesan zonal `m3.large` digunakan oleh empat instans `m3.large` karena atribut (ukuran instans, Wilayah, platform,penghunian) di antara keempatnya cocok.
- Instans Terpesan regional `m4.large` memberikan Zona Ketersediaan dan fleksibilitas ukuran instans, karena ini adalah Instans Terpesan Amazon Linux regional dengan penghunian default.

  Sebuah instans `m4.large` setara dengan 4 unit/jam yang dinormalisasi.

  Anda telah membeli empat Instans Cadangan `m4.large` regional, dan secara total, mereka sama dengan 16 dinormalisasi units/hour (4x4). Akun A memiliki dua `m4.xlarge` instance yang berjalan, yang setara dengan 16 dinormalisasi units/hour (2x8). Dalam hal ini, empat Instans Terpesan regional `m4.large` memberikan manfaat penagihan penuh untuk penggunaan kedua instans `m4.xlarge`.
- Instans Terpesan regional `c4.large` di us-east-1 memberikan Zona Ketersediaan dan fleksibilitas ukuran instans, karena ini adalah Instans Terpesan Amazon Linux regional dengan penghunian

default, dan diterapkan untuk instans `c4.xlarge`. Sebuah `c4.large` instance setara dengan 4 dinormalisasi units/hour dan a setara dengan 8 `c4.xlarge` unit/jam yang dinormalisasi.

Dalam hal ini, Instans Terpesan regional `c4.large` memberikan sebagian keuntungan untuk penggunaan `c4.xlarge`. Ini karena Instans Terpesan `c4.large` setara dengan 4 unit/jam penggunaan yang dinormalisasi, tetapi instans `c4.xlarge` membutuhkan 8 unit/jam yang dinormalisasi. Oleh karena itu, diskon penagihan Instans Terpesan `c4.large` berlaku untuk 50% dari penggunaan `c4.xlarge`. Penggunaan `c4.xlarge` yang tersisa dikenai biaya dengan tarif Sesuai Permintaan.

Skenario 2: Instans Terpesan dalam satu akun menggunakan faktor normalisasi

Anda menjalankan Instans Sesuai Permintaan berikut di akun A:

- 2 x `m3.xlarge` Amazon Linux, instans penghunian default di Zona Ketersediaan us-east-1b
- 2 x `m3.large` Amazon Linux, instans penghunian default di Zona Ketersediaan us-east-1b

Anda membeli Instans Terpesan berikut di akun A:

- 1 x `m3.2xlarge` Amazon Linux, Instans Terpesan penghunian default di Wilayah us-east-1

Keuntungan Instans Terpesan diterapkan dengan cara berikut:

- Instans Terpesan regional `m3.2xlarge` di us-east-1 memberikan Zona Ketersediaan dan fleksibilitas ukuran instans, karena ini adalah Instans Terpesan Amazon Linux regional dengan penghunian default. Ini berlaku pertama untuk instans `m3.large`, kemudian ke instans `m3.xlarge`, karena berlaku dari ukuran instans terkecil hingga terbesar dalam keluarga instans berdasarkan faktor normalisasi.

  Sebuah instans `m3.large` setara dengan 4 unit/jam yang dinormalisasi.

  Sebuah instans `m3.xlarge` setara dengan 8 unit/jam yang dinormalisasi.

  Sebuah instans `m3.2xlarge` setara dengan 16 unit/jam yang dinormalisasi.

  Manfaatnya diterapkan sebagai berikut:

Instans Cadangan `m3.2xlarge` regional memberikan manfaat penuh untuk `m3.large` penggunaan 2 x, karena bersama-sama instans ini menyumbang 8 dinormalisasi units/hour. This leaves 8 normalized units/hour untuk diterapkan pada `m3.xlarge` instans.

Dengan sisa 8 unit/jam yang dinormalisasi, Instans Terpesan regional `m3.2xlarge` memberikan manfaat penuh untuk 1 x penggunaan `m3.xlarge`, karena setiap instans `m3.xlarge` setara dengan 8 unit/jam yang dinormalisasi. Penggunaan `m3.xlarge` yang tersisa dikenai biaya dengan tarif Sesuai Permintaan.

Skenario 3: Instans Terpesan Regional dalam akun tertaut

Instans Terpesan pertama kali diterapkan untuk penggunaan dalam akun pembelian, diikuti dengan penggunaan yang memenuhi syarat di akun lain mana pun dalam organisasi. Untuk informasi selengkapnya, lihat Instans Terpesan dan penagihan gabungan. Untuk Instans Terpesan regional yang menawarkan fleksibilitas ukuran instans, keuntungan diterapkan dari ukuran instans terkecil hingga terbesar dalam keluarga instans tersebut.

Anda menjalankan Instans Sesuai Permintaan berikut di akun A (akun pembelian):

- 2 x`m4.xlarge` Linux, instans tenancy default di Availability Zone us-east-1a
- 1 x `m4.2xlarge` Linux, instans penghunian default di Zona Ketersediaan us-east-1b
- 2 x `c4.xlarge` Linux, instans penghunian default di Zona Ketersediaan us-east-1a
- 1 x `c4.2xlarge` Linux, instans penghunian default di Zona Ketersediaan us-east-1b

Pelanggan lain menjalankan Instans Sesuai Permintaan berikut di akun B—akun tertaut:

- 2 x `m4.xlarge` Linux, instans penghunian default di Zona Ketersediaan us-east-1a

Anda membeli Instans Terpesan wilayah berikut di akun A:

- 4 x `m4.xlarge` Linux, Instans Terpesan penghunian default di Wilayah us-east-1
- 2 x `c4.xlarge` Linux, Instans Terpesan penghunian default di Wilayah us-east-1

Keuntungan Instans Terpesan regional diterapkan dengan cara berikut:

- Diskon keempat Instans Terpesan `m4.xlarge` digunakan oleh kedua instans `m4.xlarge` dan satu instans `m4.2xlarge` di akun A (akun pembelian). Ketiga instans cocok dengan atribut (keluarga instans, Wilayah, platform, penghunian). Diskon diterapkan ke instans di akun pembelian (akun A) terlebih dahulu, meskipun akun B (akun tertaut) memiliki dua `m4.xlarge` yang juga cocok dengan Instans Terpesan. Tidak ada reservasi kapasitas karena Instans Terpesan adalah Instans Terpesan wilayah.
- Diskon dua Instans Terpesan `c4.xlarge` diterapkan ke kedua instans `c4.xlarge`, karena keduanya adalah ukuran instans yang lebih kecil daripada instans `c4.2xlarge`. Tidak ada reservasi kapasitas karena Instans Terpesan adalah Instans Terpesan wilayah.

Skenario 4: Instans Terpesan Zonal dalam akun tertaut

Secara umum, Instans Terpesan yang dimiliki oleh sebuah akun diterapkan terlebih dahulu ke penggunaan di akun tersebut. Namun, jika ada Instans Terpesan untuk Zona Ketersediaan tertentu (Instans Terpesan zonal) yang berkualifikasi dan tidak digunakan di akun lain dalam organisasi, instans tersebut diterapkan ke akun sebelum Instans Terpesan regional yang dimiliki oleh akun tersebut. Hal ini dilakukan untuk memastikan pemanfaatan Instans Terpesan yang maksimal dan tagihan yang lebih rendah. Untuk tujuan penagihan, semua akun di organisasi diperlakukan sebagai satu akun. Contoh berikut dapat membantu menjelaskan hal ini.

Anda menjalankan Instans Sesuai Permintaan berikut di akun A (akun pembelian):

- 1 x `m4.xlarge` Linux, instans penghunian default di Zona Ketersediaan us-east-1a

Seorang pelanggan menjalankan Instans Sesuai Permintaan berikut di akun B tertaut:

- 1 x `m4.xlarge` Linux, instans penghunian default di Zona Ketersediaan us-east-1b

Anda membeli Instans Terpesan wilayah berikut di akun A:

- 1 x `m4.xlarge` Linux, Instans Terpesan penghunian default di Wilayah us-east-1

Seorang pelanggan juga membeli Instans Terpesan zonal berikut di akun C tertaut:

- 1 x `m4.xlarge` Linux, Instans Terpesan penghunian default di Zona Ketersediaan us-east-1a

Keuntungan Instans Terpesan diterapkan dengan cara berikut:

- Diskon dari Instans Terpesan zonal `m4.xlarge` yang dimiliki oleh akun C diterapkan ke penggunaan `m4.xlarge` di akun A.
- Diskon dari Instans Terpesan regional `m4.xlarge` yang dimiliki oleh akun A diterapkan ke penggunaan `m4.xlarge` di akun B.
- Jika Instans Terpesan regional yang dimiliki oleh akun A diterapkan pada penggunaan di akun A terlebih dahulu, Instans Terpesan zonal yang dimiliki oleh akun C tetap tidak digunakan dan penggunaan di akun B dikenai biaya dengan tarif Sesuai Permintaan.

Untuk informasi selengkapnya, lihat Memahami reservasi Anda di. AWS Cost and Usage Report

> **Note**
>
> Instans Terpesan Zona mereservasi kapasitas untuk akun pemilik saja dan tidak dapat dibagikan dengan Akun AWS lain. Jika Anda perlu berbagi kapasitas dengan Akun AWS lain, gunakan Cadangan kapasitas komputasi dengan Reservasi Kapasitas Sesuai Permintaan EC2.

Menggunakan Instans Terpesan Anda

Instans Terpesan secara otomatis diterapkan untuk menjalankan Instans Sesuai Permintaan asalkan spesifikasinya cocok. Jika Anda tidak memiliki Instans Sesuai Permintaan yang berjalan yang sesuai dengan spesifikasi Instans Terpesan Anda, Instans Terpesan tidak akan digunakan hingga Anda meluncurkan instans dengan spesifikasi yang diperlukan.

Jika Anda meluncurkan Instans Sesuai Permintaan untuk memanfaatkan keuntungan penagihan Instans Terpesan, pastikan Anda menentukan informasi berikut saat mengonfigurasi Instans Sesuai Permintaan:

Platform

Anda harus menentukan Amazon Machine Image (AMI) yang cocok dengan platform (deskripsi produk) dari Instans Terpesan Anda. Misalnya, jika Anda menentukan `Linux/UNIX` untuk instans Terpesan, Anda dapat meluncurkan instans dari AMI Amazon Linux atau AMI Ubuntu.

Jenis instans

Jika membeli Instans Terpesan zonal, Anda harus menentukan tipe instans yang sama dengan Instans Terpesan Anda. Misalnya, `t3.large`. Untuk informasi selengkapnya, lihat Bagaimana Instans Terpesan zonal diterapkan.

Jika membeli Instans Terpesan regional, Anda harus menentukan tipe instans dari keluarga instans yang sama dengan tipe instans dari Instans Terpesan Anda. Misalnya, jika Anda menetapkan `t3.xlarge` untuk Instans Terpesan, Anda harus meluncurkan instans Anda dari keluarga T3, tetapi Anda dapat menentukan berapa pun ukuran apa pun. Misalnya, `t3.medium`. Untuk informasi selengkapnya, lihat Bagaimana Instans Terpesan regional diterapkan.

Zona Ketersediaan

Jika Anda membeli Instans Terpesan zonal untuk Zona Ketersediaan tertentu, Anda harus meluncurkan instans tersebut ke dalam Zona Ketersediaan yang sama.

Jika Anda membeli Instans Terpesan regional, Anda dapat meluncurkan instans ke Zona Ketersediaan mana pun di Wilayah yang Anda tentukan untuk Instans Terpesan tersebut.

Penghunian

Penghunian (`dedicated` atau `shared`) instans Anda harus cocok dengan penghunian Instans Terpesan. Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.

Untuk contoh tentang bagaimana Instans Terpesan diterapkan ke Instans Sesuai Permintaan berjalan Anda, lihat Bagaimana diskon Instans Cadangan diterapkan. Untuk informasi selengkapnya, lihat Mengapa Instans Cadangan Amazon EC2 saya tidak berlaku untuk AWS penagihan saya dengan cara yang saya harapkan?

Anda dapat menggunakan berbagai metode untuk meluncurkan Instans Sesuai Permintaan yang menggunakan diskon Instans Terpesan Anda. Untuk informasi selengkapnya tentang berbagai metode peluncuran, lihat Luncurkan instans Amazon EC2. Anda juga dapat menggunakan Amazon EC2 Auto Scaling untuk meluncurkan instans. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon EC2 Auto Scaling.

Cara kerja penagihan dengan Instans Cadangan

Semua Instans Terpesan menyediakan diskon dibandingkan dengan harga Sesuai Permintaan. Dengan Instans Terpesan, Anda membayar untuk seluruh jangka waktu terlepas dari penggunaan

sebenarnya. Anda dapat memilih untuk membayar Instans Terpesan di muka, sebagian di muka, atau bulanan, tergantung opsi pembayaran yang ditentukan untuk Instans Terpesan.

Saat Instans Terpesan kedaluwarsa, Anda akan dikenai tarif Sesuai Permintaan untuk penggunaan instans EC2. Anda dapat mengantrekan Instans Terpesan untuk pembelian hingga tiga tahun sebelumnya. Hal ini dapat membantu Anda memastikan bahwa Anda memiliki cakupan tanpa gangguan. Untuk informasi selengkapnya, lihat Mengantrekan pembelian Anda.

Tersedia AWS Tingkat Gratis untuk yang baru Akun AWS. Jika Anda menggunakan instans Amazon EC2 AWS Tingkat Gratis untuk menjalankan instans Amazon EC2, dan Anda membeli Instans Cadangan, Anda akan dikenakan harga standar. Untuk informasi, lihat AWS Tingkat Gratis.

Daftar Isi

- Penagihan penggunaan
- Melihat tagihan Anda
- Instans Terpesan dan penagihan gabungan
- Tingkat harga diskon Instans Terpesan

Penagihan penggunaan

Instans Terpesan ditagih untuk setiap jam aktual selama jangka waktu yang Anda pilih, terlepas dari apakah sebuah instans sedang berjalan. Setiap jam aktual dimulai pada jam (nol menit dan nol detik setelah jam) aktual 24 jam standar. Misalnya, 1:00:00 hingga 1:59:59 adalah satu jam-jam. Untuk informasi selengkapnya tentang status instans, lihat Perubahan status EC2 instans Amazon.

Keuntungan penagihan Instans Terpesan dapat diterapkan ke instans yang berjalan dengan basis per detik. Penagihan per detik tersedia untuk instans yang menggunakan distribusi Linux sumber terbuka, seperti Amazon Linux dan Ubuntu. Penagihan per jam digunakan untuk distribusi Linux komersial, seperti Red Hat Enterprise Linux dan SUSE Linux Enterprise Server.

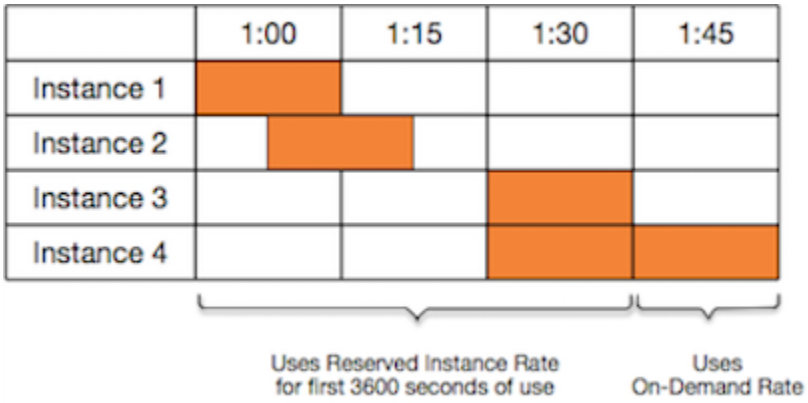
Keuntungan tagihan Instans Terpesan dapat diterapkan ke maksimum 3.600 detik (satu jam) penggunaan instans per jam aktual. Anda dapat menjalankan banyak instans secara bersamaan, tetapi hanya dapat menerima keuntungan diskon Instans Terpesan dengan total 3.600 detik per jam. Penggunaan instans yang melebihi 3.600 detik dalam satu jam akan ditagih dengan tarif Sesuai Permintaan.

Misalnya, jika Anda membeli satu Instans Terpesan `m4.xlarge` dan menjalankan empat `m4.xlarge` Instans secara bersamaan selama satu jam, satu instans dikenai biaya pada satu jam

penggunaan Instans Terpesan dan tiga instans lainnya dikenai biaya pada tiga jam penggunaan Sesuai Permintaan.

Namun, jika Anda membeli satu Instans Terpesan `m4.xlarge` dan menjalankan empat instans `m4.xlarge` selama 15 menit (900 detik) masing-masing dalam jam yang sama, total waktu berjalan untuk instans adalah satu jam, yang menghasilkan satu jam penggunaan Instans Terpesan dan 0 jam penggunaan Sesuai Permintaan.

Jika banyak instans yang memenuhi syarat berjalan secara bersamaan, keuntungan penagihan Instans Terpesan diterapkan ke semua instans pada waktu yang sama hingga maksimum 3.600 detik dalam satu jam. Setelah itu, tarif Sesuai Permintaan berlaku.



Cost Explorer di konsol Manajemen Penagihan dan Biaya memungkinkan Anda menganalisis penghematan terhadap Instans Sesuai Permintaan yang berjalan. FAQ Instans Terpesan menyertakan contoh penghitungan nilai daftar.

Jika Anda menutup AWS akun, penagihan On-Demand untuk sumber daya Anda akan berhenti. Namun, jika Anda memiliki Instans Terpesan di akun, Anda terus menerima tagihan untuk ini hingga kedaluwarsa.

Melihat tagihan Anda

Anda dapat mencari tahu tentang biaya dan tarif ke akun Anda dengan melihat konsol AWS Manajemen Penagihan dan Biaya tersebut.

- Dasbor menampilkan ringkasan pengeluaran untuk akun Anda.
- Pada halaman Tagihan, di bawah Detail, perluas bagian Elastic Compute Cloud dan Wilayah untuk mendapatkan informasi penagihan terkait Instans Terpesan Anda.

Anda dapat melihat tagihannya secara online, atau Anda dapat mengunduh file CSV.

Anda juga dapat melacak penggunaan Instans Cadangan menggunakan Laporan AWS Biaya dan Penggunaan. Untuk informasi selengkapnya, lihat Memahami reservasi Anda.

Instans Terpesan dan penagihan gabungan

Keuntungan harga dari Instans Terpesan dibagikan ketika akun pembelian merupakan bagian dari sekumpulan akun yang ditagih dalam satu akun pembayar penagihan gabungan. Penggunaan instans di semua akun anggota dikumpulkan di akun pembayar setiap bulan. Hal ini biasanya berguna untuk perusahaan yang memiliki tim atau grup fungsional yang berbeda. Kemudian, logika Instans Terpesan normal diterapkan untuk menghitung tagihan. Untuk informasi selengkapnya, lihat Tagihan Gabungan untuk AWS Organizations.

Jika Anda menutup akun yang membeli Instans Terpesan, maka akun pembayar akan dikenai biaya untuk Instans Terpesan hingga Instans Terpesan tersebut kedaluwarsa. Setelah akun yang ditutup dihapus secara permanen dalam 90 hari, akun anggota tidak akan lagi mendapatkan keuntungan dari diskon penagihan Instans Terpesan.

> **Note**
>
> Instans Terpesan Zona mereservasi kapasitas untuk akun pemilik saja dan tidak dapat dibagikan dengan Akun AWS lain. Jika Anda perlu berbagi kapasitas dengan Akun AWS lain, gunakan Cadangan kapasitas komputasi dengan Reservasi Kapasitas Sesuai Permintaan EC2.

Tingkat harga diskon Instans Terpesan

Jika memenuhi syarat untuk tingkat harga diskon, maka akun Anda secara otomatis menerima diskon di muka dan biaya penggunaan instans untuk pembelian Instans Terpesan yang Anda lakukan dalam level tingkat tersebut sejak saat itu. Agar memenuhi syarat untuk mendapatkan diskon, nilai daftar Instans Terpesan Anda di Wilayah harus sebanyak 500.000 USD atau lebih.

Aturan-aturan berikut berlaku:

- Tingkat harga dan diskon terkait hanya berlaku untuk pembelian Instans Terpesan Standar Amazon EC2.
- Tingkat harga tidak berlaku untuk Instans Terpesan Windows dengan SQL Server Standard, SQL Server Web, dan SQL Server Enterprise.
- Tingkatan harga tidak berlaku untuk Instans Cadangan untuk Linux dengan SQL Server dalam bentuk apa pun.
- Diskon tingkat harga hanya berlaku untuk pembelian yang dilakukan dari AWS. Diskon ini tidak berlaku untuk pembelian Instans Terpesan pihak ketiga.
- Tingkat harga diskon saat ini tidak berlaku untuk pembelian Instans Terpesan Konvertibel.

Topik

- Menghitung diskon harga Instans Terpesan
- Membeli dengan tingkat diskon
- Melewati tingkat harga
- Penagihan gabungan untuk tingkatan harga

Menghitung diskon harga Instans Terpesan

Anda dapat menentukan tingkat harga akun dengan menghitung nilai daftar untuk semua Instans Terpesan Anda di suatu Wilayah. Kalikan harga berulang per jam untuk setiap reservasi dengan total jumlah jam untuk jangka waktu tersebut dan tambahkan harga di muka yang tidak didiskon (juga dikenal sebagai harga tetap) pada saat pembelian. Karena didasarkan pada harga yang tidak didiskon (publik), nilai daftar tidak terpengaruh jika Anda memenuhi syarat untuk diskon volume atau jika harga turun setelah Anda membeli Instans Terpesan.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Misalnya, untuk Instans Terpesan `t2.small` Biaya di Muka Sebagian 1 tahun, asumsikan harga di muka adalah USD60,00 dan tarif per jam adalah USD0,007. Ini memberikan nilai daftar sebesar 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

Untuk melihat nilai harga tetap untuk Instans Cadangan menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans Terpesan.
3. Untuk menampilkan kolom Harga di muka, pilih pengaturan
   ( )
   di pojok kanan atas, aktifkan Harga di muka, lalu pilih Konfirmasi.

Untuk melihat nilai harga tetap untuk Instans Terpesan menggunakan baris perintah

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)

Membeli dengan tingkat diskon

Saat Anda membeli Instans Terpesan, Amazon EC2 secara otomatis menerapkan diskon ke bagian pembelian Anda yang termasuk dalam tingkat harga diskon. Anda tidak perlu melakukan sesuatu secara berbeda, dan Anda dapat membeli Instans Terpesan menggunakan salah satu alat Amazon EC2. Untuk informasi selengkapnya, lihat Beli Instans Cadangan untuk Amazon EC2.

Setelah nilai daftar Instans Terpesan aktif Anda di suatu Wilayah melintasi tingkat harga diskon, setiap pembelian Instans Terpesan di Wilayah tersebut pada masa mendatang akan dikenakan tarif diskon. Jika satu pembelian Instans Terpesan di suatu Wilayah membawa Anda melewati ambang batas tingkat diskon, maka porsi pembelian yang berada di atas ambang harga akan dikenakan tarif diskon. Untuk informasi selengkapnya tentang Instans Cadangan sementara IDs yang dibuat selama proses pembelian, lihatMelewati tingkat harga.

Jika nilai daftar Anda berada di bawah titik harga untuk tingkat harga diskon tersebut—misalnya, jika beberapa Instans Terpesan Anda kedaluwarsa—pembelian Instans Terpesan di Wilayah ini pada masa mendatang tidak didiskon. Namun, Anda terus mendapatkan diskon yang berlaku pada setiap Instans Terpesan yang awalnya dibeli dalam tingkat harga diskon.

Saat Anda membeli Instans Terpesan, salah satu dari empat skenario mungkin terjadi:

- Tanpa diskon—Pembelian Anda dalam suatu Wilayah masih di bawah ambang batas diskon.
- Diskon sebagian—Pembelian Anda dalam suatu Wilayah melewati ambang batas tingkat diskon pertama. Tidak ada diskon yang diterapkan untuk satu atau lebih reservasi dan tarif diskon berlaku untuk reservasi yang tersisa.

- Diskon penuh—Seluruh pembelian Anda dalam suatu Wilayah termasuk dalam satu tingkat diskon dan didiskon dengan tepat.
- Dua tarif diskon—Pembelian Anda dalam suatu Wilayah melintasi dari tingkat diskon yang lebih rendah ke tingkat diskon yang lebih tinggi. Anda akan dikenai dua tarif berbeda: satu atau beberapa reservasi dengan tarif diskon lebih rendah, dan reservasi lainnya dengan tarif diskon lebih tinggi.

Melewati tingkat harga

Jika pembelian masuk ke tingkat harga diskon, Anda akan melihat banyak entri untuk pembelian itu: satu untuk bagian pembelian yang ditagih dengan harga reguler, dan yang lain untuk bagian pembelian yang ditagih dengan tarif diskon yang berlaku.

Layanan Instans Cadangan menghasilkan beberapa Instans Cadangan IDs karena pembelian Anda berpindah dari tingkat yang tidak didiskon, atau dari satu tingkat diskon ke tingkat yang lain. Ada ID untuk setiap set reservasi dalam satu tingkatan. Akibatnya, ID yang dikembalikan oleh perintah CLI atau tindakan API pembelian Anda berbeda dari ID Instans Terpesan baru yang sebenarnya.

Penagihan gabungan untuk tingkatan harga

Akun penagihan gabungan menggabungkan nilai daftar akun anggota dalam satu Wilayah. Ketika nilai daftar dari semua Instans Terpesan yang aktif untuk akun penagihan gabungan mencapai tingkat harga diskon, setiap Instans Terpesan yang dibeli setelah titik ini oleh anggota mana pun dari akun penagihan gabungan akan dikenakan tarif diskon (selama nilai daftar untuk itu akun gabungan tersebut tetap di atas ambang batas tingkat harga diskon). Untuk informasi selengkapnya, lihat Instans Terpesan dan penagihan gabungan.

Beli Instans Cadangan untuk Amazon EC2

Untuk membeli Instans Cadangan untuk Amazon EC2, Anda dapat menggunakan konsol Amazon EC2, alat baris perintah, atau SDK untuk mencari penawaran Instans Cadangan AWS dari dan penjual pihak ketiga, menyesuaikan parameter penelusuran hingga menemukan kecocokan persis yang Anda cari.

Saat mencari Instans Terpesan untuk dibeli, Anda menerima penawaran kuota dari penawaran yang ditampilkan. Saat Anda melanjutkan pembelian, AWS secara otomatis menempatkan batas harga pada harga pembelian. Total biaya Instans Terpesan Anda tidak akan melebihi jumlah kuota Anda.

Jika harga naik atau berubah untuk alasan apa pun, pembelian tidak selesai. Saat Anda membeli Instans Cadangan penjual pihak ketiga dari Marketplace Instans Cadangan Amazon EC2, jika ada

penawaran yang mirip dengan pilihan Anda tetapi dengan harga di muka yang lebih rendah, AWS menjual penawaran dengan harga di muka yang lebih rendah.

Sebelum Anda mengonfirmasi pembelian, tinjau detail Instans Terpesan yang akan dibeli dan pastikan semua parameternya akurat. Setelah membeli Instans Cadangan (baik dari penjual pihak ketiga di Marketplace Instans Cadangan atau dari AWS), Anda tidak dapat membatalkan pembelian. Anda dapat mengantri pembelian untuk tanggal masa depan, dan membatalkan pembelian antrian sebelum waktu yang dijadwalkan.

Untuk membeli dan memodifikasi Instans Terpesan, pastikan bahwa pengguna Anda memiliki izin yang sesuai, seperti kemampuan untuk menjelaskan Zona Ktersediaan. Untuk selengkapnya, lihat the section called “Cara Menggunakan Instans Cadangan” (API) atau the section called “Cara Menggunakan Instans Cadangan” (konsol).

Tugas

- Memilih platform
- Mengantrekan pembelian Anda
- Membeli Instans Terpesan Standar
- Membeli Instans Terpesan Konvertibel
- Membeli dari Marketplace Instans Terpesan
- Membatalkan antrean pembelian
- Memperbarui Instans Terpesan

Memilih platform

Amazon EC2 mendukung platform berikut untuk Instans Cadangan:

- Linux/UNIX
- Linux dengan SQL Server Standard
- Linux dengan SQL Server Web
- Linux dengan SQL Server Enterprise
- SUSE Linux
- Linux Red Hat Enterprise
- Linux Red Hat Enterprise dengan HA

- Windows
- Windows dengan SQL Server Standard
- Windows dengan SQL Server Web
- Windows dengan SQL Server Enterprise

Pertimbangan-pertimbangan

- Jika Anda membawa langganan yang ada (BYOS) untuk Red Hat Enterprise Linux, SUSE Linux, atau Ubuntu Pro, Anda harus memilih penawaran untuk platform Linux/Unix.
- Instans Cadangan tidak didukung pada instans yang menjalankan macOS atau Ubuntu Pro (termasuk langganan EC2, yaitu, bukan BYOS). Untuk menyimpan dengan harga instans Sesuai Permintaan, sebaiknya gunakan instans macOS dan Ubuntu Pro (termasuk langganan EC2) dengan Savings Plans. Untuk informasi selengkapnya, lihat Panduan Pengguna Savings Plans.

Untuk memastikan bahwa instance berjalan dalam Instans Cadangan tertentu, platform Instans Cadangan harus cocok dengan platform AMI yang digunakan untuk meluncurkan instance. Untuk Linux AMIs, penting untuk memeriksa apakah platform AMI menggunakan nilai umum Linux/UNIX atau nilai yang lebih spesifik seperti SUSE Linux.

Console

Untuk memeriksa platform AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI.
4. Pada tab Detail, perhatikan nilai detail Platform.

AWS CLI

Untuk memeriksa platform AMI

Gunakan perintah deskripsi-gambar dan periksa nilai. `PlatformDetails`

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
```

```
    --query Images[*].PlatformDetails
```

Berikut ini adalah output contoh.

```
[
    "Linux/UNIX"
]
```

PowerShell

Untuk memeriksa platform AMI

Gunakan Get-EC2Imagecmdlet dan periksa nilai. `PlatformDetails`

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Select PlatformDetails
```

Berikut ini adalah output contoh.

```
PlatformDetails
---------------
Linux/UNIX
```

Mengantrekan pembelian Anda

Secara default, saat Anda membeli Instans Terpesan, pembelian tersebut langsung dibuat. Atau, Anda dapat mengantrekan pembelian untuk tanggal dan waktu pada masa mendatang. Misalnya, Anda dapat mengantrekan pembelian sekitar waktu Instans Terpesan yang ada kedaluwarsa. Hal ini dapat membantu Anda memastikan bahwa Anda memiliki cakupan tanpa gangguan.

Anda dapat mengantrekan pembelian untuk Instans Terpesan regional, tetapi tidak untuk Instans Terpesan zonal atau Instans Terpesan dari penjual lain. Anda dapat mengantrekan pembelian hingga tiga tahun ke depan. Pada tanggal dan waktu yang dijadwalkan, pembelian dilakukan menggunakan metode pembayaran default. Setelah pembayaran berhasil, keuntungan penagihan diterapkan.

Anda dapat menetapkan tanggal untuk pembelian antrian Anda di konsol Amazon EC2, dan pembelian antri hingga 00:00 UTC pada tanggal ini. Untuk menentukan waktu yang berbeda untuk pembelian antrian, gunakan AWS SDK atau alat baris perintah.

Anda dapat melihat antrean pembelian Anda di konsol Amazon EC2. Status antrean pembelian adalah antre. Anda dapat membatalkan antrean pembelian kapan saja sebelum waktu yang dijadwalkan. Untuk detailnya, lihat Membatalkan antrean pembelian.

Membeli Instans Terpesan Standar

Anda dapat membeli Instans Terpesan Standar di Zona Ketersediaan tertentu dan mendapatkan reservasi kapasitas. Atau, Anda dapat melepaskan reservasi kapasitas dan membeli Instans Terpesan Standar regional.

Setelah pembelian selesai, jika Anda sudah memiliki instans berjalan yang cocok dengan spesifikasi Instans Terpesan, keuntungan penagihan langsung diterapkan. Anda tidak perlu me-restart instance Anda. Jika Anda tidak memiliki instans berjalan yang sesuai, luncurkan instance dan pastikan bahwa Anda cocok dengan kriteria persis yang Anda tentukan untuk Instans Cadangan Anda. Untuk informasi selengkapnya, lihat Menggunakan Instans Terpesan Anda.

Untuk contoh tentang bagaimana Instans Terpesan diterapkan ke instans berjalan Anda, lihat Bagaimana diskon Instans Cadangan diterapkan.

Console

Untuk membeli Instans Cadangan Standar

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans Terpesan, lalu pilih Beli Instans Terpesan.
3. Untuk Kelas Penawaran, pilih Standar untuk menampilkan Tnstans Terpesan Standar.
4. Untuk membeli reservasi kapasitas, aktifkan Hanya tampilkan penawaran yang memiliki kapasitas di sudut kanan atas layar pembelian. Ketika Anda mengaktifkan pengaturan ini, bidang Zona Ketersediaan akan muncul.

   Untuk membeli Instans Terpesan wilayah, nonaktifkan pengaturan ini. Ketika Anda menonaktifkan pengaturan ini, bidang Zona Ketersediaan akan hilang.
5. Pilih konfigurasi lain sesuai kebutuhan, lalu pilih Cari.
6. Untuk setiap Instans Terpesan yang ingin Anda beli, masukkan jumlah yang diinginkan, dan pilih Tambahkan ke keranjang.

   Untuk membeli Instans Terpesan Standar dari Marketplace Instans Terpesan, cari Pihak ke-3 di kolom Penjual pada hasil pencarian. Kolom Istilah menampilkan istilah nonstandar. Untuk informasi selengkapnya, lihat Membeli dari Marketplace Instans Terpesan.

7. Untuk melihat ringkasan Instans Terpesan yang Anda pilih, klik Lihat keranjang.
8. Jika Pesanan pada adalah Sekarang, pembelian akan segera diselesaikan setelah Anda memilih Pesan semua. Untuk mengantrekan pembelian, pilih Sekarang dan pilih tanggal. Anda dapat memilih tanggal yang berbeda untuk setiap penawaran yang memenuhi syarat di keranjang. Pembelian diantrekan sampai pukul 00:00 UTC pada tanggal yang dipilih.
9. Untuk menyelesaikan pesanan, pilih Pesan semua.

   Jika, pada saat melakukan pemesanan, ada penawaran yang mirip dengan pilihan Anda tetapi dengan harga lebih rendah, AWS menjual penawaran kepada Anda dengan harga lebih rendah.
10. Pilih Tutup.

    Status pesanan Anda tercantum di kolom Status. Ketika pesanan Anda selesai, nilai Status berubah dari `Payment-pending` menjadi.`Active` Ketika Instans Terpesan sudah `Active`, instans tersebut siap digunakan.

    Jika statusnya masuk ke`Retired`, AWS mungkin belum menerima pembayaran Anda.

AWS CLI

Untuk membeli Instans Cadangan Standar

1. Temukan Instans Cadangan yang tersedia menggunakan describe-reserved-instances-offeringsperintah. Tentukan `--offering-class` opsi `standard` untuk mengembalikan hanya Instans Cadangan Standar. Anda dapat menerapkan kriteria tambahan untuk mempersempit hasil Anda. Misalnya, gunakan perintah berikut untuk membeli Instans `t2.large` Cadangan regional dengan penyewaan default `Linux/UNIX` untuk jangka waktu 1 tahun saja.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=duration,Values=31536000 \
              Name=scope,Values=Region
```

Untuk menemukan Instans Terpesan di Marketplace Instans Terpesan saja, gunakan filter `marketplace` dan jangan tentukan durasi dalam permintaan karena jangka waktu mungkin lebih pendek dari jangka waktu 1 atau 3 tahun.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

Saat Anda menemukan Instans Terpesan yang memenuhi kebutuhan Anda, catat ID penawarannya. Contoh:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Gunakan purchase-reserved-instances-offeringperintah untuk membeli Instans Cadangan Anda. Anda harus menentukan ID penawaran Instans Terpesan yang Anda peroleh pada langkah sebelumnya dan Anda harus menentukan jumlah instans untuk reservasi.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Secara default, pembelian segera diselesaikan. Atau, untuk mengantri pembelian, tambahkan opsi berikut ke panggilan sebelumnya.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Gunakan describe-reserved-instancesperintah untuk mendapatkan status Instans Cadangan Anda.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327 \
    --query ReservedInstances[].State
```

PowerShell

Untuk membeli Instans Cadangan Standar

1. Temukan Instans Cadangan yang tersedia menggunakan Get-EC2ReservedInstancesOfferingcmdlet. Tetapkan `standard` untuk parameter `-OfferingClass` agar hanya menampilkan Instans Terpesan Standar. Anda dapat menerapkan kriteria tambahan untuk mempersempit hasil Anda. Misalnya, gunakan perintah berikut untuk membeli Instans `t2.large` Cadangan regional dengan penyewaan default `Linux/UNIX` untuk jangka waktu 1 tahun saja.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType "t2.large" `
    -OfferingClass "standard" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy "default" `
    -Filters @{Name="duration"; Values="31536000"} `
             @{Name="scope"; Values="Region"
```

   Untuk menemukan Instans Terpesan di Marketplace Instans Terpesan saja, gunakan filter `marketplace` dan jangan tentukan durasi dalam permintaan karena jangka waktu mungkin lebih pendek dari jangka waktu 1 atau 3 tahun.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType t2.large `
    -OfferingClass "standard" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy default `
    -Filters @{Name="marketplace"; Values="true"}
```

   Saat Anda menemukan Instans Terpesan yang memenuhi kebutuhan Anda, catat ID penawarannya. Contoh:

```
bec624df-a8cc-4aad-a72f-4f8abc34caf2
```

2. Gunakan New-EC2ReservedInstancecmdlet untuk membeli Instans Cadangan Anda. Anda harus menentukan ID penawaran Instans Terpesan yang Anda peroleh pada langkah sebelumnya dan Anda harus menentukan jumlah instans untuk reservasi.

```
New-EC2ReservedInstance `
```

```
    -ReservedInstancesOfferingId "bec624df-a8cc-4aad-a72f-4f8abc34caf2" `
    -InstanceCount 1
```

Secara default, pembelian segera diselesaikan. Atau, untuk mengantrekan pembelian, tambahkan parameter berikut ke panggilan sebelumnya.

```
-PurchaseTime "2020-12-01T00:00:00Z"
```

3. Gunakan Get-EC2ReservedInstancecmdlet untuk mendapatkan status Instans Cadangan Anda.

```
Get-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327 | `
    Select State
```

Membeli Instans Terpesan Konvertibel

Anda dapat membeli Instans Terpesan Konvertibel di Zona Ketersediaan tertentu dan mendapatkan reservasi kapasitas. Atau, Anda dapat melepaskan reservasi kapasitas dan membeli Instans Terpesan Konvertibel regional.

Jika Anda sudah memiliki instans berjalan yang cocok dengan spesifikasi Instans Terpesan, keuntungan penagihan langsung diterapkan. Anda tidak perlu memulai ulang instans Anda. Jika Anda tidak memiliki instans berjalan yang cocok, luncurkan sebuah instans dan pastikan kesamaannya dengan kriteria yang sudah Anda tentukan untuk Instans Terpesan Anda. Untuk informasi selengkapnya, lihat Menggunakan Instans Terpesan Anda.

Untuk contoh tentang bagaimana Instans Terpesan diterapkan ke instans berjalan Anda, lihat Bagaimana diskon Instans Cadangan diterapkan.

Console

Untuk membeli Instans Cadangan Konvertibel

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans Terpesan, lalu pilih Beli Instans Terpesan.
3. Untuk Kelas Penawaran, pilih Konvertibel untuk menampilkan Instans Terpesan Konvertibel.

4. Untuk membeli reservasi kapasitas, aktifkan Hanya tampilkan penawaran yang memiliki kapasitas di sudut kanan atas layar pembelian. Ketika Anda mengaktifkan pengaturan ini, bidang Zona Ketersediaan akan muncul.

   Untuk membeli Instans Terpesan wilayah, nonaktifkan pengaturan ini. Ketika Anda menonaktifkan pengaturan ini, bidang Zona Ketersediaan akan hilang.

5. Pilih konfigurasi lain sesuai kebutuhan dan pilih Cari.
6. Untuk setiap Instans Terpesan Konvertibel yang ingin Anda beli, masukkan jumlahnya, dan pilih Tambahkan ke keranjang.
7. Untuk melihat ringkasan pilihan Anda, pilih Lihat keranjang.
8. Jika Pesanan pada adalah Sekarang, pembelian akan segera diselesaikan setelah Anda memilih Pesan semua. Untuk mengantrekan pembelian, pilih Sekarang dan pilih tanggal. Anda dapat memilih tanggal yang berbeda untuk setiap penawaran yang memenuhi syarat di keranjang. Pembelian diantrekan sampai pukul 00:00 UTC pada tanggal yang dipilih.
9. Untuk menyelesaikan pesanan, pilih Pesan semua.

   Jika, pada saat melakukan pemesanan, ada penawaran yang mirip dengan pilihan Anda tetapi dengan harga lebih rendah, AWS menjual penawaran kepada Anda dengan harga lebih rendah.

10. Pilih Tutup.

    Status pesanan Anda tercantum di kolom Status. Ketika pesanan Anda selesai, nilai Status berubah dari `Payment-pending` menjadi.`Active` Ketika Instans Terpesan sudah `Active`, instans tersebut siap digunakan.

    Jika statusnya masuk ke`Retired`, AWS mungkin belum menerima pembayaran Anda.

AWS CLI

Untuk membeli Instans Cadangan Konvertibel

1. Temukan Instans Cadangan yang tersedia menggunakan describe-reserved-instances-offeringsperintah. Tentukan `--offering-class` opsi `convertible` untuk mengembalikan hanya Instans Cadangan Konvertibel. Anda dapat menerapkan kriteria tambahan untuk mempersempit hasil Anda. Misalnya, gunakan perintah berikut untuk membeli Instans `t2.large` Cadangan regional dengan penyewaan default untuk`Linux/UNIX`.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class convertible \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=scope,Values=Region
```

Saat Anda menemukan Instans Terpesan yang memenuhi kebutuhan Anda, catat ID penawarannya. Contoh:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Gunakan purchase-reserved-instances-offeringperintah untuk membeli Instans Cadangan Anda. Anda harus menentukan ID penawaran Instans Terpesan yang Anda peroleh pada langkah sebelumnya dan Anda harus menentukan jumlah instans untuk reservasi.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Secara default, pembelian segera diselesaikan. Atau, untuk mengantri pembelian, tambahkan opsi berikut ke panggilan sebelumnya.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Gunakan describe-reserved-instancesperintah untuk mendapatkan status Instans Cadangan Anda.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327 \
    --query ReservedInstances[].State
```

PowerShell

Untuk membeli Instans Cadangan Konvertibel

1. Temukan Instans Cadangan yang tersedia menggunakan Get-EC2ReservedInstancesOfferingcmdlet. Tentukan `convertible` untuk parameter -

`OfferingClass` agar hanya menampilkan Instans Terpesan Konvertibel. Anda dapat menerapkan kriteria tambahan untuk mempersempit hasil Anda. Misalnya, gunakan perintah berikut untuk membeli Instans `t2.large` Cadangan regional dengan penyewaan default untuk`Linux/UNIX`.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType "t2.large" `
    -OfferingClass "convertible" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy "default" `
    -Filters @{Name="scope"; Values="Region"
```

Saat Anda menemukan Instans Terpesan yang memenuhi kebutuhan Anda, catat ID penawarannya. Contoh:

```
bec624df-a8cc-4aad-a72f-4f8abc34caf2
```

2. Gunakan New-EC2ReservedInstancecmdlet untuk membeli Instans Cadangan Anda. Anda harus menentukan ID penawaran Instans Cadangan yang Anda dapatkan pada langkah sebelumnya dan Anda harus menentukan jumlah instans untuk reservasi.

```
New-EC2ReservedInstance `
    -ReservedInstancesOfferingId "bec624df-a8cc-4aad-a72f-4f8abc34caf2" `
    -InstanceCount 1
```

Secara default, pembelian segera diselesaikan. Atau, untuk mengantrekan pembelian, tambahkan parameter berikut ke panggilan sebelumnya.

```
-PurchaseTime "2020-12-01T00:00:00Z"
```

3. Gunakan Get-EC2ReservedInstancecmdlet untuk mendapatkan status Instans Cadangan Anda.

```
Get-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327 | `
    Select State
```

Membeli dari Marketplace Instans Terpesan

Anda dapat membeli Instans Terpesan dari penjual pihak ketiga yang memiliki Instans Terpesan yang tidak lagi diperlukan dari Marketplace Instans Terpesan. Anda dapat melakukan hal ini menggunakan konsol Amazon EC2 atau alat baris perintah. Prosesnya mirip dengan membeli Instans Cadangan dari AWS. Untuk informasi selengkapnya, lihat Membeli Instans Terpesan Standar.

Ada beberapa perbedaan antara Instans Cadangan yang dibeli di Marketplace Instans Cadangan dan Instans Cadangan yang dibeli langsung dari: AWS

- Jangka Waktu – Instans Terpesan yang Anda beli dari penjual pihak ketiga memiliki sisa jangka waktu kurang dari standar penuh. Ketentuan standar penuh dari AWS berjalan selama satu tahun atau tiga tahun.
- Harga di muka – Instans Terpesan pihak ketiga dapat dijual dengan harga di muka yang berbeda. Biaya penggunaan atau berulang tetap sama dengan biaya yang ditetapkan saat Instans Terpesan awalnya dibeli dari AWS.
- Tipe Instans Terpesan – Hanya Instans Terpesan Standar Amazon EC2 yang dapat dibeli dari Marketplace Instans Terpesan. Instans Cadangan Konvertibel, Amazon RDS, dan Instans ElastiCache Cadangan Amazon tidak tersedia untuk dibeli di Marketplace Instans Cadangan.

Informasi dasar tentang Anda dibagikan dengan penjual. Misalnya, kode pos dan informasi negara Anda.

Informasi ini memungkinkan penjual untuk menghitung pajak transaksi yang diperlukan yang harus mereka serahkan kepada pemerintah (seperti pajak penjualan atau pajak pertambahan nilai) dan disediakan sebagai laporan pencairan. Dalam keadaan yang jarang terjadi, AWS mungkin harus memberikan penjual dengan alamat email Anda, sehingga mereka dapat menghubungi Anda mengenai pertanyaan yang terkait dengan penjualan (misalnya, pertanyaan pajak).

Untuk alasan yang sama, AWS bagikan nama badan hukum penjual pada faktur pembelian pembeli. Jika Anda memerlukan informasi tambahan tentang penjual untuk pajak atau alasan terkait, hubungi Dukungan.

Membatalkan antrean pembelian

Anda dapat mengantrekan pembelian hingga tiga tahun ke depan. Anda dapat membatalkan antrean pembelian kapan saja sebelum waktu yang dijadwalkan.

Console

Untuk membatalkan pembelian antrian

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans Terpesan.
3. Pilih satu atau lebih Instans Terpesan.
4. Pilih Tindakan, Hapus antrean Instans Terpesan.
5. Ketika diminta untuk mengonfirmasi, masukkan Hapus, lalu Tutup.

AWS CLI

Untuk membatalkan antrean pembelian

Gunakan perintah delete-queued-reserved-instances.

```
aws ec2 delete-queued-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327
```

PowerShell

Untuk membatalkan antrean pembelian

Gunakan Remove-EC2QueuedReservedInstancecmdlet.

```
Remove-EC2QueuedReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327
```

Memperbarui Instans Terpesan

Anda dapat memperbarui Instans Terpesan sebelum dijadwalkan kedaluwarsa. Memperbarui Instans Terpesan akan mengantrekan pembelian Instans Terpesan dengan konfigurasi yang sama hingga Instans Terpesan saat ini kedaluwarsa.

Anda harus memperbarui Instans Cadangan menggunakan konsol Amazon EC2.

Untuk memperpanjang Instans Terpesan menggunakan pembelian yang diantrekan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Di panel navigasi, pilih Instans Terpesan.
3. Pilih Instans Terpesan yang akan diperpanjang.
4. Pilih Tindakan, Perpanjang Instans Terpesan.
5. Untuk menyelesaikan pesanan, pilih Pesan semua, lalu Tutup.

Jual Instans Cadangan untuk Amazon EC2 di Marketplace Instans Cadangan

Marketplace Instans Cadangan Amazon EC2 adalah platform yang memfasilitasi penjualan Instans Cadangan Standar yang tidak digunakan dari AWS pelanggan dan penjual pihak ketiga. Instans Cadangan ini dapat bervariasi dalam jangka waktu dan opsi harga. Anda mungkin ingin menjual Instans Cadangan saat tidak lagi membutuhkannya, seperti saat memindahkan instans ke instans baru AWS Region, mengubah ke jenis instans yang berbeda, menyelesaikan proyek sebelum jangka waktu Instans Cadangan berakhir, kebutuhan bisnis Anda berubah, atau Anda memiliki kapasitas berlebih.

Segera setelah Anda mencantumkan Instans Terpesan di Marketplace Instans Terpesan, instans tersebut akan tersedia untuk ditemukan oleh calon pembeli. Semua Instans Terpesan dikelompokkan menurut durasi sisa jangka waktu dan harga per jam.

Untuk memenuhi permintaan pembeli untuk membeli Instans Cadangan penjual pihak ketiga melalui Marketplace Instans Cadangan, AWS pertama-tama jual Instans Cadangan dengan harga dimuka terendah dalam pengelompokan yang ditentukan. Kemudian, AWS jual Instans Cadangan dengan harga terendah berikutnya, sampai seluruh pesanan pembeli terpenuhi. AWS kemudian memproses transaksi dan mentransfer kepemilikan Instans Cadangan kepada pembeli.

Anda memiliki Instans Terpesan hingga terjual. Setelah penjualan, Anda telah melepaskan reservasi kapasitas dan diskon biaya berulang. Jika Anda terus menggunakan instans, AWS membebankan harga Sesuai Permintaan mulai dari saat Instans Terpesan Anda dijual.

Jika ingin menjual Instans Terpesan yang tidak digunakan di Marketplace Instans Terpesan, Anda harus memenuhi kriteria kelayakan tertentu.

Untuk informasi tentang membeli Instans Terpesan di Marketplace Instans Terpesan, lihat Membeli dari Marketplace Instans Terpesan.

Daftar Isi

- Pembatasan dan batasan
- Mendaftar sebagai penjual

- Rekening bank untuk pencairan
- Informasi pajak
- Menentukan Harga Instans Terpesan Anda
- Mengiklankan Instans Terpesan Anda
- Status iklan Instans Terpesan
- Siklus hidup iklan
- Setelah Instans Terpesan Anda terjual
- Mendapatkan pembayaran
- Informasi yang dibagikan dengan pembeli

Pembatasan dan batasan

Sebelum dapat menjual reservasi yang tidak digunakan, Anda harus mendaftar sebagai penjual di Marketplace Instans Terpesan. Untuk informasi, lihat Mendaftar sebagai penjual.

Batasan dan larangan berikut berlaku saat menjual Instans Terpesan:

- Hanya Instans Terpesan regional dan zonal Standar Amazon EC2 yang dapat dijual di Marketplace Instans Terpesan.
- Instans Cadangan Amazon EC2 Convertible tidak dapat dijual di Marketplace Instans Cadangan.
- Instans Cadangan untuk AWS layanan lain, seperti Amazon RDS dan Amazon ElastiCache, tidak dapat dijual di Marketplace Instans Cadangan.
- Harus ada setidaknya satu bulan tersisa dalam jangka waktu Instans Terpesan Standar.
- Anda tidak dapat menjual Instans Cadangan Standar di Wilayah yang dinonaktifkan secara default.
- Harga minimum yang diizinkan di Marketplace Instans Terpesan adalah 0,00 USD.
- Anda dapat menjual Instans Terpesan Tanpa Biaya di Muka, Sebagian di Muka, atau Semua di Muka di Marketplace Instans Terpesan selama instans aktif di akun Anda setidaknya selama 30 hari. Selain itu, jika ada pembayaran di muka pada Instans Cadangan, itu hanya dapat dijual AWS setelah menerima pembayaran di muka.
- Anda tidak dapat menjual Instans Cadangan di Marketplace Instans Cadangan jika membelinya menggunakan volume discount.
- Anda tidak dapat mengubah daftar di Marketplace Instans Terpesan secara langsung. Namun, Anda dapat mengubah daftar Anda dengan membatalkannya terlebih dahulu, lalu membuat daftar

lain dengan parameter baru. Untuk informasi, lihat Menentukan Harga Instans Terpesan Anda. Anda juga dapat memodifikasi Instans Terpesan sebelum mendaftarnya. Untuk informasi, lihat Memodifikasi Instans Terpesan.

- AWS membebankan biaya layanan sebesar 12 persen dari total harga dimuka setiap Instans Cadangan Standar yang Anda jual di Marketplace Instans Cadangan. Harga di muka adalah harga yang dibebankan penjual untuk Instans Terpesan Standar.
- Saat Anda mendaftar sebagai penjual, bank yang Anda tentukan harus memiliki alamat AS. Untuk informasi selengkapnya, lihat Persyaratan penjual tambahan untuk produk berbayar di Panduan Penjual AWS Marketplace .
- Pelanggan Amazon Web Services India Private Limited (AWS India) tidak dapat mendaftar sebagai penjual di Marketplace Instans Cadangan EC2 dan tidak dapat mencantumkan atau menjual Instans Cadangan di Marketplace Instans Cadangan EC2, meskipun mereka memiliki rekening bank AS. Untuk informasi lebih lanjut, lihat Apa perbedaan antara akun AWS India Akun AWS dan India?
- Jika Anda mengubah penjual catatan menjadi Amazon Web Services India Private Limited (AWS India), Anda akan dideregistrasi sebagai penjual dari Marketplace Instans Cadangan EC2 dan semua iklan aktif yang ada di Marketplace Instans Cadangan EC2 akan dihapus. Untuk mengembalikan status penjual Anda, Anda harus mengubah lokasi akun Anda ke negara selain India dan menyelesaikan proses pendaftaran penjual lagi.

Mendaftar sebagai penjual

> **Note**
>
> Hanya yang Pengguna root akun AWS dapat mendaftarkan akun sebagai penjual.

Untuk menjual di Marketplace Instans Terpesan, Anda harus mendaftar sebagai penjual terlebih dahulu. Selama pendaftaran, Anda memberikan informasi berikut:

- Informasi bank —AWS harus memiliki informasi bank Anda untuk mencairkan dana yang dikumpulkan saat Anda menjual reservasi Anda. Bank yang Anda tentukan harus memiliki alamat AS. Untuk informasi selengkapnya, lihat Rekening bank untuk pencairan.
- Informasi pajak—Semua penjual wajib menyelesaikan wawancara informasi pajak untuk menentukan kewajiban pelaporan pajak yang diperlukan. Untuk informasi selengkapnya, lihat Informasi pajak.

Setelah AWS menerima pendaftaran penjual yang telah selesai, Anda menerima email yang mengonfirmasi pendaftaran dan memberi tahu Anda bahwa Anda dapat mulai menjual di Marketplace Instans Cadangan.

Rekening bank untuk pencairan

AWS harus memiliki informasi bank Anda untuk mencairkan dana yang dikumpulkan saat Anda menjual Instans Cadangan Anda. Bank yang Anda tentukan harus memiliki alamat di AS. Untuk informasi selengkapnya, lihat Persyaratan penjual tambahan untuk produk berbayar di Panduan Penjual AWS Marketplace .

Untuk mendaftarkan rekening bank default untuk pencairan

1. Buka halaman Pendaftaran Penjual Marketplace Instans Terpesan dan masuk menggunakan kredensial AWS Anda.
2. Pada halaman Kelola Rekening Bank, berikan informasi tentang bank berikut untuk menerima pembayaran:

   - Nama Pemilik Rekening Bank
   - Nomor perutean
   - Nomor rekening
   - Tipe rekening bank

   > **Note**
   >
   > Jika menggunakan rekening bank perusahaan, Anda akan diminta untuk mengirimkan informasi tentang rekening bank tersebut melalui faks (1-206-765-3424).

Setelah pendaftaran, rekening bank yang diberikan ditetapkan sebagai default, menunggu verifikasi dari bank. Diperlukan waktu hingga dua minggu untuk memverifikasi rekening bank baru, selama itu Anda tidak dapat menerima pencairan. Untuk rekening yang sudah ditetapkan, biasanya diperlukan waktu sekitar dua hari untuk menyelesaikan pembayaran.

Untuk mengubah rekening bank default untuk pencairan

1. Pada halaman Pendaftaran Penjual Marketplace Instans Terpesan, masuk dengan akun yang Anda gunakan saat mendaftar.

2. Pada halaman Kelola Rekening Bank, tambahkan rekening bank baru atau ubah rekening bank default sesuai kebutuhan.

Informasi pajak

Penjualan Instans Terpesan Anda mungkin dikenai pajak berbasis transaksi, seperti pajak penjualan atau pajak pertambahan nilai. Anda harus memeriksanya dengan departemen pajak, hukum, keuangan, atau akuntansi bisnis Anda untuk menentukan apakah pajak berbasis transaksi berlaku. Anda bertanggung jawab untuk mengumpulkan dan mengirim pajak berbasis transaksi ke otoritas pajak yang sesuai.

Sebagai bagian dari proses pendaftaran penjual, Anda harus menyelesaikan wawancara pajak di Portal Pendaftaran Penjual. Wawancara tersebut mengumpulkan informasi pajak Anda dan mengisi formulir IRS W-9, W-8BEN, atau W-8BEN-E, yang digunakan untuk menentukan kewajiban pelaporan pajak yang diperlukan.

Informasi pajak yang Anda masukkan sebagai bagian dari wawancara pajak mungkin berbeda, bergantung pada apakah Anda beroperasi sebagai individu atau bisnis, dan apakah Anda atau bisnis Anda adalah orang atau entitas AS atau non-AS. Saat Anda mengisi wawancara pajak, perhatikan hal-hal berikut:

- Informasi yang diberikan oleh AWS, termasuk informasi dalam topik ini, bukan merupakan nasihat pajak, hukum, atau profesional lainnya. Untuk mengetahui bagaimana persyaratan pelaporan IRS dapat memengaruhi bisnis Anda, atau jika Anda memiliki pertanyaan lain, hubungi penasihat pajak, hukum, atau profesional lainnya.
- Untuk memenuhi persyaratan pelaporan IRS seefisien mungkin, jawab semua pertanyaan dan masukkan semua informasi yang diminta selama wawancara.
- Periksa jawaban Anda. Hindari salah eja atau salah memasukkan nomor identifikasi pajak. Kesalahan tersebut dapat mengakibatkan formulir pajak tidak valid.

Berdasarkan respons wawancara pajak dan ambang batas pelaporan IRS Anda, Amazon mungkin mengajukan Formulir 1099-K. Amazon mengirimkan salinan Formulir 1099-K Anda pada atau sebelum tanggal 31 Januari pada tahun setelah tahun ketika akun pajak Anda mencapai tingkat ambang batas. Misalnya, jika akun Anda mencapai ambang batas pada tahun 2018, Formulir 1099-K Anda akan dikirimkan pada atau sebelum tanggal 31 Januari 2019.

Untuk informasi lebih lanjut tentang persyaratan IRS dan Formulir 1099-K, lihat Formulir FAQs 1099-K di situs web IRS.

Menentukan Harga Instans Terpesan Anda

Saat menetapkan harga untuk Instans Terpesan Anda, pertimbangkan hal berikut:

- Harga di muka – Harga di muka adalah satu-satunya harga yang dapat Anda tentukan untuk Instans Terpesan yang Anda jual. Harga dimuka adalah harga satu kali yang dibayar pembeli ketika mereka membeli setiap Instans Cadangan.

  Karena nilai Instans Cadangan menurun dari waktu ke waktu, secara default, AWS dapat menetapkan harga untuk menurun dalam kenaikan yang sama dari bulan ke bulan. Namun, Anda dapat menetapkan harga di muka yang berbeda berdasarkan kapan reservasi Anda terjual. Misalnya, jika Instans Terpesan Anda memiliki sisa jangka waktu sembilan bulan, Anda dapat menentukan jumlah yang ingin Anda terima jika pelanggan membeli Instans Terpesan tersebut dengan sembilan bulan tersisa. Anda dapat menetapkan harga lain dengan sisa lima bulan, dan harga lain dengan sisa satu bulan.

  Harga minimum yang diizinkan di Pasar Instans Terpesan adalah 0,00 USD.
- Batas – Batasan penjualan Instans Terpesan berikut berlaku untuk masa pakai Akun AWS Anda. Mereka bukan batas tahunan dan mereka tidak dapat ditingkatkan.
  - Anda dapat menjual hingga 50.000 USD dalam Instans Terpesan.
  - Anda dapat menjual hingga 5.000 USD Instans Terpesan.
- Tidak dapat mengubah — Anda tidak dapat mengubah iklan Anda secara langsung. Namun, Anda dapat mengubah daftar Anda dengan membatalkannya terlebih dahulu, lalu membuat daftar lain dengan parameter baru.
- Dapat membatalkan – Anda dapat membatalkan iklan Anda kapan saja, selama ada dalam status `active`. Anda tidak dapat membatalkan ikan jika sudah cocok atau sedang diproses untuk dijual. Jika beberapa instans dalam iklan Anda cocok dan Anda membatalkan iklan, hanya instans yang tidak cocok yang tersisa yang dihapus dari iklan.

Mengiklankan Instans Terpesan Anda

Sebagai penjual terdaftar, Anda dapat memilih untuk menjual satu atau lebih dari Instans Terpesan Anda. Anda dapat memilih untuk menjual semuanya dalam satu iklan atau sebagian. Selain itu, Anda dapat mencantumkan Instans Terpesan dengan konfigurasi tipe instans, platform, dan cakupan apa pun.

Konsol menentukan harga yang disarankan. Konsol memeriksa penawaran yang cocok dengan Instans Terpesan Anda dan cocok dengan intans yang memiliki harga terendah. Jika tidak, konsol

menghitung harga yang disarankan berdasarkan biaya Instans Terpesan untuk sisa waktunya. Jika nilai yang dihitung kurang dari 1,01 USD, harga yang disarankan adalah 1,01 USD.

Jika Anda membatalkan iklan Anda dan sebagian dari iklan itu telah terjual, pembatalan tidak berlaku untuk porsi yang telah terjual. Hanya bagian yang tidak terjual dari listingan yang tidak lagi tersedia di Marketplace Instans Cadangan.

Console

Untuk mencantumkan Instans Cadangan di Marketplace Instans Cadangan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans Terpesan.
3. Pilih Instans Terpesan yang akan diiklankan, lalu pilih Tindakan, Jual Instans Terpesan.
4. Pada halaman Konfigurasikan Daftar Instans Terpesan Anda, tetapkan jumlah instans yang akan dijual dan harga dimuka untuk jangka waktu yang tersisa di kolom yang relevan. Lihat bagaimana nilai reservasi Anda berubah selama sisa jangka waktu dengan memilih panah di sebelah kolom Sisa Bulan.
5. Jika Anda adalah pengguna mahir dan ingin menyesuaikan harga, Anda dapat memasukkan nilai yang berbeda untuk bulan berikutnya. Untuk kembali ke penurunan harga linier default, pilih Atur ulang.
6. Pilih Lanjutkan setelah Anda selesai mengonfigurasi iklan Anda.
7. Konfirmasikan detail iklan Anda pada halaman Konfirmasi Iklan Instans Terpesan Anda, dan jika Anda puas, pilih Iklankan Instans Terpesan.

Untuk melihat iklan Anda di konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans Terpesan.
3. Pilih Instans Terpesan yang Anda iklankan dan pilih tab Iklan Saya di dekat bagian bawah halaman.

AWS CLI

Untuk mengelola Instans Cadangan di Marketplace Instans Cadangan

1. Dapatkan daftar Instans Cadangan Anda dengan menggunakan describe-reserved-instancesperintah. Perhatikan bahwa ID dari Instans Cadangan yang ingin Anda cantumkan.
2. Gunakan perintah create-reserved-instances-listing. Anda harus menentukan ID Instans Terpesan, jumlah instans, dan jadwal harga.
3. Untuk melihat daftar Anda, gunakan describe-reserved-instances-listingsperintah.
4. Untuk membatalkan daftar Anda, gunakan cancel-reserved-instances-listingperintah.

PowerShell

Untuk mengelola Instans Cadangan di Marketplace Instans Cadangan

1. Dapatkan daftar Instans Cadangan Anda dengan menggunakan Get-EC2ReservedInstancecmdlet. Perhatikan bahwa ID dari Instans Cadangan yang ingin Anda cantumkan.
2. Gunakan New-EC2ReservedInstancesListingcmdlet. Anda harus menentukan ID Instans Terpesan, jumlah instans, dan jadwal harga.
3. Untuk melihat iklan Anda, gunakan Get-EC2ReservedInstancesListingcmdlet.
4. Untuk membatalkan iklan Anda, gunakan Stop-EC2ReservedInstancesListingcmdlet.

Status iklan Instans Terpesan

Status Iklan pada tab Iklan saya dari halaman Instans Terpesan menampilkan status iklan Anda:

Informasi yang ditampilkan oleh Status Iklan adalah tentang status iklan Anda di Pasar Instans Terpesan. Hal ini berbeda dari informasi status yang ditampilkan oleh kolom Status di halaman Instans Terpesan. Informasi Status ini adalah tentang reservasi Anda.

- aktif—Iklan ini tersedia untuk dibeli.
- dibatalkan—Iklan dibatalkan dan tidak tersedia untuk dibeli di Pasar Instans Terpesan.
- ditutup — Instans Terpesan tidak diiklankan. Instans Terpesan mungkin saja`closed` karena penjualan iklan telah selesai.

Siklus hidup iklan

Jika semua instans dalam iklan Anda cocok dan terjual, tab Iklan Saya menunjukkan bahwa Jumlah instans total sama dengan jumlah yang tercantum dalam Terjual. Selain itu, tidak ada instans yang tersedia yang tersisa untuk iklan Anda, dan Status-nya adalah `closed`.

Jika hanya sebagian dari iklan Anda yang terjual, AWS menghentikan Instans Cadangan dalam daftar dan membuat jumlah Instans Cadangan yang sama dengan Instans Cadangan yang tersisa dalam hitungan. Jadi, ID iklan dan iklan yang diwakilinya, yang sekarang memiliki lebih sedikit reservasi untuk dijual, masih aktif.

Semua penjualan Instans Terpesan di masa mendatang dalam iklan ini diproses dengan cara ini. Ketika semua Instans Cadangan dalam daftar terjual, AWS tandai daftar sebagai`closed`.

Misalnya, Anda membuat iklan ID iklan Instans Terpesan 5ec28771-05ff-4b9b-aa31-9e57dexample dengan jumlah iklan 5.

Tab Iklan Saya di halaman konsol Instans Terpesan menampilkan iklan dengan cara ini:

ID daftar penawaran Instans Terpesan 5ec28771-05ff-4b9b-aa31-9e57dexample

- Jumlah total reservasi = 5
- Terjual = 0
- Tersedia = 5
- Status = aktif

Seorang pembeli membeli dua reservasi, sehingga tiga reservasi masih tersedia untuk dijual. Karena penjualan sebagian ini, AWS buat reservasi baru dengan hitungan tiga untuk mewakili sisa reservasi yang masih dijual.

Berikut tampilan iklan Anda di tab Iklan Saya:

ID daftar penawaran Instans Terpesan 5ec28771-05ff-4b9b-aa31-9e57dexample

- Jumlah total reservasi = 5
- Terjual = 2
- Tersedia = 3
- Status = aktif

Jika Anda membatalkan iklan Anda dan sebagian dari iklan itu telah terjual, pembatalan tidak berlaku untuk porsi yang telah terjual. Hanya bagian yang tidak terjual dari daftar penawaran yang tidak lagi tersedia di Marketplace Instans Terpesan.

Setelah Instans Terpesan Anda terjual

Saat Instans Cadangan Anda terjual, AWS mengirimkan pemberitahuan email kepada Anda. Setiap hari saat ada aktivitas apa pun, Anda menerima satu notifikasi email yang merekam semua aktivitas hari itu. Aktivitas dapat mencakup saat Anda membuat atau menjual iklan, atau saat AWS mengirim dana ke akun Anda.

Console

Untuk melacak status daftar Instans Cadangan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di halaman navigasi, pilih Instans Terpesan.
3. Pada tab Daftar Saya, temukan nilai Status Daftar. Tab ini juga berisi informasi tentang istilah, harga daftar, dan rincian berapa banyak contoh dalam daftar yang tersedia, tertunda, dijual, dan dibatalkan.

AWS CLI

Untuk melacak status daftar Instans Cadangan

Gunakan describe-reserved-instances-listingsperintah dengan filter yang sesuai untuk mendapatkan informasi tentang daftar Anda.

```
aws ec2 describe-reserved-instances-listings
```

PowerShell

Untuk melacak status daftar Instans Cadangan

Gunakan Get-EC2ReservedInstancesListingcmdlet.

```
Get-EC2ReservedInstancesListing
```

Mendapatkan pembayaran

Segera setelah AWS menerima dana dari pembeli, pesan dikirim ke email akun pemilik terdaftar untuk Instans Cadangan yang dijual.

AWS mengirimkan transfer kawat Automated Clearing House (ACH) ke rekening bank yang Anda tentukan. Biasanya, transfer ini dilakukan antara satu hingga tiga hari setelah Instans Terpesan Anda terjual. Pencairan dilakukan sekali sehari. Anda akan menerima email dengan laporan pencairan setelah dana dikeluarkan. Perlu diingat bahwa Anda tidak dapat menerima pencairan sampai AWS menerima verifikasi dari bank Anda. Verifikasi ini bisa memakan waktu hingga dua minggu.

Instans Terpesan yang Anda jual terus muncul jika Anda menjelaskan Instans Terpesan Anda.

Anda menerima pencairan tunai untuk Instans Cadangan Anda melalui transfer kawat langsung ke rekening bank Anda. AWS membebankan biaya layanan sebesar 12 persen dari total harga dimuka setiap Instans Cadangan yang Anda jual di Marketplace Instans Cadangan.

Informasi yang dibagikan dengan pembeli

Saat Anda menjual di Marketplace Instans Cadangan, AWS bagikan nama resmi perusahaan Anda pada pernyataan pembeli sesuai dengan peraturan AS. Selain itu, jika pembeli menghubungi Dukungan karena pembeli perlu menghubungi Anda untuk mendapatkan faktur atau untuk beberapa alasan terkait pajak lainnya, AWS mungkin harus memberikan alamat email Anda kepada pembeli sehingga pembeli dapat menghubungi Anda secara langsung.

Untuk alasan serupa, kode pos pembeli dan informasi negara diberikan kepada penjual dalam laporan pencairan. Sebagai penjual, Anda mungkin memerlukan informasi ini untuk menyertai pajak transaksi yang diperlukan, yang Anda serahkan ke pemerintah (seperti pajak penjualan dan pajak pertambahan nilai).

AWS tidak dapat menawarkan saran pajak, tetapi jika spesialis pajak Anda menentukan bahwa Anda memerlukan informasi tambahan spesifik, hubungi Dukungan.

Memodifikasi Instans Terpesan

Saat kebutuhan berubah, Anda dapat mengubah Instans Terpesan Standar atau Konvertibel dan terus mendapatkan keuntungan dari manfaat penagihan. Anda dapat memodifikasi atribut, seperti Zona Ketersediaan, ukuran instans (dalam keluarga dan generasi instans yang sama), serta cakupan Instans Terpesan Anda.

> **Note**
>
> Anda juga dapat menukar Instans Terpesan Konvertibel dengan Instans Terpesan Konvertibel lain dengan konfigurasi yang berbeda. Untuk informasi selengkapnya, lihat Menukar Instans Terpesan Konvertibel.

Anda dapat memodifikasi semua atau sebagian Instans Terpesan Anda. Anda dapat memisahkan Instans Terpesan asli menjadi dua atau lebih Instans Terpesan baru. Misalnya, jika Anda memiliki reservasi untuk 10 instans di `us-east-1a` dan memutuskan untuk memindahkan 5 instans ke `us-east-1b`, permintaan modifikasi menghasilkan dua reservasi baru: satu untuk 5 instans di `us-east-1a` dan yang lainnya untuk 5 instans di `us-east-1b`.

Anda juga dapat menggabungkan dua atau lebih Instans Terpesan menjadi satu Instans Terpesan. Misalnya, jika Anda memiliki empat Instans Terpesan `t2.small` dari masing-masing satu instans, Anda dapat menggabungkannya untuk membuat satu Instans Terpesan `t2.large`. Untuk informasi selengkapnya, lihat Dukungan untuk memodifikasi ukuran instans.

Setelah modifikasi, keuntungan dari Instans Terpesan hanya diterapkan pada instans yang cocok dengan parameter baru. Misalnya, jika Anda mengubah Zona Ketersediaan suatu reservasi, reservasi kapasitas dan keuntungan harga secara otomatis diterapkan ke penggunaan instans di Zona Ketersediaan yang baru. Instans yang tidak lagi cocok dengan parameter baru akan dikenai tarif Sesuai Permintaan, kecuali akun Anda memiliki reservasi lain yang berlaku.

Jika permintaan modifikasi Anda berhasil:

- Modifikasi reservasi akan langsung berlaku dan keuntungan harga diterapkan ke instans baru yang dimulai pada jam permintaan modifikasi. Misalnya, jika Anda berhasil memodifikasi reservasi pada pukul 21.15, keuntungan harga ditransfer ke instans baru Anda pada pukul 21.00. Anda bisa mendapatkan tanggal efektif Instans Cadangan yang dimodifikasi dengan menggunakan describe-reserved-instancesperintah.
- Reservasi asli telah pensiun. Tanggal berakhir reservasi adalah tanggal mulai reservasi baru, dan tanggal akhir reservasi baru sama dengan tanggal akhir Instans Terpesan asli. Jika Anda memodifikasi reservasi tiga tahun yang memiliki sisa 16 bulan dalam jangka waktunya, hasil reservasi yang dimodifikasi adalah reservasi 16 bulan dengan tanggal akhir yang sama seperti yang asli.
- Reservasi yang dimodifikasi mencantumkan harga tetap 0 USD dan bukan harga tetap dari reservasi asli.

- Harga tetap dari reservasi yang dimodifikasi tidak memengaruhi penghitungan tingkat harga diskon yang diterapkan ke akun Anda, yang didasarkan pada harga tetap dari reservasi asli.

Jika permintaan modifikasi gagal, Instans Terpesan Anda mempertahankan konfigurasi aslinya, dan langsung tersedia untuk permintaan modifikasi lainnya.

Tidak ada biaya untuk modifikasi, dan Anda tidak menerima tagihan atau faktur baru.

Anda dapat memodifikasi reservasi sesering apa pun, tetapi Anda tidak dapat mengubah atau membatalkan permintaan modifikasi yang menunggu keputusan setelah Anda mengirimkannya. Setelah modifikasi berhasil diselesaikan, Anda dapat mengirimkan permintaan modifikasi lain untuk membatalkan perubahan yang dibuat, jika perlu.

Daftar Isi

- Persyaratan dan pembatasan untuk modifikasi
- Dukungan untuk memodifikasi ukuran instans
- Mengirimkan permintaan modifikasi
- Memecahkan masalah permintaan modifikasi

Persyaratan dan pembatasan untuk modifikasi

Anda dapat memodifikasi atribut ini sebagai berikut.

Atribut yang dapat dimodifikasi	Platform yang didukung	Batasan dan pertimbangan
Ubah Zona Ketersediaan dalam Wilayah yang sama	Linux dan Windows	-
Ubah cakupan dari Zona Ketersediaan ke Wilayah dan sebaliknya	Linux dan Windows	Instans Terpesan zonal tercakup dalam Zona Ketersediaan dan kapasitas terpesan di Zona Ketersediaan tersebut. Jika Anda mengubah cakupan dari Zona Ketersedi aan ke Wilayah (dengan kata lain, dari zonal ke regional),

Atribut yang dapat dimodifikasi	Platform yang didukung	Batasan dan pertimbangan
		Anda kehilangan keuntungan reservasi kapasitas. Instans Terpesan regional tercakup dalam Wilayah. Diskon Instans Terpesan Anda dapat diterapkan ke instans yang berjalan di Zona Ketersediaan mana pun di Wilayah tersebut. Selain itu, diskon Instans Terpesan berlaku untuk penggunaa n instans di semua ukuran dalam keluarga instans yang dipilih. Jika Anda mengubah cakupan dari Wilayah ke Zona Ketersediaan (dengan kata lain, dari regional ke zonal), Anda kehilangan fleksibil itas Zona Ketersediaan dan fleksibilitas ukuran instans (jika berlaku). Untuk informasi selengkap nya, lihat Bagaimana diskon Instans Cadangan diterapkan.

Atribut yang dapat dimodifikasi	Platform yang didukung	Batasan dan pertimbangan
Ubah ukuran instans dalam keluarga dan generasi instans yang sama	Linux/UNIX saja Fleksibilitas ukuran instans tidak tersedia untuk Instans Terpesan di platform lain, yang mencakup Linux dengan SQL Server Standard, Linux dengan SQL Server Web, Linux dengan SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows dengan SQL Standard, Windows dengan SQL Server Enterprise, dan Windows dengan SQL Server Web.	Reservasi harus menggunakan penghunian default. Beberapa keluarga instans tidak didukung karena tidak ada ukuran lain yang tersedia. Untuk informasi selengkapnya, lihat Dukungan untuk memodifikasi ukuran instans

Persyaratan

Amazon EC2 memproses permintaan modifikasi jika ada kapasitas yang memadai untuk konfigurasi baru Anda (jika berlaku), dan jika kondisi berikut terpenuhi:

- Instans Terpesan tidak dapat dimodifikasi sebelum atau pada saat yang sama Anda membelinya
- Instans Terpesan harus aktif
- Tidak ada permintaan modifikasi yang menunggu keputusan
- Instans Terpesan tidak terdaftar di Marketplace Instans Terpesan
- Harus ada kecocokan antara jejak ukuran instans reservasi asli dan konfigurasi baru. Untuk informasi selengkapnya, lihat Dukungan untuk memodifikasi ukuran instans.
- Instans Terpesan asli adalah semua Instans Terpesan Standar atau semua Instans Terpesan Konvertibel, bukan beberapa tipe Instans Terpesan
- Instans Terpesan asli harus kedaluwarsa dalam jam yang sama, jika instans Terpesan tersebut adalah Instans Terpesan Standar

- Untuk memodifikasi ukuran instans, Instans Cadangan harus mendukung fleksibilitas ukuran instans. Untuk daftar Instans Cadangan yang tidak mendukung fleksibilitas ukuran instans, lihatFleksibilitas ukuran instans.

Dukungan untuk memodifikasi ukuran instans

Anda dapat memodifikasi ukuran instans dari Instans Terpesan jika persyaratan berikut terpenuhi.

Persyaratan

- Platformnya adalah Linux/UNIX.
- Anda harus memilih ukuran instans lain dalam keluarga instans yang sama (ditunjukkan dengan huruf, misalnya, T) dan generas yang sama (ditunjukkan oleh angka, misalnya, 2).

  Misalnya, Anda dapat memodifikasi Instans Terpesan dari `t2.small` ke `t2.large` karena keduanya berada dalam keluarga dan generasi T2 yang sama. Namun, Anda tidak dapat memodifikasi Instans Terpesan dari T2 ke M2 atau dari T2 ke T3, karena dalam kedua contoh ini, keluarga dan generasi instans target tidak sama dengan Instans Terpesan asli.
- Anda dapat memodifikasi ukuran instans dari Instans Cadangan hanya jika mendukung fleksibilitas ukuran instans. Untuk daftar Instans Cadangan yang tidak mendukung fleksibilitas ukuran instans, lihatFleksibilitas ukuran instans.
- Anda tidak dapat mengubah ukuran instans Instans Cadangan untuk `t1.micro` instans, karena hanya `t1.micro` memiliki satu ukuran.
- Instans Terpesan yang asli dan baru harus memiliki jejak ukuran instans yang sama.

Daftar Isi

- Jejak ukuran instans
- Faktor normalisasi untuk instans bare metal

Jejak ukuran instans

Setiap Instans Terpesan memiliki jejak ukuran instans, yang ditentukan oleh faktor normalisasi ukuran instans dan jumlah instans dalam reservasi. Saat Anda memodifikasi ukuran instans dalam Instans Terpesan, jejak konfigurasi baru harus cocok dengan konfigurasi asli, jika tidak, permintaan modifikasi tidak akan diproses.

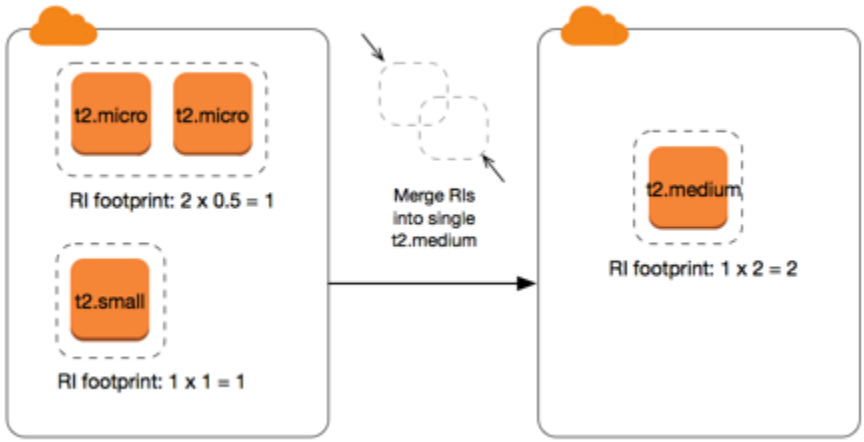
Untuk menghitung jejak ukuran instans dari Instans Terpesan, kalikan jumlah instans dengan faktor normalisasi. Di konsol Amazon EC2, faktor normalisasi diukur dalam satuan. Tabel berikut menjelaskan faktor normalisasi untuk ukuran instans dalam suatu keluarga instans. Misalnya, `t2.medium` memiliki faktor normalisasi 2, jadi reservasi untuk empat instans `t2.medium` memiliki jejak dari 8 unit.

Ukuran instans	Faktor normalisasi
nano	0,25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192

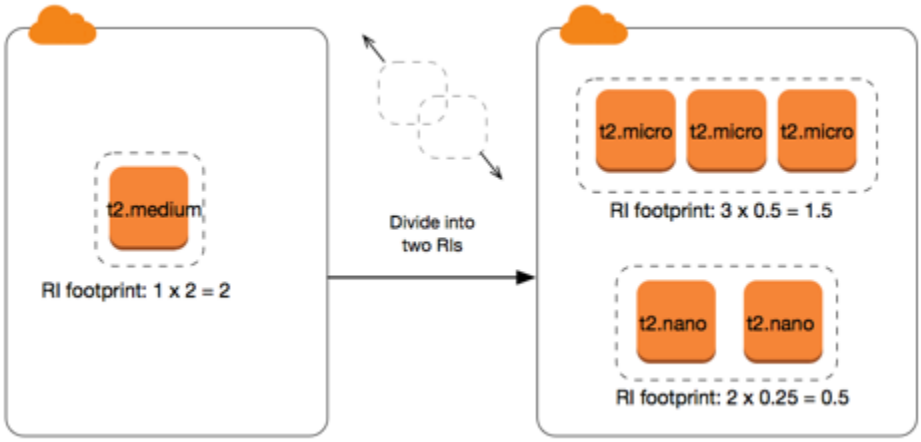
Ukuran instans	Faktor normalisasi
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Anda dapat mengalokasikan reservasi Anda ke dalam ukuran instans yang berbeda di seluruh keluarga instans yang sama selama jejak ukuran instans reservasi Anda tetap sama. Misalnya, Anda dapat membagi reservasi untuk satu instans (1 @ 4 unit) `t2.large` menjadi empat instans (4 @ 1 unit) `t2.small`. Demikian pula, Anda dapat menggabungkan reservasi untuk empat instans `t2.small` menjadi satu instans `t2.large`. Namun, Anda tidak dapat mengubah reservasi untuk dua instans `t2.small` menjadi satu instans `t2.large` karena jejak reservasi baru (4 unit) lebih besar dari jejak reservasi asli (2 unit).

Dalam contoh berikut, Anda memiliki reservasi dengan dua instans `t2.micro` (1 unit) dan reservasi dengan satu instans `t2.small` (1 unit). Jika Anda menggabungkan kedua reservasi ini menjadi satu reservasi dengan satu instans `t2.medium` (2 unit), maka jejak dari reservasi baru sama dengan jejak dari reservasi gabungan.



Anda juga dapat memodifikasi reservasi untuk membaginya menjadi dua reservasi atau lebih. Dalam contoh berikut, Anda memiliki reservasi dengan satu instans `t2.medium` (2 unit). Anda dapat membagi reservasi menjadi dua, satu dengan dua instans `t2.nano` (0,5 unit) dan yang lainnya dengan tiga instans `t2.micro` (1,5 unit).



Faktor normalisasi untuk instans bare metal

Anda dapat memodifikasi reservasi dengan instans `metal` menggunakan ukuran lain dalam keluarga instans yang sama. Demikian pula, Anda dapat memodifikasi reservasi dengan instans selain instans bare metal menggunakan ukuran `metal` dalam keluarga instans yang sama. Umumnya, instans bare metal memiliki ukuran yang sama dengan ukuran instans terbesar yang tersedia dalam keluarga instans yang sama. Misalnya, sebuah instans `i3.metal` berukuran sama dengan instans `i3.16xlarge`, sehingga keduanya memiliki faktor normalisasi yang sama.

Tabel berikut menjelaskan faktor normalisasi untuk ukuran instans bare metal dalam keluarga instans yang memiliki instans bare metal. Faktor normalisasi untuk instans `metal` bergantung pada keluarga instans, tidak seperti ukuran instans lainnya.

Ukuran instans	Faktor normalisasi
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128
`c5n.metal`	144
`c5.metal` | `c5d.metal` | `i3en.metal` | `m5.metal` | `m5d.metal` | `m5dn.metal` | `m5n.metal` | `r5.metal` | `r5b.metal` | `r5d.metal` | `r5dn.metal` | `r5n.metal`	192

Ukuran instans	Faktor normalisasi
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-18tb1.metal | u-24tb1.metal	448
u-6tb1.metal | u-9tb1.metal | u-12tb1.metal	896

Misalnya, instans i3.metal memiliki faktor normalisasi 128. Jika membeli Instans Terpesan Amazon Linux/Unix penghunian default i3.metal, Anda dapat membagi reservasi sebagai berikut:

- Sebuah instans i3.16xlarge berukuran sama dengan instans i3.metal, sehingga faktor normalisasinya adalah 128 (128/1). Reservasi untuk satu instans i3.metal dapat dimodifikasi menjadi satu instans i3.16xlarge.
- Sebuah instans i3.8xlarge berukuran setengah dari instans i3.metal, sehingga faktor normalisasinya adalah 64 (128/2). Reservasi untuk satu instans i3.metal dapat dibagi menjadi dua instans i3.8xlarge.
- Sebuah instans i3.4xlarge berukuran seperempat dari instans i3.metal, sehingga faktor normalisasinya adalah 32 (128/4). Reservasi untuk satu instans i3.metal dapat dibagi menjadi empat instans i3.4xlarge.

Mengirimkan permintaan modifikasi

Sebelum mengubah Instans Cadangan, pastikan Anda telah membaca batasan yang berlaku. Sebelum Anda mengubah ukuran instans, hitung total ukuran instance footprint dari reservasi asli yang ingin Anda modifikasi dan pastikan bahwa itu cocok dengan total ukuran instance footprint konfigurasi baru Anda.

Console

Untuk mengubah Instans Cadangan Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di halaman Instans Terpesan, pilih satu atau beberapa Instans Terpesan yang akan dimodifikasi, dan pilih Tindakan, Modifikasi Instans Terpesan.

Jika Instans Terpesan Anda tidak dalam keadaan aktif atau tidak dapat dimodifikasi, Modifikasi Instans Terpesan akan dinonaktifkan.

3. Entri pertama dalam tabel modifikasi menampilkan atribut dari Instans Terpesan yang dipilih, dan setidaknya satu konfigurasi target di bawahnya. Kolom Unit menampilkan jejak ukuran instans secara total. Pilih Tambahkan untuk setiap konfigurasi baru yang akan ditambahkan. Modifikasi atribut seperlunya untuk setiap konfigurasi.

   - Cakupan: Pilih apakah konfigurasi berlaku untuk sebuah Zona Ketersediaan atau seluruh Wilayah.
   - Zona Ketersediaan: Pilih Zona Ketersediaan yang dibutuhkan. Tidak berlaku untuk Instans Terpesan wilayah.
   - Jenis instans: Pilih jenis instance yang diperlukan. Konfigurasi gabungan harus mempunyai jejak ukuran instans yang sama dengan konfigurasi asli Anda.
   - Jumlah: Tentukan jumlah instans. Untuk membagi Instans Terpesan ke dalam banyak konfigurasi, kurangi jumlah, pilih Tambahkan, dan tentukan jumlah untuk konfigurasi tambahan. Misalnya, jika Anda memiliki konfigurasi tunggal dengan jumlah 10, Anda dapat mengubah jumlahnya menjadi 6 dan menambahkan konfigurasi dengan jumlah 4. Proses ini memensiunkan Instans Terpesan asli setelah Instans Terpesan baru diaktifkan.
4. Pilih Lanjutkan.
5. Untuk mengonfirmasi pilihan modifikasi setelah Anda selesai menentukan konfigurasi target Anda, pilih Kirim modifikasi.
6. Anda dapat menentukan status permintaan modifikasi dengan melihat kolom Status di layar Instans Terpesan. Berikut ini adalah beberapa kemungkinan status.

   - aktif (modifikasi tertunda) — Status transisi untuk Instans Terpesan asli
   - pensiun (modifikasi tertunda) — Status transisi untuk Instans Terpesan asli sementara Instans Terpesan baru sedang dibuat
   - pensiun — Instans Terpesan berhasil dimodifikasi dan diganti
   - aktif — Salah satu dari berikut ini:
     - Instans Terpesan baru dibuat dari permintaan modifikasi yang berhasil
     - Instans Terpesan Asli setelah permintaan modifikasi gagal

AWS CLI

Untuk mengubah Instans Cadangan Anda

Gunakan perintah modify-reserved-instances. Anda dapat memberikan detail konfigurasi dalam file JSON.

```
aws ec2 modify-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342f5bd7c02 \
    --target-configurations file://configuration.json
```

Untuk mendapatkan status permintaan modifikasi Anda

Gunakan perintah describe-reserved-instances-modifications. Statusnya adalah`processing`,`fulfilled`, atau`failed`.

```
aws ec2 describe-reserved-instances-modifications \
    --reserved-instances-modification-ids rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687
 \
    --query ReservedInstancesModifications[].Status
```

PowerShell

Untuk mengubah Instans Cadangan Anda

Gunakan Edit-EC2ReservedInstancecmdlet. Anda dapat memberikan detail konfigurasi dalam objek tipe`Amazon.EC2.Model.ReservedInstancesConfiguration`.

```
Edit-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342f5bd7c02 `
    -TargetConfiguration $configuration
```

Untuk mendapatkan status permintaan modifikasi Anda

Gunakan Get-EC2ReservedInstancesModificationcmdlet. Statusnya adalah`processing`,`fulfilled`, atau`failed`.

```
Get-EC2ReservedInstancesModification `
    -ReservedInstancesModificationId rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687 | `
    Select Status
```

Memecahkan masalah permintaan modifikasi

Jika pengaturan konfigurasi target yang Anda minta unik, Anda menerima pesan bahwa permintaan Anda sedang diproses. Pada titik ini, Amazon EC2 hanya menentukan bahwa parameter permintaan modifikasi Anda valid. Permintaan modifikasi Anda masih bisa gagal selama pemrosesan karena ketidaktersediaan kapasitas.

Dalam beberapa situasi, Anda mungkin mendapatkan pesan yang menunjukkan permintaan modifikasi yang tidak selesai atau gagal alih-alih konfirmasi. Gunakan informasi dalam pesan tersebut sebagai titik awal untuk mengirim ulang permintaan modifikasi lainnya. Pastikan Anda telah membaca pembatasan berlaku sebelum mengirimkan permintaan.

Tidak semua Instans Terpesan yang dipilih dapat diproses untuk modifikasi

Amazon EC2 mengidentifikasi dan mencantumkan daftar Instans Terpesan yang tidak dapat dimodifikasi. Jika Anda menerima pesan seperti ini, buka halaman Instans Terpesan di konsol Amazon EC2 dan periksa informasi untuk Instans Terpesan.

Kesalahan dalam memproses permintaan modifikasi Anda

Anda mengirimkan satu atau lebih Instans Terpesan untuk modifikasi dan tidak ada permintaan Anda yang dapat diproses. Tergantung jumlah reservasi yang dimodifikasi, Anda bisa mendapatkan versi berbeda dari pesan tersebut.

Amazon EC2 menampilkan alasan mengapa permintaan Anda tidak dapat diproses. Misalnya, Anda mungkin telah menetapkan konfigurasi target yang sama—kombinasi dari Zona Ketersediaan dan platform—untuk satu atau beberapa subset Instans Terpesan yang Anda modifikasi. Coba kirimkan permintaan modifikasi lagi, tetapi pastikan bahwa detail instans dari reservasi cocok, dan bahwa konfigurasi target untuk semua subset yang dimodifikasi adalah unik.

Menukar Instans Terpesan Konvertibel

Anda dapat menukar satu atau beberapa Instans Terpesan Konvertibel dengan Instans Terpesan Konvertibel lainnya dengan konfigurasi yang berbeda, termasuk keluarga instans, sistem operasi, dan penghunian. Tidak ada batasan terkait frekuensi penukaran, selama Instans Terpesan Konvertibel baru memiliki nilai yang sama atau lebih tinggi dari Instans Terpesan Konvertibel asli yang Anda tukar.

Saat Anda menukar Instans Terpesan Konvertibel, jumlah instans untuk reservasi Anda saat ini ditukar dengan sejumlah instans yang mencakup nilai yang sama atau lebih tinggi dari konfigurasi

Instans Terpesan Konvertibel baru. Amazon EC2 menghitung jumlah Instans Terpesan yang dapat Anda terima sebagai hasil dari pertukaran.

Anda tidak dapat menukar Instans Terpesan Standar, tetapi Anda dapat memodifikasinya. Untuk informasi selengkapnya, lihat Memodifikasi Instans Terpesan.

Daftar Isi

- Persyaratan untuk menukar Instans Terpesan Konvertibel
- Menghitung pertukaran Instans Terpesan Konvertibel
- Menggabungkan Instans Terpesan Konvertibel
- Menukar sebagian dari Instans Terpesan Konvertibel
- Mengirimkan permintaan pertukaran

Persyaratan untuk menukar Instans Terpesan Konvertibel

Jika kondisi berikut terpenuhi, Amazon EC2 memproses permintaan pertukaran Anda. Instans Terpesan Konvertibel Anda harus:

- Aktif
- Tidak menunggu permintaan pertukaran sebelumnya
- Memiliki setidaknya 24 jam yang tersisa sebelum kedaluwarsa

Aturan-aturan berikut berlaku:

- Instans Cadangan Konvertibel harus ditukar dengan Instans Cadangan Konvertibel lainnya yang saat ini ditawarkan oleh. AWS
- Instans Terpesan Konvertibel dikaitkan dengan Wilayah tertentu, yang ditetapkan selama jangka waktu reservasi. Anda tidak dapat menukar Instans Cadangan Konvertibel dengan Instans Cadangan Konvertibel di Wilayah lain.
- Untuk menukar Instans Cadangan Konvertibel zona, AWS harus memiliki kapasitas yang cukup untuk jenis instans baru di Wilayah.
- Anda dapat menukar satu atau beberapa Instans Terpesan Konvertibel untuk satu Instans Terpesan Konvertibel yang baru saja dalam satu waktu.
- Untuk menukar sebagian Instans Terpesan Konvertibel, Anda dapat memodifikasinya menjadi dua atau lebih reservasi, lalu menukar satu atau lebih reservasi dengan Instans Terpesan Konvertibel yang baru. Untuk informasi selengkapnya, lihat Menukar sebagian dari Instans

Terpesan Konvertibel. Untuk informasi selengkapnya tentang memodifikasi Instans Terpesan, lihat Memodifikasi Instans Terpesan.

- Semua Instans Terpesan Konvertibel di Muka dapat ditukar dengan Instans Terpesan Konvertibel Sebagian di Muka, dan sebaliknya.

> **Note**
>
> Jika total pembayaran di muka yang diperlukan untuk pertukaran (biaya true-up) kurang dari $0,00, AWS secara otomatis memberi Anda sejumlah contoh dalam Instans Cadangan Konvertibel yang memastikan bahwa biaya true-up adalah $0,00 atau lebih.

> **Note**
>
> Jika nilai total (harga dimuka +harga per jam* jumlah jam yang tersisa) dari Instans Cadangan Konvertibel baru kurang dari nilai total Instans Cadangan Konvertibel yang dipertukarkan, AWS secara otomatis memberi Anda sejumlah instans dalam Instans Cadangan Konvertibel yang memastikan bahwa nilai totalnya sama atau lebih tinggi dari Instans Cadangan Konvertibel yang dipertukarkan.

- Untuk mendapatkan keuntungan dari harga yang lebih baik, Anda dapat menukar Instans Terpesan Konvertibel Tanpa Biaya di Muka dengan Instans Terpesan Konvertibel Biaya Semua di muka atau Sebagian di Muka.
- Anda tidak dapat menukar Semua Instans Cadangan Konvertibel di Muka dan Sebagian di Depan dengan Instans Cadangan Tanpa Konvertibel di Muka.
- Anda dapat menukar Instans Terpesan Konvertibel Tanpa Biaya di Muka dengan Instans Terpesan Konvertibel Tanpa Biaya di Muka lainnya hanya jika harga per jam Instans Terpesan Konvertibel yang baru sama atau lebih tinggi dari harga per jam Instans Terpesan Konvertibel yang ditukar.

> **Note**
>
> Jika nilai total (harga per jam * jumlah jam yang tersisa) dari Instans Terpesan Konvertibel yang baru kurang dari nilai total Instans Terpesan Konvertibel yang ditukar, AWS secara otomatis memberi Anda sejumlah instans dalam Instans Terpesan Konvertibel yang memastikan bahwa total instans nilainya sama atau lebih tinggi dari Instans Terpesan Konvertibel yang ditukar.

- Jika Anda menukar banyak Instans Terpesan Konvertibel yang memiliki tanggal kedaluwarsa berbeda, tanggal kedaluwarsa untuk Instans Terpesan Konvertibel yang baru adalah tanggal terjauh di masa mendatang.
- Jika Anda menukar satu Instans Terpesan Konvertibel, instans tersebut harus memiliki jangka waktu yang sama (1 tahun atau 3 tahun) dengan Instans Terpesan Konvertibel yang baru. Jika Anda menggabungkan beberapa Instans Terpesan Konvertibel dengan jangka waktu berbeda, Instans Terpesan Konvertibel yang baru memiliki jangka waktu 3 tahun. Untuk informasi selengkapnya, lihat Menggabungkan Instans Terpesan Konvertibel.
- Saat Amazon EC2 menukar Instans Terpesan Konvertibel, mereka memensiunkan reservasi terkait, dan mentransfer tanggal akhir ke reservasi baru. Setelah pertukaran, Amazon EC2 menetapkan tanggal akhir untuk reservasi lama dan tanggal mulai untuk reservasi baru sama dengan tanggal pertukaran. Misalnya, jika Anda menukar reservasi tiga tahun yang memiliki sisa jangka waktu 16 bulan, reservasi baru adalah reservasi 16 bulan dengan tanggal akhir yang sama dengan reservasi dari Instans Terpesan Konvertibel yang Anda tukarkan.

Menghitung pertukaran Instans Terpesan Konvertibel

Bertukar Instans Terpesan Konvertibel bersifat gratis. Namun, Anda mungkin diharuskan untuk membayar biaya true-up, yang merupakan biaya di muka yang dihitung prorata dari selisih antara Instans Terpesan Konvertibel yang Anda miliki dan Instans Terpesan Konvertibel baru yang Anda terima dari pertukaran tersebut.

Setiap Instans Terpesan Konvertibel memiliki nilai daftar. Nilai daftar ini dibandingkan dengan nilai daftar Instans Terpesan Konvertibel yang Anda inginkan untuk menentukan banyaknya reservasi instans yang dapat Anda terima dari pertukaran tersebut.

Sebagai contoh: Anda memiliki Instans Terpesan Konvertibel dengan nilai daftar 1 x 35 USD yang ingin Anda tukarkan dengan tipe instans baru dengan nilai daftar 10 USD.

```
$35/$10 = 3.5
```

Anda dapat menukar Instans Terpesan Konvertibel dengan tiga Instans Terpesan Konvertibel senilai 10 USD. Membeli setengah reservasi tidak dimungkinkan; oleh karena itu Anda harus membeli Instans Terpesan Konvertibel tambahan untuk menutupi sisanya:

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

Instans Terpesan Konvertibel keempat memiliki tanggal berakhir yang sama dengan tiga lainnya. Jika Anda menukar Instans Terpesan Konvertibel secara Sebagian atau secara Penuh di Muka, Anda membayar biaya true-up untuk reservasi keempat. Jika biaya di muka yang tersisa dari Instans Terpesan Konvertibel adalah 500 USD, dan reservasi baru biasanya akan dikenakan biaya 600 USD secara prorata, maka Anda akan dikenai biaya 100 USD.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Menggabungkan Instans Terpesan Konvertibel

Jika Anda menggabungkan dua atau lebih Instans Terpesan Konvertibel, jangka waktu Instans Terpesan Konvertibel yang baru harus sama dengan Instans Terpesan Konvertibel yang lama, atau yang tertinggi dari Instans Terpesan Konvertibel. Tanggal kedaluwarsa untuk Instans Terpesan Konvertibel yang baru adalah tanggal kedaluwarsa yang terjauh di masa mendatang.

Misalnya, Anda memiliki Instans Terpesan Konvertibel berikut ini di akun Anda:

ID Instans Terpesan	Jangka waktu	Tanggal kedaluwarsa
aaaa1111	1 tahun	31/12/2018
bbbb2222	1 tahun	31/07/2018
cccc3333	3 tahun	30/06/2018
dddd4444	3 tahun	31/12/2019

- Anda dapat menggabungkan `aaaa1111` dan `bbbb2222`, serta menukarnya dengan Instans Terpesan Konvertibel 1 tahun. Anda tidak dapat menukarnya dengan Instans Terpesan Konvertibel 3 tahun. Tanggal kedaluwarsa Instans Terpesan Konvertibel yang baru adalah 31-12-2018.
- Anda dapat menggabungkan `bbbb2222` dan `cccc3333` serta menukarnya dengan Instans Terpesan Konvertibel 3 tahun. Anda tidak dapat menukarnya dengan Instans Terpesan Konvertibel 1 tahun. Tanggal kedaluwarsa Instans Terpesan Konvertibel yang baru adalah 31-07-2018.
- Anda dapat menggabungkan `cccc3333` dan `dddd4444` serta menukarnya dengan Instans Terpesan Konvertibel 3 tahun. Anda tidak dapat menukarnya dengan Instans Terpesan Konvertibel 1 tahun. Tanggal kedaluwarsa Instans Terpesan Konvertibel yang baru adalah 31-12-2019.

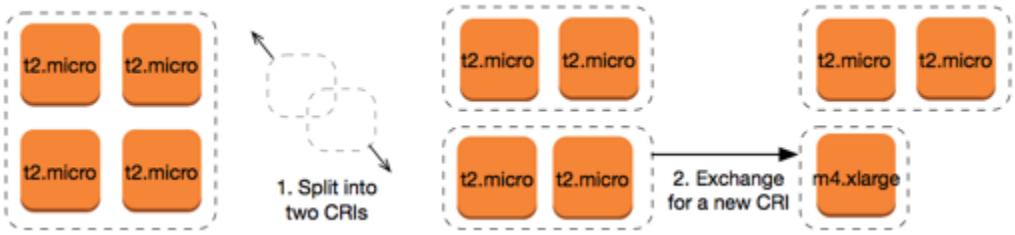
Menukar sebagian dari Instans Terpesan Konvertibel

Anda dapat menggunakan proses modifikasi untuk membagi Instans Terpesan Konvertibel menjadi reservasi yang lebih kecil, kemudian menukar satu atau lebih reservasi baru untuk Instans Terpesan Konvertibel baru. Contoh berikut menunjukkan cara untuk melakukannya.

Example Contoh: Instans Terpesan Konvertibel dengan lebih dari satu instans

Dalam contoh ini, Anda memiliki file Instans Terpesan Konvertibel `t2.micro` dengan empat instans dalam reservasi. Untuk menukar dua instans `t2.micro` dengan instans `m4.xlarge`:

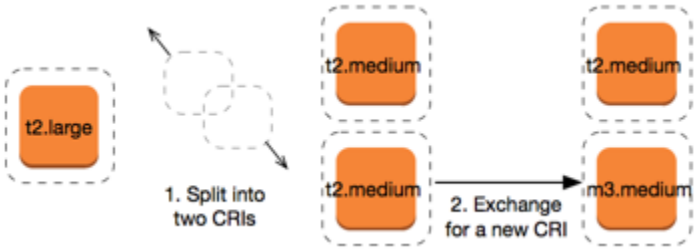
1. Modifikasi Instans Terpesan Konvertibel `t2.micro` dengan membaginya menjadi dua Instans Terpesan Konvertibel `t2.micro`, masing-masing dua instans.
2. Tukar salah satu Instans Terpesan Konvertibel `t2.micro` yang baru dengan Instans Terpesan Konvertibel `m4.xlarge`.



Example Contoh: Instans Terpesan Konvertibel dengan satu instans

Dalam contoh ini, Anda memiliki Instans Terpesan Konvertibel `t2.large`. Untuk mengubahnya menjadi instans `t2.medium` dan instans `m3.medium` yang lebih kecil:

1. Modifikasi Instans Terpesan Konvertibel `t2.large` dengan membaginya menjadi dua Instans Terpesan Konvertibel `t2.medium`. Satu instans `t2.large` memiliki jejak ukuran instans yang sama dengan dua instans `t2.medium`.
2. Tukar salah satu Instans Terpesan Konvertibel `t2.medium` yang baru dengan Instans Terpesan Konvertibel `m3.medium`.



Untuk informasi selengkapnya, lihat Dukungan untuk memodifikasi ukuran instans dan Mengirimkan permintaan pertukaran.

Mengirimkan permintaan pertukaran

Anda dapat menukar Instans Cadangan Konvertibel Anda. Instans Cadangan yang dipertukarkan sudah pensiun.

Console

Untuk menukar Instans Cadangan Konvertibel

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Instans Terpesan, pilih Instans Terpesan Konvertibel yang akan ditukar, dan pilih Tindakan, Tukar Instans Terpesan.
3. Pilih atribut dari konfigurasi yang diinginkan, dan pilih Temukan Penawaran.
4. Pilih Instans Terpesan Konvertibel baru. Di bagian bawah layar, Anda dapat melihat jumlah Instans Terpesan yang Anda terima untuk pertukaran tersebut, dan biaya tambahannya.
5. Jika Anda telah memilih Instans Terpesan Konvertibel yang memenuhi kebutuhan Anda, pilih Tinjau.
6. Pilih Tukar, kemudian Tutup.

AWS CLI

Untuk menukar Instans Cadangan Konvertibel

1. Temukan Instans Cadangan Konvertibel baru yang memenuhi kebutuhan Anda dengan menggunakan describe-reserved-instances-offeringsperintah.
2. Dapatkan penawaran untuk pertukaran dengan menggunakan perintah get-reserved-instances-exchange-quote. Ini termasuk jumlah Instans Cadangan yang Anda dapatkan dari bursa, dan biaya sebenarnya untuk pertukaran:

3. Lakukan pertukaran dengan menggunakan perintah accept-reserved-instances-exchange-quote.

PowerShell

Untuk menukar Instans Cadangan Konvertibel

1. Temukan Instans Cadangan Konvertibel baru yang memenuhi kebutuhan Anda dengan menggunakan Get-EC2ReservedInstancesOfferingcmdlet.
2. Dapatkan penawaran untuk pertukaran dengan menggunakan Get EC2 - ReservedInstancesExchangeQuote cmdlet. Ini termasuk jumlah Instans Cadangan yang Anda dapatkan dari bursa, dan biaya sebenarnya untuk pertukaran:
3. Lakukan pertukaran dengan menggunakan Approve-EC2ReservedInstancesExchangeQuotecmdlet

Kuota Instans Terpesan

Anda dapat membeli Instans Terpesan baru setiap bulan. Jumlah Instans Terpesan baru yang dapat Anda beli setiap bulan ditentukan oleh kuota bulanan Anda, sebagai berikut:

Deskripsi kuota	Kuota default
Instans Terpesan regional baru	20 per Wilayah per bulan
Instans Terpesan zonal baru	20 per Zona Ketersediaan per bulan

Misalnya, di Wilayah dengan tiga Zona Ketersediaan, kuota default-nya adalah 80 Instans Terpesan per bulan, dihitung sebagai berikut:

- 20 Instans Terpesan regional untuk Wilayah
- Ditambah 60 Instans Terpesan zonal (20 untuk masing-masing dari tiga Zona Ketersediaan)

Contoh di `running` negara bagian dihitung terhadap kuota Anda. Contoh yang ada di`pending`,, `stopping``stopped`, dan `hibernated` negara bagian tidak dihitung dalam kuota Anda.

Melihat jumlah Instans Terpesan yang telah Anda beli

Jumlah Instans Terpesan yang Anda beli ditunjukkan oleh bidang Jumlah instans (konsol) atau parameter `InstanceCount` (AWS CLI). Saat Anda membeli Instans Terpesan baru, kuota diukur terhadap jumlah instans total. Misalnya, jika Anda membeli satu konfigurasi Instans Terpesan dengan satu instans berjumlah 10, pembelian diperhitungkan dengan kuota Anda sebagai 10, bukan 1.

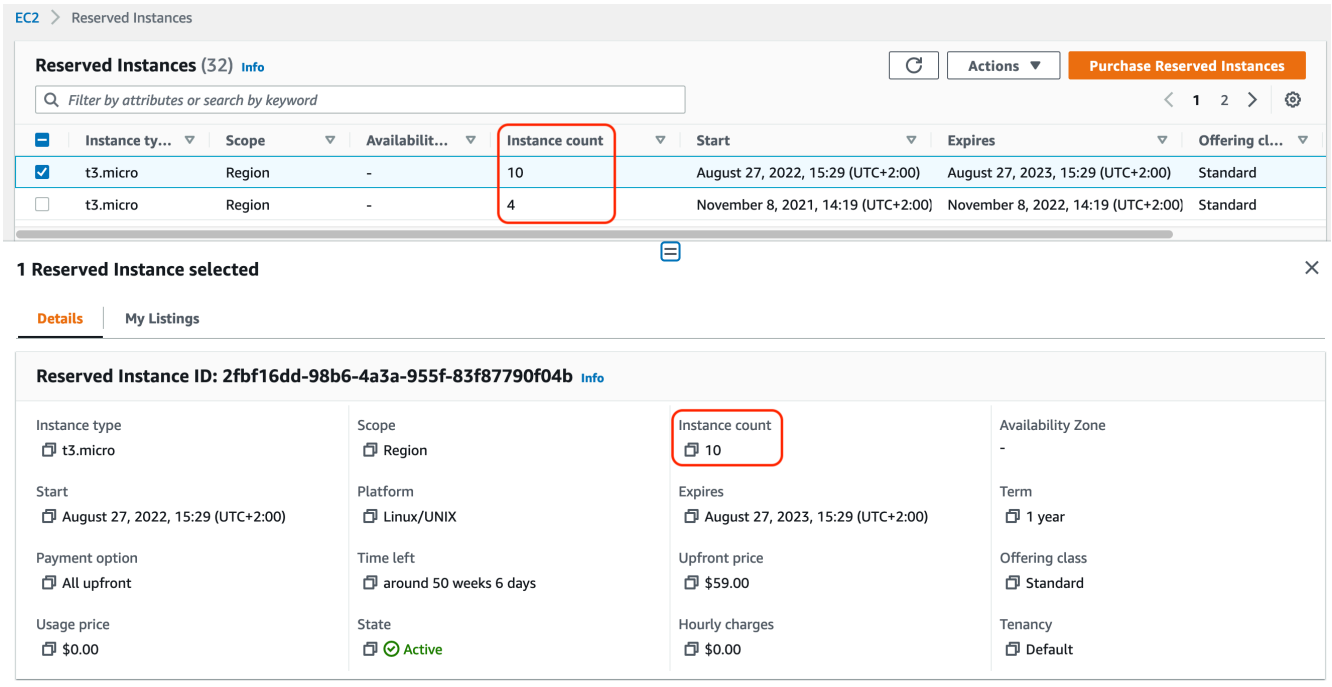
Anda dapat melihat jumlah Instans Terpesan yang telah dibeli menggunakan Amazon EC2 atau AWS CLI.

Console

Untuk melihat jumlah Instans Terpesan yang telah Anda beli

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans Terpesan.
3. Pilih konfigurasi Instans Terpesan dari tabel, dan periksa bidang Jumlah instans.

   Pada tangkapan layar berikut, baris yang dipilih mewakili konfigurasi satu Instans Terpesan untuk tipe instans `t3.micro`. Kolom Jumlah instans dalam tampilan tabel dan bidang Jumlah instans dalam tampilan detail (diuraikan dalam tangkapan layar) menunjukkan bahwa ada 10 Instans Terpesan untuk konfigurasi ini.



AWS CLI

Untuk melihat jumlah Instans Terpesan yang telah Anda beli

Gunakan describe-reserved-instancesperintah dan tentukan ID konfigurasi Instans Cadangan.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --output table
```

Berikut ini adalah output contoh. `InstanceCount`Bidang menunjukkan bahwa ada 10 Instans Cadangan untuk konfigurasi ini.

```
-------------------------------------------------------------------
|                    DescribeReservedInstances                    |
+-----------------------------------------------------------------+
||                       ReservedInstances                       ||
|+----------------------+----------------------------------------+|
||  CurrencyCode        |  USD                                   ||
||  Duration            |  31536000                              ||
||  End                 |  2023-08-27T13:29:44+00:00             ||
||  FixedPrice          |  59.0                                  ||
||  InstanceCount       |  10                                    ||
||  InstanceTenancy     |  default                               ||
||  InstanceType        |  t3.micro                              ||
||  OfferingClass       |  standard                              ||
||  OfferingType        |  All Upfront                           ||
||  ProductDescription  |  Linux/UNIX                            ||
||  ReservedInstancesId |  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111  ||
||  Scope               |  Region                                ||
||  Start               |  2022-08-27T13:29:45.938000+00:00      ||
||  State               |  active                                ||
||  UsagePrice          |  0.0                                   ||
|+----------------------+----------------------------------------+|
|||                      RecurringCharges                       |||
||+---------------------------------+--------------------------+||
|||  Amount                         |  0.0                     |||
|||  Frequency                      |  Hourly                  |||
||+---------------------------------+--------------------------+||
```

PowerShell

Untuk melihat jumlah Instans Terpesan yang telah Anda beli

Gunakan Get-EC2ReservedInstanceCmdlet dan tentukan ID konfigurasi Instans Cadangan.

```
Get-EC2ReservedInstance -ReservedInstancesId a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Berikut ini adalah output contoh. `InstanceCount`Bidang menunjukkan bahwa ada 10 Instans Cadangan untuk konfigurasi ini.

```
AvailabilityZone    :
CurrencyCode        : USD
Duration            : 31536000
End                 : 1/12/2017 8:57:08 PM
FixedPrice          : 0
InstanceCount       : 10
InstanceTenancy     : default
InstanceType        : t3.medium
OfferingClass       : standard
OfferingType        : All Upfront
ProductDescription  : Windows
RecurringCharges    : {}
ReservedInstancesId : a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
Scope               : Region
Start               : 10/12/2016 4:00:00 PM
State               : active
Tags                : {}
UsagePrice          : 0
```

Pertimbangan-pertimbangan

Instans Terpesan regional menerapkan diskon ke Instans Sesuai Permintaan yang sedang berjalan. Batas Instans Sesuai Permintaan default adalah 20. Anda tidak dapat melebihi batas Instans Sesuai Permintaan yang sedang berjalan dengan membeli Instans Terpesan regional. Misalnya, jika Anda sudah memiliki 20 Instans Sesuai Permintaan yang sedang dan membeli 20 Instans Terpesan regional, 20 Instans Terpesan regional digunakan untuk menerapkan diskon ke 20 Instans Sesuai Permintaan yang sedang berjalan. Jika membeli lebih banyak Instans Terpesan regional, Anda tidak akan dapat meluncurkan lebih banyak instans karena Anda telah mencapai batas Instans Sesuai Permintaan.

Sebelum membeli Instans Terpesan regional, pastikan batas Instans Sesuai Permintaan Anda sesuai atau melebihi jumlah Instans Terpesan regional yang ingin dimiliki. Jika perlu, pastikan Anda meminta

peningkatan batas Instans Sesuai Permintaan sebelum membeli lebih banyak Instans Terpesan regional.

Instans Terpesan zonal—Instans Terpesanyang dibeli untuk Zona Ketersediaan tertentu—memberikan reservasi kapasitas serta diskon. Anda dapat melebihi batas Instans Sesuai Permintaan yang sedang berjalan dengan membeli Instans Terpesan zonal. Misalnya, jika Anda sudah memiliki 20 Instans Sesuai Permintaan yang sedang berjalan dan membeli 20 Instans Terpesan zonal, Anda dapat meluncurkan 20 Instans Sesuai Permintaan lain yang sesuai dengan spesifikasi Instans Terpesan Anda, sehingg Anda memiliki total 40 instans yang sedang berjalan.

Melihat kuota Instans Terpesan Anda dan meminta peningkatan kuota

Konsol Amazon EC2 menyediakan informasi kuota. Anda juga dapat meminta peningkatan kuota. Lihat informasi yang lebih lengkap di Melihat kuota Anda saat ini dan Meminta peningkatan.

Instans Spot

Instans Spot adalah instans yang menggunakan kapasitas EC2 tidak terpakai yang tersedia dengan harga yang lebih rendah dari harga Sesuai Permintaan. Karena Instans Spot memungkinkan Anda meminta instans EC2 yang tidak digunakan dengan diskon besar, Anda dapat menurunkan biaya Amazon EC2 secara signifikan. Harga per jam untuk Instans Spot disebut harga Spot. Harga Spot dari setiap tipe instans di setiap Zona Ketersediaan ditetapkan oleh Amazon EC2, dan disesuaikan secara bertahap berdasarkan pasokan dan permintaan jangka panjang untuk Instans Spot. Instans Spot Anda berjalan setiap kali kapasitas tersedia.

Instans Spot adalah pilihan hemat biaya jika Anda dapat bersikap fleksibel tentang kapan aplikasi Anda berjalan dan apakah aplikasi Anda dapat diinterupsi. Misalnya, Instans Spot sangat cocok untuk analisis data, pekerjaan batch, pemrosesan latar belakang, dan tugas opsional. Untuk informasi selengkapnya, lihat Instans Spot Amazon EC2.

Untuk perbandingan opsi pembelian yang berbeda untuk instans EC2, lihat Opsi penagihan dan pembelian Amazon EC2.

Konsep

Sebelum memulai Instans Spot, Anda harus terbiasa dengan konsep berikut:

- Kolam kapasitas spot – Satu set instans EC2 yang tidak digunakan dengan tipe instans yang sama (misalnya, `m5.large`) dan Zona Ketersediaan yang sama pula.

- Harga spot – Harga Instans Spot saat ini per jam.
- Permintaan Instans Spot – Meminta Instans Spot. Saat kapasitas tersedia, Amazon EC2 memenuhi permintaan Anda. Permintaan Instans Spot bisa satu kali atau tetap. Amazon EC2 secara otomatis mengirimkan kembali permintaan Instans Spot yang persisten setelah Instans Spot yang terkait dengan permintaan tersebut diinterupsi.
- Rekomendasi penyeimbangan kembali instans EC2 – Amazon EC2 memancarkan sinyal rekomendasi penyeimbangan kembali instans untuk memberi tahu Anda bahwa Instans Spot berisiko tinggi mengalami interupsi. Sinyal ini memberikan kesempatan untuk secara proaktif menyeimbangkan kembali beban kerja Anda di Instans Spot yang ada atau yang baru tanpa harus menunggu pemberitahuan interupsi Instans Spot selama dua menit.
- Interupsi Instans Spot – Amazon EC2 mengakhiri, menghentikan, atau menghibernasi Instans Spot Anda saat Amazon EC2 membutuhkan kapasitas kembali. Amazon EC2 memberikan pemberitahuan interupsi Instans Spot, yang memberikan peringatan dua menit pada instans sebelum diinterupsi.

Perbedaan antara Instans Spot dan Instans Sesuai Permintaan

Tabel berikut mencantumkan daftar perbedaan utama antara Instans Spot dan Instans Sesuai Permintaan.

	Instans Spot	Instans Sesuai Permintaan
Waktu peluncuran	Hanya dapat diluncurkan segera jika permintaan Instans Spot dan kapasitas tersedia.	Hanya dapat diluncurkan segera jika Anda membuat permintaan peluncuran manual dan kapasitas tersedia.
Kapasitas yang tersedia	Jika kapasitas tidak tersedia, permintaan Instans Spot akan terus membuat permintaan peluncuran secara otomatis hingga kapasitas tersedia.	Jika kapasitas tidak tersedia saat Anda membuat permintaan peluncuran, Anda mendapatkan pesan kesalahan kapasitas tidak mencukupi (ICE).
Harga per jam	Harga per jam untuk Instans Spot bervariasi berdasarkan pasokan dan permintaan jangka panjang.	Harga per jam untuk Instans Sesuai Permintaan bersifat statis.

	Instans Spot	Instans Sesuai Permintaan
Rekomendasi penyeimbangan kembali	Sinyal yang dipancarkan oleh Amazon EC2 untuk Instans Spot yang sedang berjalan saat instans berada pada risiko interupsi yang tinggi.	Anda menentukan kapan Instans Sesuai Permintaan diinterupsi (dihentikan, hibernasi, atau diakhiri).
Interupsi instans	Anda dapat menghentikan dan memulai Instans Spot yang didukung Amazon EBS. Selain itu, Amazon EC2 dapat menginterupsi Instans Spot individu jika kapasitas tidak lagi tersedia.	Anda menentukan kapan Instans Sesuai Permintaan diinterupsi (dihentikan, hibernasi, atau diakhiri).

Penetapan harga dan penghematan

Anda membayar harga Spot untuk Instans Spot, yang ditetapkan oleh Amazon EC2 dan disesuaikan secara bertahap berdasarkan pasokan dan permintaan jangka panjang untuk Instans Spot. Instans Spot berjalan hingga Anda mengakhirinya, kapasitas tidak lagi tersedia, atau grup Amazon EC2 Auto Scaling Anda mengakhirinya selama diskalakan ke dalam.

Jika Anda atau Amazon EC2 menginterupsi Instans Spot yang sedang berjalan, Anda akan dikenai biaya untuk detik yang digunakan atau satu jam penuh, atau Anda tidak dikenai biaya, tergantung sistem operasi yang digunakan dan siapa yang menginterupsi Instans Spot. Untuk informasi selengkapnya, lihat Penagihan untuk Instans Spot yang diinterupsi.

Instans Spot tidak dicakup oleh Savings Plans. Jika Anda memiliki Savings Plans, itu tidak memberikan penghematan tambahan selain tabungan yang sudah Anda dapatkan dari menggunakan Instans Spot. Selain itu, pengeluaran Anda untuk Instans Spot tidak menerapkan komitmen dalam Compute Savings Plans Anda.

Tampilkan harga

Untuk melihat harga Spot terendah saat ini (diperbarui setiap lima menit) per AWS Region jenis instans, lihat halaman Harga Instans Spot Amazon EC2.

Untuk melihat riwayat harga Spot selama tiga bulan terakhir, gunakan konsol Amazon EC2 atau perintah. describe-spot-price-history Untuk informasi selengkapnya, lihat Lihat riwayat harga Spot Instance.

Kami secara independen memetakan Availability Zone ke kode untuk masing-masing kode Akun AWS. Oleh karena itu, Anda bisa mendapatkan hasil yang berbeda untuk kode Zona Ketersediaan yang sama (misalnya, `us-west-2a`) di antara akun yang berbeda.

Tampilkan penghematan

Anda dapat menampilkan penghematan yang dihasilkan dari penggunaan Instans Spot untuk satu Armada Spot atau untuk semua Instans Spot. Anda dapat menampilkan penghematan yang dilakukan dalam satu jam terakhir atau tiga hari terakhir, dan Anda dapat menampilkan biaya rata-rata per jam vCPU dan per jam memori (GiB). Penghematan diperkirakan dan mungkin berbeda dari penghematan sebenarnya karena tidak menyertakan penyesuaian penagihan untuk penggunaan Anda. Untuk informasi selengkapnya tentang menampilkan informasi penghematan, lihat Penghematan dari pembelian Instans Spot.

Tampilkan penagihan

Tagihan Anda memberikan detail tentang penggunaan layanan Anda. Untuk informasi selengkapnya, lihat Melihat tagihan Anda dalam Panduan Pengguna AWS Billing .

Praktik terbaik untuk Amazon EC2 Spot

Amazon EC2 menyediakan akses ke kapasitas komputasi EC2 cadangan di Instans Spot AWS Cloud melalui dengan penghematan hingga 90% dibandingkan dengan harga Sesuai Permintaan. Satu-satunya perbedaan antara Instans Sesuai Permintaan dan Instans Spot adalah Instans Spot dapat diinterupsi oleh Amazon EC2, dengan pemberitahuan dua menit, jika Amazon EC2 perlu merebut kembali kapasitasnya. Untuk memastikan pengalaman terbaik dengan Instans Spot, penting untuk memahami dan menerapkan praktik terbaik untuk penggunaannya.

Instans Spot direkomendasikan untuk aplikasi tanpa stateless, toleransi kesalahan, dan fleksibel. Misalnya, Instans Spot berfungsi dengan baik untuk big data, beban kerja terkontainer, CI/CD, server web stateless, komputasi performa tinggi (HPC), dan beban kerja rendering.

Saat berjalan, Instans Spot sama persis dengan Instans Sesuai Permintaan. Namun, Spot tidak menjamin bahwa Anda dapat mempertahankan instans agar berjalan cukup lama untuk menyelesaikan beban kerja Anda. Spot juga tidak menjamin bahwa Anda bisa langsung

mendapatkan ketersediaan instans yang Anda cari, atau bahwa Anda selalu bisa mendapatkan kapasitas agregat yang Anda minta. Selain itu, interupsi dan kapasitas Instans Spot dapat berubah dari waktu ke waktu karena ketersediaan Instans Spot bervariasi berdasarkan pasokan dan permintaan. Selain itu, performa masa lalu bukanlah jaminan untuk hasil di masa mendatang.

Instans Spot tidak cocok untuk beban kerja yang tidak fleksibel, stateful, tidak toleran terhadap kesalahan, atau digabungkan erat di antara simpul instans. Kami tidak merekomendasikan Instans Spot untuk beban kerja yang tidak toleran terhadap periode sesekali ketika seluruh kapasitas target tidak sepenuhnya tersedia. Meskipun mengikuti praktik terbaik Spot agar fleksibel tentang jenis instans dan Availability Zone memberikan peluang terbaik untuk ketersediaan tinggi, tidak ada jaminan bahwa kapasitas akan tersedia, karena lonjakan permintaan untuk Instans Sesuai Permintaan dapat mengganggu beban kerja pada Instans Spot.

Kami sangat tidak menyarankan menggunakan Instans Spot untuk beban kerja ini atau mencoba gagal ke Instans Sesuai Permintaan untuk menangani interupsi atau periode tidak tersedianya. Kegagalan pada Instans Sesuai Permintaan dapat secara tidak sengaja mendorong interupsi untuk Instans Spot Anda yang lain. Selain itu, jika Instans Spot untuk kombinasi tipe instans dan Availability Zone terputus, mungkin akan sulit bagi Anda untuk mendapatkan Instans Sesuai Permintaan dengan kombinasi yang sama.

Terlepas dari apakah Anda pengguna Spot berpengalaman atau baru menggunakan Instans Spot, jika saat ini Anda mengalami masalah terkait interupsi atau ketersediaan Instans Spot, kami sarankan Anda mengikuti praktik terbaik ini untuk mendapatkan pengalaman terbaik menggunakan layanan Spot.

Praktik terbaik Spot

- Menyiapkan instans individu untuk interupsi
- Bersikaplah fleksibel terkait tipe instans dan Zona Ketersediaan
- Gunakan pemilihan tipe instans berbasis atribut
- Gunakan skor penempatan Spot untuk mengidentifikasi Wilayah dan Zona Ketersediaan yang optimal
- Menggunakan grup EC2 Auto Scaling atau EC2 Fleet untuk mengelola kapasitas agregat Anda
- Menggunakan strategi alokasi harga dan kapasitas yang dioptimalkan
- Gunakan AWS layanan terintegrasi untuk mengelola Instans Spot Anda
- Metode permintaan Spot mana yang terbaik untuk digunakan?

Menyiapkan instans individu untuk interupsi

Cara terbaik agar Anda dapat menangani interupsi Instans Spot dengan baik adalah dengan merancang aplikasi Anda agar toleran terhadap kesalahan. Untuk melakukannya, Anda dapat memanfaatkan rekomendasi penyeimbangan kembali instans EC2 dan notifikasi interupsi Instans Spot.

Rekomendasi penyeimbangan kembali Instans EC2 adalah sinyal yang memberi tahu Anda saat Instans Spot berada pada risiko interupsi yang tinggi. Sinyal tersebut memberi Anda kesempatan untuk secara proaktif mengelola Instans Spot sebelum pemberitahuan interupsi Instans Spot dua menit. Anda dapat memutuskan untuk menyeimbangkan kembali beban kerja Anda ke Instans Spot baru atau lama yang tidak berisiko tinggi mengalami interupsi. Kami telah mempermudah Anda untuk menggunakan sinyal ini dengan fitur Penyeimbangan Kembali Kapasitas di grup Auto Scaling dan EC2 Fleet.

Pemberitahuan interupsi Instans Spot adalah peringatan yang dikeluarkan dua menit sebelum Amazon EC2 menginterupsi Instans Spot. Jika beban kerja Anda “fleksibel waktu”, Anda dapat mengonfigurasi Instans Spot untuk dihentikan atau dihibernasi, alih-alih diakhiri, saat terinterupsi. Amazon EC2 secara otomatis menghentikan atau menghibernasi Instans Spot Anda saat terjadi interupsi, dan secara otomatis melanjutkan instans saat kami memiliki kapasitas yang tersedia.

Kami menyarankan Anda membuat aturan di Amazon EventBridge yang menangkap rekomendasi penyeimbangan ulang dan pemberitahuan gangguan, lalu memicu titik pemeriksaan untuk kemajuan beban kerja Anda atau menangani gangguan dengan baik. Untuk informasi selengkapnya, lihat Pantau sinyal rekomendasi penyeimbangan kembali. Untuk contoh terperinci yang akan memandu Anda tentang cara membuat dan menggunakan aturan peristiwa, lihat Memanfaatkan Notifikasi Interupsi Instans Spot Amazon EC2.

Untuk informasi lebih lanjut, lihat Rekomendasi penyeimbangan ulang instans EC2 dan.Interupsi Instans Spot

Bersikaplah fleksibel terkait tipe instans dan Zona Ketersediaan

Kolam kapasitas Spot adalah sekumpulan instans EC2 yang tidak digunakan dengan tipe instans yang sama (misalnya, `m5.large`) dan Zona Ketersediaan yang sama pula (misalnya, us-east-1a). Anda harus fleksibel terkait tipe instans yang Anda minta dan di Zona Ketersediaan mana Anda dapat menerapkan beban kerja. Hal ini memberi Spot peluang yang lebih baik untuk menemukan dan mengalokasikan jumlah kapasitas komputasi yang Anda butuhkan. Misalnya, jangan hanya meminta `c5.large` jika Anda ingin menggunakan keluarga c4, m5, dan m4 yang lebih besar.

Tergantung kebutuhan tertentu, Anda dapat mengevaluasi tipe instans yang bisa digunakan secara fleksibel untuk memenuhi persyaratan komputasi Anda. Jika beban kerja dapat diskalakan secara vertikal, Anda harus menyertakan jenis instans yang lebih besar (lebih banyak v CPUs dan memori) dalam permintaan Anda. Jika hanya dapat menskalakan secara horizontal, Anda harus menyertakan tipe instans generasi sebelumnya karena permintaan dari pelanggan Sesuai Permintaan lebih sedikit.

Aturan praktis yang baik adalah bersikap fleksibel pada setidaknya 10 tipe instans untuk setiap beban kerja. Selain itu, pastikan semua Zona Ketersediaan dikonfigurasi untuk digunakan di VPC Anda dan dipilih untuk beban kerja Anda.

Gunakan pemilihan tipe instans berbasis atribut

Dengan pemilihan tipe instans berbasis atribut, Anda dapat menentukan atribut instans—seperti vCPU, memori, dan penyimpanan—untuk beban kerja yang ingin Anda jalankan. EC2 Auto Scaling atau Armada EC2 kemudian akan secara otomatis mengidentifikasi dan meluncurkan instance yang cocok dengan atribut yang Anda tentukan. Ini menghilangkan upaya yang diperlukan untuk memilih jenis instans tertentu secara manual, yang memerlukan pemahaman mendalam tentang penawaran setiap jenis instance.

Selain itu, pemilihan tipe instans berbasis atribut memungkinkan Anda untuk secara otomatis menggunakan tipe instans yang baru dirilis saat tersedia. Ini memastikan akses yang mulus ke jangkauan kapasitas Instans Spot yang semakin luas.

Pemilihan tipe instans berbasis atribut sangat ideal untuk beban kerja dan kerangka kerja yang dapat fleksibel tentang jenis instans yang mereka jalankan, seperti High Performance Computing (HPC) dan beban kerja big data.

Untuk informasi selengkapnya, lihat Membuat grup instans campuran menggunakan pemilihan jenis instans berbasis atribut di Panduan Pengguna Amazon EC2 Auto Scaling dan dalam panduan ini. Tentukan atribut untuk pemilihan tipe contoh untuk Armada EC2 atau Armada Spot

Gunakan skor penempatan Spot untuk mengidentifikasi Wilayah dan Zona Ketersediaan yang optimal

Instans Spot adalah kapasitas EC2 yang tidak digunakan, dan kapasitas ini berfluktuasi berdasarkan penawaran dan permintaan EC2. Akibatnya, Anda mungkin tidak selalu mendapatkan kapasitas Spot yang tepat yang Anda butuhkan di lokasi tertentu pada waktu tertentu. Untuk mengurangi ketidakpastian ini, Anda dapat menggunakan fitur Skor penempatan Spot. Fitur ini memberikan rekomendasi untuk Wilayah atau Availability Zone yang lebih mungkin memiliki kapasitas yang cukup untuk memenuhi kebutuhan kapasitas Spot Anda tanpa mengharuskan Anda meluncurkan Instans Spot di lokasi tersebut terlebih dahulu.

Skor penempatan spot paling baik digunakan untuk beban kerja yang fleksibel tentang jenis instans dan Wilayah atau Zona Ketersediaan yang dapat mereka gunakan. Yang perlu Anda lakukan hanyalah menentukan kapasitas Spot yang Anda butuhkan, persyaratan jenis instans Anda, dan apakah Anda menginginkan rekomendasi untuk Wilayah atau Zona Ketersediaan. Sebagai imbalannya, Anda menerima skor mulai dari 1 hingga 10 untuk setiap Wilayah atau Availability Zone, yang menunjukkan kemungkinan berhasil menyediakan kapasitas Spot yang Anda minta di lokasi tersebut. Skor 10 menunjukkan bahwa permintaan Spot Anda sangat mungkin berhasil.

Penting untuk dicatat bahwa skor penempatan Spot adalah point-in-time rekomendasi, karena kapasitas dapat bervariasi dari waktu ke waktu. Ini tidak menjamin kapasitas yang tersedia atau memprediksi risiko gangguan.

Anda dapat menggunakan fitur Skor penempatan Spot di konsol Amazon EC2 AWS CLI, atau SDK. Untuk informasi selengkapnya, lihat Skor penempatan Spot.

Menggunakan grup EC2 Auto Scaling atau EC2 Fleet untuk mengelola kapasitas agregat Anda

Spot memungkinkan Anda untuk berpikir dalam hal kapasitas agregat—dalam unit yang mencakup vCPU, memori, penyimpanan, atau throughput jaringan—bukan berpikir dalam hal kapasitas instans. Grup Auto Scaling dan EC2 Fleet memungkinkan Anda untuk meluncurkan dan mempertahankan kapasitas target, serta secara otomatis meminta sumber daya untuk menggantikan sumber daya yang terganggu atau diakhiri secara manual. Saat mengonfigurasi grup Auto Scaling atau EC2 Fleet, Anda hanya perlu menentukan tipe instans dan kapasitas target berdasarkan kebutuhan aplikasi Anda. Untuk informasi selengkapnya, lihat Grup Auto Scaling dalam Panduan Pengguna Amazon EC2 Auto Scaling dan Membuat Armada EC2 dalam panduan pengguna ini.

Menggunakan strategi alokasi harga dan kapasitas yang dioptimalkan

Strategi alokasi dalam grup Auto Scaling membantu Anda menyediakan kapasitas target tanpa perlu mencari kolam kapasitas Spot secara manual dengan kapasitas tak terpakai. Kami merekomendasikan penggunaan strategi `price-capacity-optimized` karena strategi ini secara otomatis menyediakan instans dari kolam kapasitas Spot yang juga memiliki potensi harga paling rendah. Anda juga dapat memanfaatkan strategi alokasi `price-capacity-optimized` di Armada EC2. Karena kapasitas Instans Spot Anda bersumber dari kolam dengan kapasitas optimal, hal ini mengurangi kemungkinan bahwa Instans Spot Anda diklaim kembali. Untuk informasi selengkapnya, lihat Strategi alokasi untuk beberapa jenis instans di Panduan Pengguna Amazon EC2 Auto Scaling Ketika beban kerja memiliki biaya interupsi yang tinggi dan dalam panduan pengguna ini.

Gunakan AWS layanan terintegrasi untuk mengelola Instans Spot Anda

AWS Layanan lain terintegrasi dengan Spot untuk mengurangi biaya komputasi secara keseluruhan tanpa perlu mengelola instans atau armada individu. Kami menyarankan Anda mempertimbangkan solusi berikut untuk beban kerja yang berlaku: Amazon EMR, Amazon Elastic Container Service AWS Batch, Amazon Elastic Kubernetes Service, Amazon AI SageMaker , dan Amazon AWS Elastic Beanstalk Servers. GameLift Untuk mempelajari selengkapnya tentang praktik terbaik Spot dengan layanan ini, lihat Situs Web Lokakarya Instans Spot Amazon EC2.

Metode permintaan Spot mana yang terbaik untuk digunakan?

Gunakan tabel berikut untuk menentukan API yang akan digunakan saat meminta Instans Spot.

API	Kapan harus menggunakan?	Kasus penggunaan	Haruskah saya menggunakan API ini?
CreateAutoScalingGroup	• Anda memerlukan beberapa instans dengan konfigurasi tunggal atau konfigurasi campuran. • Anda ingin mengotomatiskan manajemen siklus hidup melalui API yang dapat dikonfigurasi.	Buat grup Auto Scaling yang mengelola siklus hidup instans Anda sambil mempertahankan jumlah instans yang diinginkan. Mendukung penskalaan horizontal (menambahkan lebih banyak instans) antara batas minimum dan maksimum yang ditentukan.	Ya
CreateFleet	• Anda memerlukan beberapa instans dengan konfigurasi tunggal	Buat armada Instans Sesuai Permintaan dan Instans Spot dalam satu permintaan dengan banyak spesifikasi peluncura	Ya – dalam mode `instant` jika Anda tidak memerlukan penskalaan otomatis

API	Kapan harus menggunakan?	Kasus penggunaan	Haruskah saya menggunakan API ini?
	atau konfigurasi campuran. • Anda ingin mengelola sendiri siklus hidup instans Anda. • Jika Anda tidak memerlukan penskalaan otomatis, kami sarankan Anda menggunakan armada tipe `instant`.	n yang bervariasi menurut tipe instans, AMI, Zona Ketersediaan, atau subnet. Strategi alokasi Instans Spot default ke `lowest-price` per unit, tetapi Anda dapat mengubahnya menjadi `price-capacity-optimized` , `capacity-optimized` , atau `diversified` .	

API	Kapan harus menggunakan?	Kasus penggunaan	Haruskah saya menggunakan API ini?
RunInstances	• Anda sudah menggunakan RunInstances API untuk meluncurkan Instans Sesuai Permintaan, dan Anda hanya ingin mengubah untuk meluncurkan Instans Spot dengan mengubah satu parameter. • Anda tidak memerlukan banyak instans dengan tipe instans yang berbeda.	Luncurkan sejumlah tertentu instans menggunakan AMI dan satu tipe instans.	Tidak - karena RunInstances tidak mengizinkan jenis instance campuran dalam satu permintaan

API	Kapan harus menggunakan?	Kasus penggunaan	Haruskah saya menggunakan API ini?
RequestSpotFleet	• Kami sangat tidak menyarankan menggunakan RequestSpotFleet API karena ini adalah API lama tanpa investasi yang direncanakan. • Jika Anda ingin mengelola siklus hidup instance, gunakan API. CreateFleet • Jika Anda tidak ingin mengelola siklus hidup instance, gunakan API. CreateAutoScalingGroup	JANGAN GUNAKAN. RequestSpotFleet adalah API lama tanpa investasi yang direncanakan.	Tidak
RequestSpotInstances	• Kami sangat tidak menyarankan menggunakan RequestSpotInstances API karena ini adalah API lama tanpa investasi yang direncanakan.	JANGAN GUNAKAN. RequestSpotInstances adalah API lama tanpa investasi yang direncanakan.	Tidak

Cara kerja Instans Spot

Untuk meluncurkan Instans Spot, Anda dapat membuat permintaan Instans Spot, atau Amazon EC2 membuat permintaan Instans Spot atas nama Anda. Instans Spot diluncurkan ketika permintaan Instans Spot dipenuhi.

Anda dapat meluncurkan Instans Spot menggunakan beberapa layanan berbeda. Untuk informasi selengkapnya, lihat Memulai Instans Spot Amazon EC2. Dalam panduan pengguna ini, kami menjelaskan cara-cara berikut untuk meluncurkan Instans Spot menggunakan EC2:

- Anda dapat membuat permintaan Instans Spot dengan menggunakan wizard instans peluncuran di konsol Amazon EC2 atau perintah run-instances. Untuk informasi selengkapnya, lihat Mengelola Instans Spot Anda.
- Anda dapat membuat EC2 Fleet, tempat Anda menentukan jumlah Instans Spot yang diinginkan. Amazon EC2 membuat permintaan Instans Spot atas nama Anda untuk setiap Instans Spot yang ditentukan di EC2 Fleet. Untuk informasi selengkapnya, lihat Membuat Armada EC2.
- Anda dapat membuat permintaan Armada Spot, tempat Anda menentukan jumlah Instans Spot yang diinginkan. Amazon EC2 membuat permintaan Instans Spot atas nama Anda untuk setiap Instans Spot yang ditentukan pada permintaan Armada Spot. Untuk informasi selengkapnya, lihat Membuat Armada Spot.

Instans Spot Anda diluncurkan jika ada kapasitas yang tersedia. Instans Spot berjalan hingga Anda menghentikan atau mengakhirinya, atau hingga Amazon EC2 menginterupsi (dikenal sebagai Interupsi Instans Spot). Amazon EC2 dapat menghentikan, menghentikan, atau hibernasi Instans Spot saat menginterupsi Instans Spot.

Saat menggunakan Instans Spot, Anda harus siap menghadapi interupsi. Amazon EC2 dapat menginterupsi Instans Spot Anda saat permintaan Instans Spot naik atau saat pasokan Instans Spot berkurang. Saat menginterupsi Instans Spot, Amazon EC2 memberikan pemberitahuan interupsi Instans Spot, yang memberi instans peringatan dua menit sebelum Amazon EC2 menginterupsi. Anda tidak dapat mengaktifkan perlindungan pengakhiran untuk Instans Spot. Untuk informasi selengkapnya, lihat Interupsi Instans Spot.

Daftar Isi

- Status permintaan Instans Spot
- Meluncurkan Instans Spot dalam grup peluncuran
- Meluncurkan Instans Spot dalam grup Zona Ketersediaan

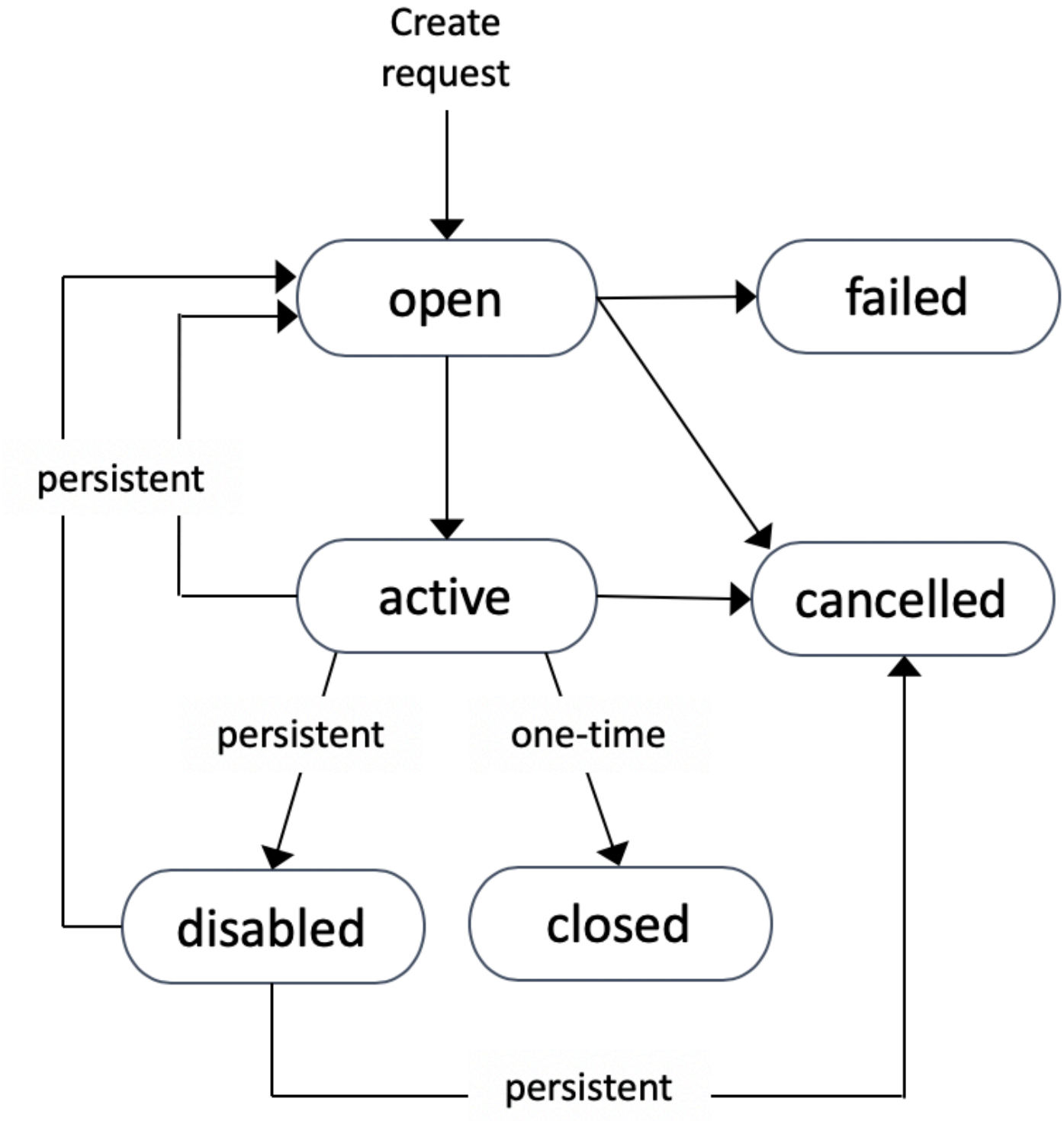
- Meluncurkan Instans Spot di VPC
- Luncurkan instance kinerja yang dapat meledak
- Peluncuran pada perangkat keras penyewa tunggal

Status permintaan Instans Spot

Permintaan Instans Spot dapat berada dalam salah satu status berikut:

- `open` – Permintaan menunggu untuk dipenuhi.
- `active` – Permintaan Instans Spot terpenuhi dan memiliki Instans Spot terkait.
- `failed` – Permintaan memiliki satu atau beberapa parameter buruk.
- `closed` – Instans Spot diinterupsi atau diakhiri.
- `disabled` – Anda menghentikan Instans Spot.
- `cancelled` – Anda membatalkan permintaan, atau permintaan kedaluwarsa.

Ilustrasi berikut mewakili transisi antarstatus permintaan status. Perhatikan bahwa transisi bergantung pada tipe permintaan (satu kali atau tetap).



Permintaan Instans Spot satu kali tetap aktif hingga Amazon EC2 meluncurkan Instans Spot, permintaan kedaluwarsa, atau Anda membatalkan permintaan. Jika kapasitas tidak tersedia, Instans Spot Anda diakhiri dan permintaan Instans Spot ditutup.

Permintaan Instans Spot persisten tetap aktif hingga kedaluwarsa atau Anda membatalkannya, bahkan jika permintaan dipenuhi. Jika kapasitas tidak tersedia, Instans Spot Anda diinterupsi. Setelah instans Anda diinterupsi, saat kembali kapasitas tersedia, Instans Spot akan dimulai jika dihentikan atau dilanjutkan jika hibernasi. Anda dapat menghentikan Instans Spot dan memulainya lagi jika kapasitas tersedia. Jika Instans Spot diakhiri (terlepas dari apakah Instans Spot dalam status berhenti atau berjalan), permintaan Instans Spot dibuka kembali dan Amazon EC2 meluncurkan Instans Spot baru. Untuk informasi selengkapnya, lihat Menghentikan Instans Spot, Memulai Instans Spot, dan Menghentikan Instans Spot.

Anda dapat melacak status permintaan Instans Spot, serta status Instans Spot yang diluncurkan, melalui status. Untuk informasi selengkapnya, lihat Mendapatkan status permintaan Instans Spot.

Meluncurkan Instans Spot dalam grup peluncuran

Tentukan grup peluncuran dalam permintaan Instans Spot Anda untuk memberi tahu Amazon EC2 agar meluncurkan sekumpulan Instans Spot hanya jika dapat meluncurkan semuanya. Selain itu, jika layanan Spot harus mengakhiri salah satu instans dalam grup peluncuran, layanan tersebut harus mengakhiri semuanya. Namun, jika Anda mengakhiri satu atau beberapa instans dalam grup peluncuran, Amazon EC2 tidak mengakhiri instans yang tersisa di grup peluncuran.

Meskipun opsi ini dapat berguna, menambahkan batasan ini dapat mengurangi kemungkinan permintaan Instans Spot Anda dipenuhi dan meningkatkan kemungkinan Instans Spot Anda diakhiri. Misalnya, grup peluncuran Anda menyertakan instans di beberapa Zona Ketersediaan. Jika kapasitas di salah satu Zona Ketersediaan ini menurun dan tidak lagi tersedia, Amazon EC2 akan mengakhiri semua instans untuk grup peluncuran.

Jika Anda membuat permintaan Instans Spot sukses lain yang menetapkan grup peluncuran yang sama (yang ada) sebagai permintaan sukses sebelumnya, maka instans baru akan ditambahkan ke grup peluncuran. Selanjutnya, jika sebuah instans dalam grup peluncuran ini diakhiri, semua instans dalam grup peluncuran akan diakhiri, yang mencakup instans yang diluncurkan oleh permintaan pertama dan kedua.

Meluncurkan Instans Spot dalam grup Zona Ketersediaan

Tentukan grup Zona Ketersediaan dalam permintaan Instans Spot Anda untuk memberi tahu Amazon EC2 agar meluncurkan sekumpulan Instans Spot di Zona Ketersediaan yang sama. Amazon EC2 tidak perlu menginterupsi semua instans dalam grup Zona Ketersediaan pada saat yang bersamaan. Jika Amazon EC2 harus menginterupsi salah satu instans dalam grup Zona Ketersediaan, instans yang lainnya tetap berjalan.

Meskipun opsi ini dapat berguna, menambahkan batasan ini dapat menurunkan kemungkinan permintaan Instans Spot Anda dipenuhi.

Jika Anda menentukan grup Zona Ketersediaan, tetapi tidak menentukan Zona Ketersediaan dalam permintaan Instans Spot, hasilnya bergantung pada jaringan yang Anda tentukan.

VPC default

Amazon EC2 menggunakan Zona Ketersediaan untuk subnet yang ditentukan. Subnet yang tidak Anda tentukan akan memilih Zona Ketersediaan dan subnet default-nya, tetapi belum tentu zona harga terendah. Jika Anda menghapus subnet default untuk Zona Ketersediaan, Anda harus menentukan subnet yang berbeda.

VPC Non-default

Amazon EC2 menggunakan Zona Ketersediaan untuk subnet yang ditentukan.

Meluncurkan Instans Spot di VPC

Anda menentukan subnet untuk Instans Spot Anda dengan cara yang sama seperti menentukan subnet untuk Instans Sesuai Permintaan Anda.

- [VPC Default] Jika ingin Instans Spot diluncurkan di Zona Ketersediaan dengan harga rendah tertentu, Anda harus menentukan subnet yang sesuai dalam permintaan Instans Spot Anda. Jika Anda tidak menentukan subnet, Amazon EC2 akan memilihnya untuk Anda, dan Zona Ketersediaan untuk subnet ini mungkin tidak memiliki harga Spot terendah.
- [VPC Non-default] Anda harus menentukan subnet untuk Instans Spot Anda.

Luncurkan instance kinerja yang dapat meledak

Tipe instans T adalah instans performa yang dapat melonjak. Jika Anda meluncurkan Instans Spot menggunakan tipe instans performa yang dapat melonjak, dan jika Anda berencana untuk segera menggunakan Instans Spot performa dapat melonjak dan untuk durasi yang singkat, tanpa waktu idle untuk mengakumulasi kredit CPU, kami menyarankan Anda untuk meluncurkannya dalam mode Standar agar tidak membayar biaya yang lebih tinggi. Jika Anda meluncurkan Instans Spot performa yang dapat melonjak dalam Mode tak terbatas dan langsung melonjakkan CPU, Anda akan menghabiskan kredit surplus untuk lonjakan. Jika Anda menggunakan instans untuk durasi yang singkat, instans tersebut tidak memiliki waktu untuk mengkumulasi kredit CPU untuk membayar kredit surplus, dan Anda akan dikenai biaya untuk kredit surplus saat Anda mengakhiri instans.

Mode tidak terbatas cocok untuk Instans Spot dengan performa yang dapat melonjak hanya jika instans tersebut berjalan cukup lama untuk mengakumlasi kredit CPU untuk lonjakan. Jika tidak, pembayaran kredit surplus membuat Instans Spot performa yang dapat melonjak lebih mahal daripada menggunakan instans lain. Untuk informasi selengkapnya, lihat Kapan menggunakan mode tak terbatas versus CPU tetap.

Instans T2, ketika dikonfigurasi dalam mode Standar, dapatkan kredit peluncuran. Instans T2 adalah satu-satunya instans performa yang dapat melonjak yang mendapatkan kredit peluncuran. Kredit peluncuran dimaksudkan untuk memberikan pengalaman peluncuran awal yang produktif untuk instans T2 dengan menyediakan sumber daya komputasi yang memadai untuk mengonfigurasi instans. Peluncuran berulang dari instans T2 untuk mengakses kredit peluncuran baru tidak diizinkan. Jika Anda memerlukan CPU berkelanjutan, Anda dapat memperoleh kredit (dengan berhenti selama beberapa periode), menggunakan mode Tak Terbatas untuk Instans Spot T2, atau menggunakan tipe instans dengan CPU khusus.

Peluncuran pada perangkat keras penyewa tunggal

Anda dapat menjalankan Instans Spot pada perangkat keras penghuni tunggal. Instans Spot Khusus secara fisik terisolasi dari instans milik akun lain AWS . Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon dan Instans Khusus Amazon EC2.

Untuk menjalankan Instans Spot Khusus, lakukan salah satu hal berikut:

- Tentukan penghunian `dedicated` saat Anda membuat permintaan Instans Spot. Untuk informasi selengkapnya, lihat Mengelola Instans Spot Anda.
- Minta Instans Spot di VPC dengan penghunian instans `dedicated`. Untuk informasi selengkapnya, lihat Luncurkan Instans Khusus ke dalam VPC dengan tenancy default. Anda tidak dapat meminta Instance Spot dengan penyewaan `default` jika Anda memintanya di VPC dengan penyewaan instance sebesar. `dedicated`

Semua keluarga instans mendukung Instans Spot Khusus, kecuali instans T. Untuk setiap keluarga instans yang didukung, hanya ukuran instans atau ukuran metal terbesar yang mendukung Instans Spot Khusus.

Lihat riwayat harga Spot Instance

Harga Instans Spot ditetapkan oleh Amazon EC2 dan menyesuaikan secara bertahap berdasarkan tren jangka panjang dalam pasokan dan permintaan untuk kapasitas Instans Spot.

Saat permintaan Anda dipenuhi, Instans Spot Anda diluncurkan dengan harga Spot saat ini, tidak melebihi harga Sesuai Permintaan. Anda dapat melihat riwayat harga Spot selama 90 hari terakhir, memfilter menurut tipe instans, sistem operasi, dan Zona Ketersediaan.

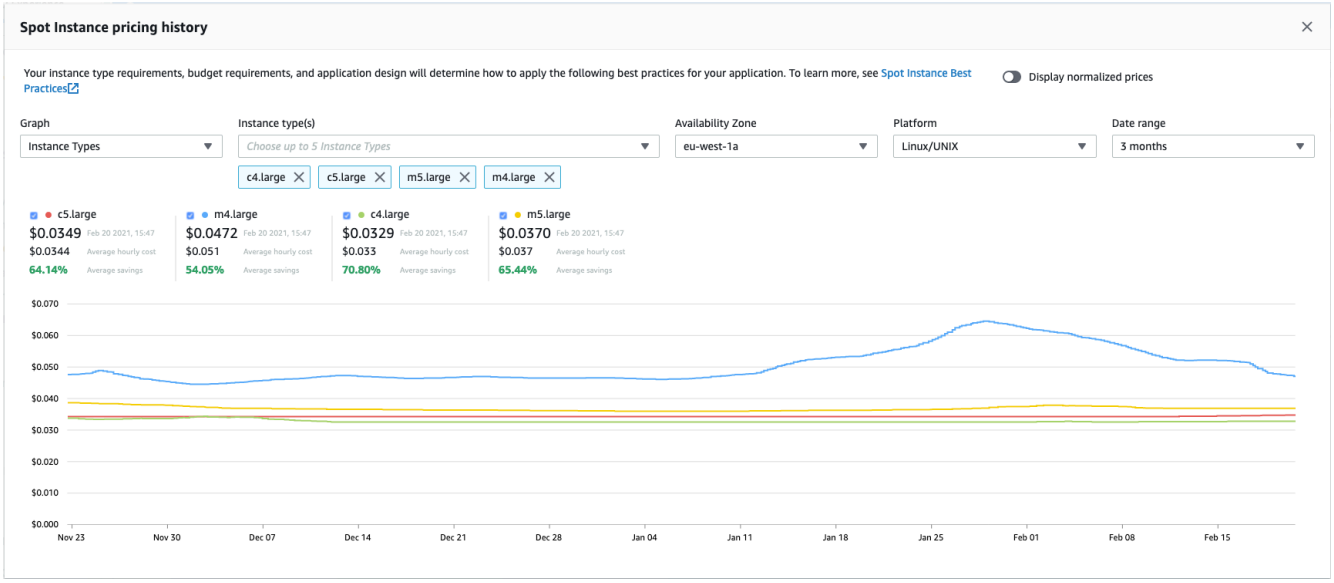
Untuk harga Instans Spot saat ini, lihat Harga Instans Spot Amazon EC2.

Console

Untuk melihat riwayat harga Spot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih Riwayat harga.
4. Untuk Grafik, pilih untuk membandingkan riwayat harga berdasarkan Zona Ketersediaan atau berdasarkan Tipe Instans.
   - Jika Anda memilih Zona Ketersediaan, maka pilih Tipe Instans, sistem operasi (Platform), dan Rentang tanggal untuk melihat riwayat harga.
   - Jika Anda memilih Tipe Instans, maka pilih sampai lima Tipe Instans, Zona Ketersediaan, sistem operasi (Platform), dan Rentang tanggal untuk melihat riwayat harga.

   Tangkapan layar berikut menunjukkan perbandingan harga untuk tipe instans yang berbeda.



5. Arahkan kursor ke grafik untuk menampilkan harga pada waktu tertentu dalam rentang tanggal yang dipilih. Harga ditampilkan di blok informasi di atas grafik. Harga yang

ditampilkan di baris atas menunjukkan harga pada tanggal tertentu. Harga yang ditampilkan di baris kedua menunjukkan harga rata-rata selama rentang tanggal yang dipilih.

6. Untuk menampilkan harga per vCPU, aktifkan Tampilkan harga yang dinormalisasi. Untuk menampilkan harga untuk tipe instans, nonaktifkan Tampilkan harga yang dinormalisasi.

AWS CLI

Untuk melihat riwayat harga Spot

Gunakan perintah berikut describe-spot-price-history.

```
aws ec2 describe-spot-price-history \
    --instance-types c6i.xlarge \
    --product-descriptions "Linux/UNIX" \
    --start-time 2025-04-01T00:00:00 \
    --end-time 2025-04-02T00:00:0
```

PowerShell

Untuk melihat riwayat harga Spot

Gunakan Get-EC2SpotPriceHistorycmdlet.

```
Get-EC2SpotPriceHistory `
    -InstanceType c6i.xlarge `
    -ProductDescription "Linux/UNIX" `
    -UtcStartTime 2025-04-01T00:00:00 `
    -UtcEndTime 2025-04-02T00:00:0
```

Penghematan dari pembelian Instans Spot

Anda dapat melihat informasi penggunaan dan penghematan untuk Instans Spot di tingkat per armada, atau untuk semua Instans Spot yang sedang berjalan. Pada tingkat per armada, informasi penggunaan dan penghematan mencakup semua instans yang diluncurkan dan diakhiri oleh armada. Anda dapat melihat informasi ini dari satu jam terakhir atau tiga hari terakhir.

Tangkapan layar dari bagian Penghematan berikut menunjukkan penggunaan Spot dan informasi penghematan untuk Armada Spot.

Anda dapat melihat informasi penggunaan dan penghematan berikut:

- Instans Spot – Jumlah Instans Spot yang diluncurkan dan diakhiri oleh Armada Spot. Saat melihat ringkasan penghematan, angka tersebut mewakili semua Instans Spot Anda yang sedang berjalan.
- vCPU-jam – Jumlah jam vCPU yang digunakan di semua Instans Spot untuk kerangka waktu yang dipilih.
- Mem(GiB)-jam – Jumlah jam GiB yang digunakan di semua Instans Spot untuk kerangka waktu yang dipilih.
- Total Sesuai Permintaan – Jumlah total yang harus Anda bayarkan untuk kerangka waktu yang dipilih jika Anda meluncurkan instans ini sebagai Instans Sesuai Permintaan.
- Total Spot – Jumlah total yang harus dibayar untuk kerangka waktu yang dipilih.
- Penghematan – Persentase yang Anda hemat dengan tidak membayar harga Sesuai Permintaan.
- Biaya rata-rata per jam VCPU — Biaya rata-rata per jam menggunakan v CPUs di semua Instans Spot untuk kerangka waktu yang dipilih, dihitung sebagai berikut: Biaya rata-rata per jam VCPU = Total Spot/jam VCPU.
- Biaya rata-rata per mem (GiB) -jam - Biaya rata-rata per jam menggunakan GiBs seluruh Instans Spot untuk kerangka waktu yang dipilih, dihitung sebagai berikut: Biaya rata-rata per mem (GiB) -jam = Total spot/Mem (GiB) -jam.

- Tabel detail – Tipe instans yang berbeda (jumlah instans per tipe instans ada dalam kurung) yang mencakup Armada Spot. Saat melihat ringkasan penghematan, ini mencakup semua Instans Spot Anda yang sedang berjalan.

Informasi penghematan hanya dapat dilihat menggunakan konsol Amazon EC2.

Untuk melihat informasi tabungan untuk Armada Spot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih ID permintaan Armada Spot dan gulir ke bagian Penghematan.

   Atau, pilih kotak centang di sebelah ID permintaan Armada Spot dan pilih tab Tabungan.
4. Secara default, halaman menampilkan informasi penggunaan dan penghematan selama tiga hari terakhir. Anda dapat memilih satu jam terakhir atau tiga hari terakhir. Untuk Armada Spot yang diluncurkan kurang dari satu jam yang lalu, halaman tersebut menunjukkan perkiraan penghematan untuk satu jam.

Untuk melihat informasi tabungan untuk semua Instans Spot yang sedang berjalan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih Riwayat Penghematan.

Membuat permintaan Instans Spot

Untuk menggunakan Instans Spot, Anda membuat permintaan Instans Spot yang menyertakan jumlah instans yang diinginkan, tipe instans, dan Zona Ketersediaan. Saat kapasitas tersedia, Amazon EC2 segera memenuhi permintaan Anda. Jika tidak, Amazon EC2 akan menunggu hingga permintaan Anda dipenuhi atau hingga Anda membatalkan permintaan.

Anda dapat menggunakan wizard instans peluncuran di konsol Amazon EC2 atau perintah run-instances untuk meminta Instans Spot dengan cara yang sama seperti Anda dapat meluncurkan Instans Sesuai Permintaan. Metode ini hanya direkomendasikan karena alasan berikut:

- Anda telah menggunakan wizard peluncuran instans atau perintah run-instances untuk meluncurkan Instans Sesuai Permintaan, dan hanya ingin mengubah untuk meluncurkan Instans Spot dengan mengubah satu parameter.
- Anda tidak memerlukan banyak instans dengan tipe instans yang berbeda.

Metode ini umumnya tidak disarankan untuk meluncurkan Instans Spot karena Anda tidak dapat menentukan banyak tipe instans, serta tidak dapat meluncurkan Instans Spot dan Instans Sesuai Permintaan dalam permintaan yang sama. Untuk metode yang lebih disukai untuk meluncurkan Instans Spot, yang mencakup peluncuran armada yang menyertakan Instans Spot dan Instans Sesuai Permintaan dengan banyak tipe instans, lihat Metode permintaan Spot mana yang terbaik untuk digunakan?

Jika Anda meminta banyak Instans Spot sekaligus, Amazon EC2 membuat permintaan Instans Spot terpisah sehingga Anda dapat melacak status setiap permintaan secara terpisah. Untuk informasi selengkapnya tentang melacak permintaan Instans Spot, lihat Mendapatkan status permintaan Instans Spot.

Console

Untuk membuat permintaan Instans Spot

Langkah 1–9 adalah langkah yang sama yang akan Anda gunakan untuk meluncurkan Instans Sesuai Permintaan. Pada Langkah 10, Anda mengonfigurasi permintaan Instans Spot.

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di bilah navigasi di bagian atas layar, pilih wilayah.
3. Dari dasbor konsol Amazon EC2, pilih Luncurkan instans.
4. (Opsional) Pada bagian Nama dan tanda, Anda dapat memberi nama pada instans, serta menandai permintaan instans Spot, instans, volume, dan grafik elastis. Untuk informasi tentang tanda, lihat Tandai sumber daya Amazon EC2 Anda.

    a. Untuk Nama, masukkan nama deskriptif untuk instans Anda.

        Nama instans adalah tanda, di mana kuncinya adalah Name, dan nilainya adalah nama yang Anda tentukan. Jika Anda tidak menentukan nama, instans dapat diidentifikasi berdasarkan ID-nya, yang secara otomatis dihasilkan saat Anda meluncurkan instans tersebut.

b. Untuk menandai permintaan Instans Spot, instans, volume, dan grafik elastis, pilih Tambahkan tanda tambahan. Pilih Tambahkan tanda, lalu masukkan kunci dan nilai, lalu pilih jenis sumber daya yang akan diberi tanda. Pilih Tambah tanda lagi untuk setiap tanda tambahan yang akan ditambahkan.

5. Di bawah Citra Aplikasi dan OS (Amazon Machine Image), pilih sistem operasi (OS) untuk instans Anda, lalu pilih AMI. Untuk informasi selengkapnya, lihat Aplikasi dan Gambar OS (Gambar Mesin Amazon).
6. Di bawah tipe instans, pilih tipe instans yang memenuhi persyaratan Anda untuk konfigurasi perangkat keras dan ukuran instans Anda. Untuk informasi selengkapnya, lihat Tipe instans.
7. Di bawah Nama pasangan kunci (login), pilih pasangan kunci yang ada, atau pilih Buat pasangan kunci baru untuk membuat yang baru. Untuk informasi selengkapnya, lihat Pasangan kunci Amazon EC2 dan instans Amazon EC2.

> **Important**
>
> Jika Anda memilih opsi Lanjutkan tanpa pasangan kunci (Tidak direkomendasikan), Anda tidak akan dapat terhubung ke instans tersebut, kecuali Anda memilih sebuah AMI yang dikonfigurasi agar pengguna dapat masuk dengan cara lain.

8. Di bawah Pengaturan jaringan, gunakan pengaturan default, atau pilih Edit untuk mengonfigurasi pengaturan jaringan jika diperlukan.

   Grup keamanan membentuk bagian dari pengaturan jaringan dan menentukan aturan firewall untuk instans Anda. Aturan ini menentukan lalu lintas jaringan yang masuk yang dikirim ke instans Anda.

   Untuk informasi selengkapnya, lihat Pengaturan jaringan.
9. AMI yang Anda pilih mencakup satu atau lebih volume penyimpanan, termasuk volume perangkat root. Pada bagian Konfigurasikan penyimpanan, Anda dapat menentukan volume tambahan untuk dilampirkan ke instans dengan memilih Tambahkan volume baru. Untuk informasi selengkapnya, lihat Mengonfigurasi penyimpanan.
10. Pada bagian Detail lanjutan, konfigurasikan permintaan Instans Spot sebagai berikut:

    a. Di bawah opsi Pembelian, pilih kotak centang Minta Instans Spot.

    b. Anda dapat menyimpan konfigurasi default untuk permintaan Instans Spot, atau memilih Sesuaikan (di sebelah kanan) agar dapat menentukan pengaturan khusus untuk permintaan Instans Spot Anda.

Saat Anda memilih Sesuaikan, bidang berikut akan muncul.

i. Harga maksimum: Anda dapat meminta Instans Spot dengan harga Spot, dibatasi dengan harga Sesuai Permintaan, atau Anda dapat menentukan jumlah maksimum yang bersedia Anda bayarkan.

> **Warning**
>
> Jika Anda menentukan harga maksimum, instans Anda akan lebih sering diinterupsi daripada jika Anda memilih Tidak ada harga maksimum.
> Jika Anda menentukan harga maksimum, itu harus lebih dari USD $0,001. Menentukan nilai di bawah USD $0,001 akan menghasilkan peluncuran yang gagal.

- Tidak ada harga maksimum: Instans Spot Anda akan diluncurkan pada harga Spot saat ini. Harga tidak akan pernah melebihi harga Sesuai Permintaan. (Direkomendasikan)
- Tetapkan harga maksimum Anda (per instans/jam): Anda dapat menentukan jumlah maksimum yang bersedia Anda bayarkan.
  - Jika Anda menentukan harga maksimum yang kurang dari harga Spot saat ini, Instans Spot Anda tidak akan diluncurkan.
  - Jika Anda menentukan harga maksimum melebihi harga Spot saat ini, Instans Spot Anda akan diluncurkan dan dikenai biaya sesuai harga Spot saat ini. Setelah Instans Spot berjalan, jika harga Spot naik di atas harga maksimum, Amazon EC2 akan menginterupsi Instans Spot Anda.
  - Berapa pun harga maksimum yang Anda tentukan, Anda akan selalu dikenai biaya sesuai harga Spot saat ini.

  Untuk meninjau tren harga Spot, lihat Lihat riwayat harga Spot Instance.

ii. Tipe permintaan: Permintaan Instans Spot yang dipilih menentukan apa yang terjadi jika Instans Spot Anda diinterupsi.

- Satu kali: Amazon EC2 menempatkan permintaan satu kali untuk Instans Spot Anda. Jika Instans Spot Anda diinterupsi, permintaan tidak akan dikirim ulang.

- Permintaan persisten: Amazon EC2 menempatkan permintaan persisten untuk Instans Spot Anda. Jika Instans Spot Anda diinterupsi, permintaan dikirimkan ulang untuk mengisi Instans Spot yang diinterupsi.

Jika Anda tidak menentukan nilai, default-nya adalah permintaan satu kali.

iii. Berlaku hingga: Tanggal kedaluwarsa dari permintaan Instans Spot persisten.

Bidang ini tidak didukung untuk permintaan satu kali. Permintaan satu kali tetap aktif hingga semua instans dalam permintaan diluncurkan atau Anda membatalkan permintaan.

- Tidak ada tanggal kedaluwarsa permintaan: Permintaan tetap aktif hingga Anda membatalkannya.
- Atur tanggal kedaluwarsa permintaan Anda: Permintaan persisten tetap aktif hingga tanggal yang Anda tentukan, atau sampai Anda membatalkannya.

iv. Perilaku interupsi: Perilaku yang Anda pilih menentukan apa yang terjadi saat Instans Spot diinterupsi.

- Untuk permintaan persisten, nilai yang valid adalah Berhenti dan Hibernasi. Saat instans dihentikan, biaya penyimpanan volume EBS diterapkan.

> **Note**
>
> Instans Spot sekarang menggunakan fungsi hibernasi yang sama seperti Instans Sesuai Permintaan. Untuk mengaktifkan hibernasi, Anda dapat memilih Hibernasi di sini, atau Anda dapat memilih Aktifkan dari bidang Perilaku Berhenti - Hibernasi, yang muncul lebih rendah di wizard peluncuran instans. Untuk prasyarat hibernasi, lihat Prasyarat untuk hibernasi instans EC2.

- Untuk permintaan satu kali, hanya Akhiri yang valid.

Jika Anda tidak menentukan nilai, default-nya Akhiri, yang tidak valid untuk permintaan Instans Spot yang persisten. Jika Anda mempertahankan default dan mencoba meluncurkan permintaan Instans Spot persisten, Anda akan mendapatkan pesan kesalahan.

Untuk informasi selengkapnya, lihat Perilaku interupsi Instance Spot.

11. Pada panel Ringkasan, untuk Jumlah instans, masukkan jumlah instans yang akan diluncurkan.

    > **Note**
    >
    > Amazon EC2 membuat permintaan terpisah untuk setiap Instans Spot.

12. Pada panel Ringkasan, tinjau detail instans Anda, dan buat perubahan yang diperlukan. Setelah mengirimkan permintaan Instans Spot, Anda tidak dapat mengubah parameter permintaan. Anda dapat secara langsung menavigasi ke bagian di wizard peluncuran instans dengan memilih tautannya di panel Ringkasan. Untuk informasi selengkapnya, lihat Ringkasan.
13. Ketika Anda siap untuk meluncurkan instans Anda, pilih Launch instans.

    Jika instans gagal diluncurkan atau status langsung menjadi `terminated`, bukan `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

AWS CLI

Untuk membuat permintaan Instans Spot menggunakan run-instances

Gunakan perintah run-instance dan tentukan opsi Spot Instance dalam `--instance-market-options` parameter sebagai berikut.

```
--instance-market-options file://spot-options.json
```

Berikut ini adalah struktur data untuk menentukan dalam file JSON. Anda juga dapat menentukan `ValidUntil` dan `InstanceInterruptionBehavior`. Jika Anda tidak menentukan bidang dalam struktur data, maka nilai default yang akan digunakan.

Contoh berikut membuat permintaan `persistent`.

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
```

```
}
```

Untuk membuat permintaan Instance Spot menggunakan request-spot-instances

> **Note**
>
> Kami sangat tidak menyarankan menggunakan request-spot-instancesperintah untuk meminta Instance Spot karena ini adalah API lama tanpa investasi yang direncanakan. Untuk informasi selengkapnya, lihat Metode permintaan Spot mana yang terbaik untuk digunakan?

Gunakan request-spot-instancesperintah untuk membuat permintaan satu kali.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Gunakan request-spot-instancesperintah untuk membuat permintaan persisten.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Misalnya, file spesifikasi peluncuran untuk digunakan dengan perintah ini, lihat Contoh spesifikasi peluncuran permintaan Instans Spot. Jika mengunduh file spesifikasi peluncuran dari konsol Permintaan Spot, Anda harus menggunakan request-spot-fleetperintah (konsol Permintaan Spot menentukan permintaan Instans Spot menggunakan Armada Spot).

PowerShell

Untuk membuat permintaan Instans Spot

Gunakan New-EC2Instancecmdlet dan tentukan opsi Instance Spot menggunakan parameter. `-InstanceMarketOption`

```
-InstanceMarketOptions $marketOptions
```

Buat struktur data untuk opsi Spot Instance sebagai berikut.

```
$spotOptions = New-Object Amazon.EC2.Model.SpotMarketOptions
$spotOptions.SpotInstanceType="persistent"
$marketOptions = New-Object Amazon.EC2.Model.InstanceMarketOptionsRequest
$marketOptions.MarketType = "spot"
$marketOptions.SpotOptions = $spotOptions
```

Contoh spesifikasi peluncuran permintaan Instans Spot

Contoh berikut menunjukkan konfigurasi peluncuran yang dapat Anda gunakan dengan request-spot-instancesperintah untuk membuat permintaan Instans Spot. Untuk informasi selengkapnya, lihat Mengelola Instans Spot Anda.

> **Important**
>
> Kami sangat tidak menyarankan menggunakan request-spot-instancesperintah untuk meminta Instance Spot karena ini adalah API lama tanpa investasi yang direncanakan. Untuk informasi selengkapnya, lihat Metode permintaan Spot mana yang terbaik untuk digunakan?

Contoh

- Contoh 1: Luncurkan Instans Spot
- Contoh 2: Luncurkan Instans Spot dalam Zona Ketersediaan yang ditentukan
- Contoh 3: Luncurkan Instans Spot di subnet yang ditentukan
- Contoh 4: Luncurkan Instans Spot Khusus

Contoh 1: Luncurkan Instans Spot

Contoh berikut tidak menyertakan Zona Ketersediaan atau subnet. Amazon EC2 memilih Zona Ketersediaan untuk Anda. Amazon EC2 meluncurkan instans di subnet default dari Zona Ketersediaan yang dipilih.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
```

```
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Contoh 2: Luncurkan Instans Spot dalam Zona Ketersediaan yang ditentukan

Contoh berikut mencakup Zona Ketersediaan. Amazon EC2 meluncurkan instans di subnet default dari Zona Ketersediaan yang dipilih.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Contoh 3: Luncurkan Instans Spot di subnet yang ditentukan

Contoh berikut menyertakan subnet. Amazon EC2 meluncurkan instans di subnet yang ditentukan. Jika VPC adalah VPC nondefault, instance tidak menerima alamat publik secara default. IPv4

```
{
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Untuk menetapkan IPv4 alamat publik ke instance dalam VPC nondefault, tentukan `AssociatePublicIpAddress` bidang seperti yang ditunjukkan pada contoh berikut. Saat Anda menentukan antarmuka jaringan, Anda harus menyertakan ID subnet dan ID grup

keamanan menggunakan antarmuka jaringan, daripada menggunakan bidang `SubnetId` dan `SecurityGroupIds` seperti yang ditunjukkan dalam blok kode sebelumnya.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Contoh 4: Luncurkan Instans Spot Khusus

Contoh berikut meminta Instans Spot dengan penghunian `dedicated`. Instans Spot Khusus harus diluncurkan di VPC.

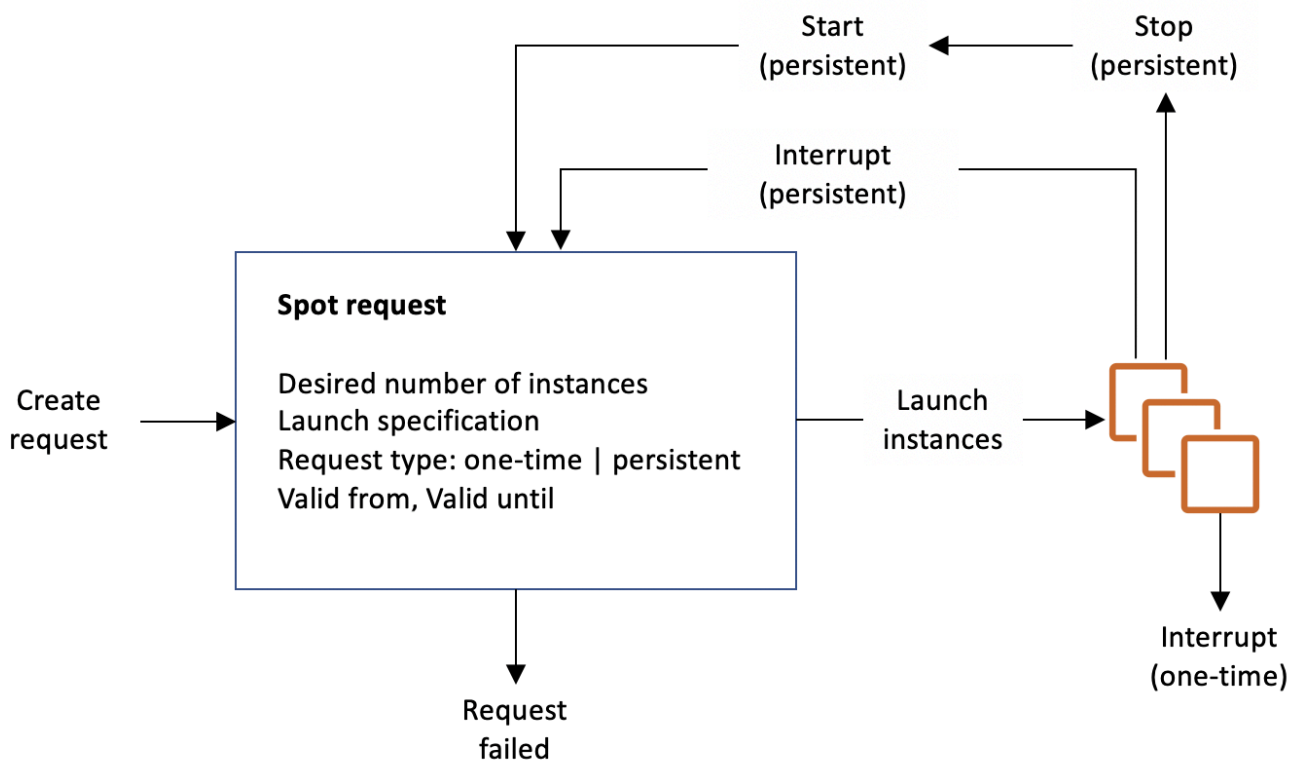
```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Mendapatkan status permintaan Instans Spot

Untuk membantu Anda melacak permintaan Instans Spot dan merencanakan penggunaan Instans Spot, gunakan status permintaan yang disediakan oleh Amazon EC2. Misalnya, status permintaan dapat memberikan alasan mengapa permintaan Spot Anda belum terpenuhi, atau mencantumkan kendala yang mencegah pemenuhan permintaan Spot Anda.

Pada setiap langkah proses—disebut juga dengan siklus hidup permintaan Spot—peristiwa spesifik menentukan status permintaan secara berurutan.

Ilustrasi berikut menunjukkan cara kerja permintaan Instans Spot. Perhatikan bahwa tipe permintaan (satu kali atau tetap) menentukan apakah permintaan dibuka lagi saat Amazon EC2 menginterupsi Instans Spot atau jika Anda menghentikan Instans Spot. Jika permintaan tetap ada, permintaan dibuka lagi setelah Instans Spot Anda diinterupsi. Jika permintaan tetap ada dan Anda menghentikan Instans Spot, permintaan tersebut hanya terbuka setelah Anda memulai Instans Spot.



Daftar Isi

- Dapatkan informasi status permintaan
- Kode status permintaan Spot
- Peristiwa Pemenuhan Permintaan Instans Spot EC2
- Perubahan status untuk permintaan Spot

Dapatkan informasi status permintaan

Anda bisa mendapatkan informasi status untuk permintaan Instans Spot Anda.

Console

Untuk mendapatkan informasi status permintaan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot, lalu pilih permintaan Spot.
3. Untuk memeriksa status, pada tab Deskripsi, periksa bidang Status.

AWS CLI

Untuk mendapatkan informasi status permintaan

Gunakan perintah berikut describe-spot-instance-requests.

```
aws ec2 describe-spot-instance-requests --spot-instance-request-
ids sir-0e54a519c9EXAMPLE
```

PowerShell

Untuk mendapatkan informasi status permintaan

Gunakan Get-EC2SpotInstanceRequestcmdlet.

```
Get-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE
```

Kode status permintaan Spot

Informasi status permintaan Spot terdiri dari kode status, waktu pembaruan, dan pesan status. Semua itu membantu Anda menentukan disposisi permintaan Spot Anda.

Berikut ini adalah kode status permintaan Spot:

`az-group-constraint`

Amazon EC2 tidak dapat meluncurkan semua instans yang Anda minta di Zona Ketersediaan yang sama.

`bad-parameters`

Satu atau lebih parameter untuk permintaan Spot Anda tidak valid (misalnya, AMI yang Anda tentukan tidak ada). Pesan status menunjukkan parameter mana yang tidak valid.

`canceled-before-fulfillment`

Pengguna membatalkan permintaan Spot sebelum permintaan dipenuhi.

`capacity-not-available`

Tidak tersedia kapasitas yang cukup untuk instans yang Anda minta.

`constraint-not-fulfillable`

Permintaan Spot tidak dapat dipenuhi karena satu atau beberapa batasan tidak valid (misalnya, Zona Ketersediaan tidak ada). Pesan status menunjukkan batasan mana yang tidak valid.

`fulfilled`

Permintaan Spot adalah `active`, dan Amazon EC2 meluncurkan Instans Spot Anda.

`instance-stopped-by-price`

Instans Anda berhenti karena harga Spot melebihi harga maksimum Anda.

`instance-stopped-by-user`

Instans Anda berhenti karena pengguna menghentikan instans atau menjalankan perintah penonaktifan dari instans tersebut.

`instance-stopped-no-capacity`

Instans Anda berhenti karena kebutuhan manajemen kapasitas EC2.

`instance-terminated-by-price`

Instans Anda diakhiri karena harga Spot melebihi harga maksimum Anda. Jika permintaan Anda persisten, prosesnya akan dimulai ulang, jadi permintaan Anda menunggu evaluasi.

`instance-terminated-by-schedule`

Instans Spot Anda diakhiri di akhir durasi yang dijadwalkan.

`instance-terminated-by-service`

Instans Anda dihentikan dari status berhenti.

`instance-terminated-by-user` atau `spot-instance-terminated-by-user`

Anda mengakhiri Instans Spot yang telah terpenuhi, jadi status permintaannya adalah `closed` (kecuali permintaan persisten) dan status instans adalah `terminated`.

`instance-terminated-launch-group-constraint`

Satu atau beberapa instans dalam grup peluncuran Anda telah diakhiri, sehingga batasan grup peluncuran tidak lagi dipenuhi.

`instance-terminated-no-capacity`

Instans Anda diakhiri karena proses manajemen kapasitas standar.

`launch-group-constraint`

Amazon EC2 tidak dapat meluncurkan semua instans yang Anda minta pada saat yang bersamaan. Semua instans dalam grup peluncuran dimulai dan diakhiri bersama.

`limit-exceeded`

Batas jumlah volume EBS atau total volume penyimpanan telah terlampaui. Untuk informasi selengkapnya, lihat Kuota untuk Amazon EBS di Panduan Pengguna Amazon EBS.

`marked-for-stop`

Instans Spot ditandai karena berhenti.

`marked-for-termination`

Instans Spot ditandai karena pengakhiran.

`not-scheduled-yet`

Permintaan Spot tidak dievaluasi hingga tanggal yang dijadwalkan.

`pending-evaluation`

Setelah Anda membuat permintaan Instans Spot, permintaan itu masuk dalam status `pending-evaluation` sementara sistem mengevaluasi parameter permintaan Anda.

`pending-fulfillment`

Amazon EC2 mencoba menyediakan Instans Spot Anda.

`placement-group-constraint`

Permintaan Spot belum dapat dipenuhi karena Instans Spot tidak dapat ditambahkan ke grup penempatan saat ini.

`price-too-low`

Permintaan belum dapat dipenuhi karena harga maksimum Anda di bawah harga Spot. Dalam kasus ini, tidak ada instans yang diluncurkan dan permintaan Anda tetap `open`.

`request-canceled-and-instance-running`

Anda membatalkan permintaan Spot saat Instans Spot masih berjalan. Permintaannya `cancelled`, tapi instans tetap `running`.

`schedule-expired`

Permintaan Spot kedaluwarsa karena tidak terpenuhi sebelum tanggal yang ditentukan.

`system-error`

Terjadi kesalahan sistem yang tidak terduga. Jika ini adalah masalah yang berulang, silakan hubungi AWS Dukungan untuk bantuan.

Peristiwa Pemenuhan Permintaan Instans Spot EC2

Ketika permintaan Instans Spot terpenuhi, Amazon EC2 mengirimkan peristiwa Pemenuhan Permintaan Instans Spot EC2 ke Amazon. EventBridge Anda dapat membuat aturan untuk mengambil tindakan kapan pun peristiwa ini terjadi, seperti menginvokasi fungsi Lambda atau memberi tahu topik Amazon SNS.

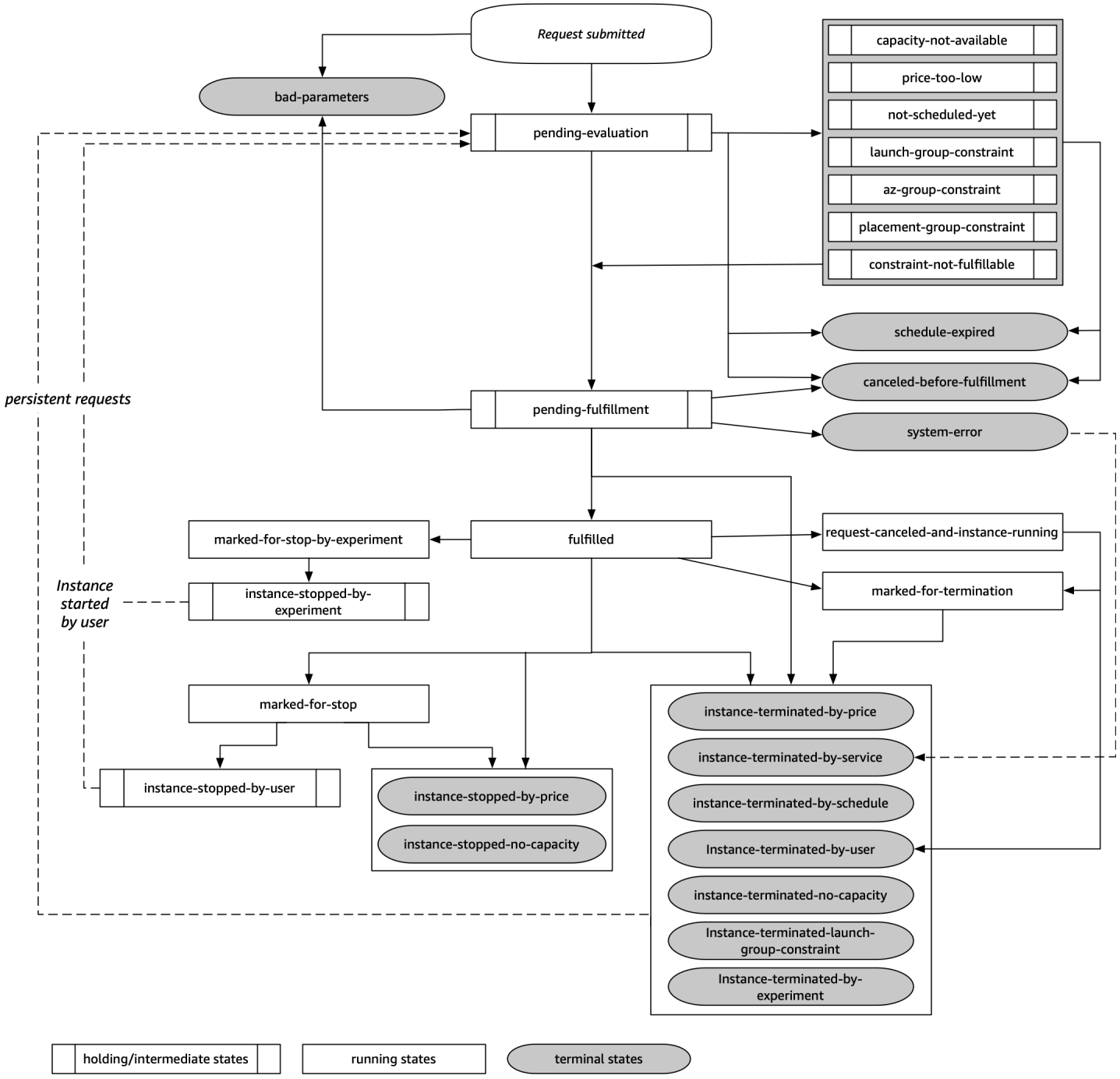
Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-0e54a519c9EXAMPLE",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Perubahan status untuk permintaan Spot

Diagram berikut menunjukkan kepada Anda jalur yang dapat diikuti oleh permintaan Spot Anda sepanjang siklus hidupnya, dari pengiriman hingga pengakhiran. Setiap langkah digambarkan sebagai suatu simpul, dan kode status untuk setiap simpul menjelaskan status permintaan Spot dan Instans Spot.



Evaluasi tertunda

Segera setelah Anda membuat permintaan Instans Spot, permintaan itu masuk ke status `pending-evaluation` kecuali jika ada satu atau lebih parameter permintaan yang tidak valid (`bad-parameters`).

Kode status	Status permintaan	Status instans
`pending-evaluation`	`open`	Tidak berlaku
`bad-parameters`	`closed`	Tidak berlaku

Menunggu

Jika satu atau beberapa batasan permintaan sudah valid tetapi belum dapat dipenuhi, atau jika kapasitas tidak mencukupi, permintaan masuk ke status menunggu sampai batasan tersebut terpenuhi. Opsi permintaan memengaruhi kemungkinan permintaan dipenuhi. Misalnya, jika tidak ada kapasitas, permintaan Anda akan tetap dalam status menunggu hingga ada kapasitas yang tersedia. Jika Anda menentukan grup Zona Ketersediaan, permintaan tetap dalam status menunggu hingga batasan Zona Ketersediaan terpenuhi.

Jika terjadi pemadaman di salah satu Zona Ketersediaan, ada kemungkinan kapasitas EC2 cadangan yang tersedia untuk permintaan Instans Spot di Zona Ketersediaan lainnya dapat terpengaruh.

Kode status	Status permintaan	Status instans
`capacity-not-available`	`open`	Tidak berlaku
`price-too-low`	`open`	Tidak berlaku
`not-scheduled-yet`	`open`	Tidak berlaku
`launch-group-constraint`	`open`	Tidak berlaku
`az-group-constraint`	`open`	Tidak berlaku

Kode status	Status permintaan	Status instans
`placement-group-constraint`	`open`	Tidak berlaku
`constraint-not-fulfillable`	`open`	Tidak berlaku

Evaluasi tertunda/terminal pemenuhan

Permintaan Instans Spot Anda dapat masuk ke status `terminal` jika Anda membuat permintaan yang valid hanya selama jangka waktu tertentu dan jangka waktu ini berakhir sebelum permintaan Anda mencapai fase pemenuhan tertunda. Mungkin juga terjadi jika Anda membatalkan permintaan, atau jika terjadi kesalahan sistem.

Kode status	Status permintaan	Status instans
`schedule-expired`	`cancelled`	Tidak berlaku
`canceled-before-fulfillment` [1]	`cancelled`	Tidak berlaku
`bad-parameters`	`failed`	Tidak berlaku
`system-error`	`closed`	Tidak berlaku

[1] Jika Anda membatalkan permintaan.

Pemenuhan tertunda

Ketika batasan yang Anda tentukan (jika ada) terpenuhi, permintaan Spot Anda masuk ke status `pending-fulfillment`.

Pada titik ini, Amazon EC2 sedang bersiap untuk menyediakan instans yang Anda minta. Jika proses berhenti pada titik ini, kemungkinan besar karena proses itu dibatalkan oleh pengguna sebelum Instans Spot diluncurkan. Hal ini mungkin juga karena terjadi kesalahan sistem yang tidak terduga.

Kode status	Status permintaan	Status instans
`pending-fulfillment`	`open`	Tidak berlaku

Terpenuhi

Saat semua spesifikasi untuk Instans Spot Anda terpenuhi, permintaan Spot Anda dipenuhi. Amazon EC2 meluncurkan Instans Spot, yang dapat memerlukan waktu beberapa menit. Jika Instans Spot menjalani hibernasi atau berhenti saat diinterupsi, Instans Spot tetap dalam status ini hingga permintaan dapat dipenuhi lagi atau permintaan dibatalkan.

Kode status	Status permintaan	Status instans
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Jika Anda menghentikan Instans Spot, permintaan Spot Anda akan masuk dalam status `marked-for-stop` atau `instance-stopped-by-user` hingga Instans Spot dapat dimulai lagi atau permintaan dibatalkan.

Kode status	Status permintaan	Status instans
`marked-for-stop`	`active`	`stopping`
`instance-stopped-by-user`[1]	`disabled` atau `cancelled`[2]	`stopped`

* Instans Spot masuk dalam status `instance-stopped-by-user` jika Anda menghentikan instans atau menjalankan perintah pematian dari instans. Setelah Anda menghentikan instans, Anda dapat memulainya lagi. Saat memulai ulang, permintaan Instans Spot kembali ke status `pending-evaluation` dan Amazon EC2 meluncurkan Instans Spot baru ketika batasan terpenuhi.

² Status permintaan Spot adalah `disabled` jika Anda menghentikan Instans Spot tetapi tidak membatalkan permintaan. Status permintaan adalah `cancelled` jika Instans Spot Anda dihentikan dan permintaan kedaluwarsa.

Terminal terpenuhi

Instans Spot Anda terus berjalan selama ada kapasitas yang tersedia untuk tipe instans Anda, dan Anda tidak mengakhiri instans. Jika Amazon EC2 harus mengakhiri Instans Spot Anda, permintaan Spot masuk ke status terminal. Permintaan juga masuk ke status terminal jika Anda membatalkan permintaan Spot atau mengakhiri Instans Spot.

Kode status	Status permintaan	Status instans
`request-canceled-and-instance-running`	`cancelled`	`running`
`marked-for-stop`	`active`	`running`
`marked-for-termination`	`active`	`running`
`instance-stopped-by-price`	`disabled`	`stopped`
`instance-stopped-by-user`	`disabled`	`stopped`
`instance-stopped-no-capacity`	`disabled`	`stopped`
`instance-terminated-by-price`	`closed`(satu kali),open (gigih)	`terminated`
`instance-terminated-by-schedule`	`closed`	`terminated`
`instance-terminated-by-service`	`cancelled`	`terminated`

Kode status	Status permintaan	Status instans
`instance-terminated-by-user`	`closed` atau `cancelled` [1]	`terminated`
`instance-terminated-no-capacity`	`closed`(satu kali),`open` (gigih)	`running` †
`instance-terminated-no-capacity`	`closed`(satu kali),`open` (gigih)	`terminated`
`instance-terminated-launch-group-constraint`	`closed`(satu kali),`open` (gigih)	`terminated`

* Status permintaan adalah `closed` jika Anda mengakhiri instans, tetapi tidak membatalkan permintaan. Status permintaan adalah `cancelled` jika Anda mengakhiri instans dan membatalkan permintaan. Meskipun Anda mengakhiri Instans Spot sebelum Anda membatalkan permintaannya, penundaan mungkin terjadi sebelum Amazon EC2 mendeteksi bahwa Instans Spot Anda telah diakhiri. Dalam hal ini, status permintaan bisa berupa `closed` atau `cancelled`.

† Saat Amazon EC2 menginterupsi Instans Spot karena memerlukan kapasitas kembali dan instans dikonfigurasi untuk berakhir saat terjadi interupsi, status akan segera diatur ke `instance-terminated-no-capacity` (tidak diatur ke `marked-for-termination`). Namun, instans tetap dalam status `running` selama 2 menit untuk mencerminkan periode 2 menit saat instans menerima pemberitahuan interupsi Instans Spot. Setelah 2 menit, status instans diatur ke `terminated`.

Eksperimen interupsi

Anda dapat menggunakan AWS Fault Injection Service untuk memulai interupsi Instans Spot sehingga Anda dapat menguji bagaimana aplikasi di Instans Spot merespons. Jika AWS FIS menghentikan Instans Spot, permintaan Spot Anda memasuki `marked-for-stop-by-experiment` status dan kemudian `instance-stopped-by-experiment` status. Jika AWS FIS mengakhiri Instans Spot, permintaan Spot Anda memasuki `instance-terminated-by-experiment` status. Untuk informasi selengkapnya, lihat the section called “Memulai interupsi”.

Kode status	Status permintaan	Status instance
`marked-for-stop-by-experiment`	`active`	`running`
`instance-stopped-by-experiment`	`disabled`	`stopped`
`instance-terminated-by-experiment`	`closed`	`terminated`

Permintaan yang persisten

Saat Instans Spot Anda diakhiri (baik oleh Anda maupun Amazon EC2), jika permintaan Spot adalah permintaan yang persisten, instans akan kembali ke status `pending-evaluation` dan Amazon EC2 dapat meluncurkan Instans Spot baru saat batasan terpenuhi.

Menandai permintaan Instans Spot

Untuk membantu mengategorikan dan mengelola permintaan Instans Spot, Anda dapat menandainya dengan metadata kustom. Anda dapat menetapkan tanda untuk permintaan Instans Spot saat Anda membuatnya, atau setelahnya. Anda dapat menetapkan tanda menggunakan konsol Amazon EC2 atau alat baris perintah.

Saat Anda menandai permintaan Instans Spot, instans dan volume yang diluncurkan oleh Instans Spot tidak secara otomatis ditandai. Anda perlu menandai instans dan volume yang diluncurkan oleh Instans Spot secara eksplisit. Anda dapat menetapkan tanda ke Instans Spot dan volume selama peluncuran, atau setelahnya.

Untuk informasi selengkapnya tentang cara kerja tag, lihat Tandai sumber daya Amazon EC2 Anda.

Daftar Isi

- Prasyarat
- Menandai permintaan Instans Spot baru
- Menandai permintaan Instans Spot yang ada
- Melihat tanda permintaan Instans Spot

Prasyarat

Berikan izin kepada pengguna untuk menandai sumber daya. Untuk informasi selengkapnya tentang kebijakan IAM dan contoh kebijakan, lihat Contoh: Memberi tanda pada sumber daya.

Kebijakan IAM yang Anda buat ditentukan oleh metode yang Anda gunakan untuk membuat permintaan Instans Spot.

- Jika Anda menggunakan wizard peluncuran instans atau `run-instances` untuk meminta Instans Spot, lihat To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Jika Anda menggunakan perintah `request-spot-instances` untuk meminta Instans Spot, lihat To grant a user the permission to tag resources when using request-spot-instances.

Untuk memberikan izin menandai sumber daya kepada pengguna saat menggunakan wizard peluncuran instans atau run-instances

Buat kebijakan IAM yang mencakup hal-hal berikut:

- Tindakan `ec2:RunInstances`. Tindaka ini memberikan izin kepada pengguna untuk meluncurkan sebuah instans.
- Untuk, `Resource`tentukan.`spot-instances-request` Ini memungkinkan pengguna untuk membuat permintaan Instans Spot, yang meminta Instans Spot.
- Tindakan `ec2:CreateTags`. Tindakan ini memberikan izin kepada pengguna untuk membuat tanda.
- Untuk `Resource`, tentukan `*`. Hal ini memungkinkan para pengguna untuk menandai semua sumber daya yang dibuat selama peluncuran.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
```

```
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Saat Anda menggunakan RunInstances tindakan untuk membuat permintaan Instans Spot dan menandai permintaan Instans Spot saat membuat, Anda harus mengetahui cara Amazon EC2 mengevaluasi `spot-instances-request` sumber daya dalam RunInstances pernyataan yang dievaluasi dalam kebijakan IAM sebagai berikut:

- Jika Anda tidak memberi tag pada permintaan Instans Spot saat dibuat, Amazon EC2 tidak mengevaluasi`spot-instances-request` sumber daya di RunInstances pernyataan.
- Jika Anda memberi tag pada permintaan Instans Spot saat dibuat, Amazon EC2 mengevaluasi`spot-instances-request` sumber daya di RunInstances pernyataan.

Oleh karena itu, untuk sumber daya `spot-instances-request`, aturan-aturan berikut berlaku untuk kebijakan IAM:

- Jika Anda menggunakan RunInstances untuk membuat permintaan Instance Spot dan Anda tidak bermaksud untuk menandai permintaan Instans Spot saat membuat, Anda tidak perlu secara eksplisit mengizinkan `spot-instances-request` sumber daya; panggilan akan berhasil.
- Jika Anda menggunakan RunInstances untuk membuat permintaan Instans Spot dan bermaksud untuk menandai permintaan Instans Spot saat membuat, Anda harus menyertakan `spot-`

`instances-request` sumber daya dalam pernyataan RunInstances allow, jika tidak panggilan akan gagal.

- Jika Anda menggunakan RunInstances untuk membuat permintaan Instans Spot dan bermaksud untuk menandai permintaan Instans Spot saat membuat, Anda harus menentukan `spot-instances-request` sumber daya atau menyertakan * wildcard dalam pernyataan CreateTags allow, jika tidak panggilan akan gagal.

Misalnya kebijakan IAM, termasuk kebijakan yang tidak didukung untuk permintaan Instans Spot, lihat Cara Menggunakan Instans Spot.

Untuk memberi pengguna izin untuk menandai sumber daya saat menggunakan request-spot-instances

Buat kebijakan IAM yang mencakup hal-hal berikut:

- Tindakan `ec2:RequestSpotInstances`. Tindakan ini memberikan izin kepada pengguna untuk membuat permintaan Instans Spot.
- Tindakan `ec2:CreateTags`. Tindakan ini memberikan izin kepada pengguna untuk membuat tanda.
- Untuk `Resource`, tentukan `spot-instances-request`. Hal ini memungkinkan pengguna untuk hanya menandai permintaan Instans Spot.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-
request/*"
        }
    ]
```

```
}
```

Menandai permintaan Instans Spot baru

Dalam PowerShell contoh AWS CLI dan, konfigurasikan permintaan Instans Spot sebagai berikut:

- Untuk `ResourceType`, tentukan `spot-instances-request`. Jika Anda menentukan nilai lain, maka permintaan Instans Spot akan gagal.
- Untuk `Tags`, tentukan pasangan nilai-kunci. Anda dapat menentukan lebih dari satu pasangan nilai-kunci.

Console

Untuk menandai permintaan Instans Spot baru

1. Ikuti prosedur Mengelola Instans Spot Anda.
2. Untuk menambahkan tanda, pada halaman Tambahkan Tanda, pilih Tambahkan Tanda, lalu masukkan kunci dan nilai untuk tanda tersebut. Pilih Tambahkan tanda lain untuk setiap tanda tambahan.

   Untuk setiap tanda, Anda dapat menandai permintaan Instans Spot, Instans Spot, dan volume dengan tanda yang sama. Untuk menandai ketiganya, pastikan bahwa Instans, Volume, dan Permintaan Instans Spot telah dipilih. Untuk menandai hanya satu atau dua, pastikan bahwa sumber daya yang ingin Anda tandai telah dipilih, dan pilihan pada sumber daya lainnya dihapus.
3. Lengkapi bidang yang diperlukan untuk membuat permintaan Instans Spot, lalu pilih Luncurkan. Untuk informasi selengkapnya, lihat Mengelola Instans Spot Anda.

AWS CLI

Untuk menandai permintaan Instans Spot baru

Gunakan perintah request-spot-instances dengan opsi `--tag-specification`.

Spesifikasi tag menambahkan dua tag ke permintaan Spot Instance: `Environment=Production` dan`Cost-Center=123`.

```
aws ec2 request-spot-instances \
```

```
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

PowerShell

Untuk menandai permintaan Instans Spot baru

Gunakan Request-EC2SpotInstancecmdlet dengan parameter. `-TagSpecification`

```
-TagSpecification $tagspec
```

Spesifikasi tag didefinisikan sebagai berikut. Ini menambahkan dua tag ke permintaan Spot Instance: `Environment=Production` dan`Cost-Center=123`.

```
$tag1 = @{Key="Environment"; Value="Production"}
$tag2 = @{Key="Cost-Center"; Value="123"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "spot-instances-request"
$tagspec.Tags = @($tag1,$tag2)
```

Menandai permintaan Instans Spot yang ada

Console

Untuk menandai permintaan Instans Spot yang ada

Setelah Anda membuat permintaan Instans Spot, Anda dapat menambahkan tanda ke permintaan Instans Spot menggunakan konsol.

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Instans Spot Anda.
4. Pilih tab Tanda dan pilih Buat Tanda.

Untuk menandai permintaan Instans Spot yang sudah ada menggunakan konsol

Setelah permintaan Instans Spot Anda meluncurkan Instans Spot, Anda dapat menambahkan tanda ke instans menggunakan konsol. Untuk informasi selengkapnya, lihat Tambahkan tag menggunakan konsol.

AWS CLI

Untuk menandai permintaan Instans Spot atau Instance Spot yang ada

Gunakan perintah create-tags untuk menandai sumber daya yang ada. Dalam contoh berikut, permintaan Instans Spot yang ada dan Instance Spot ditandai dengan`purpose=test`.

```
aws ec2 create-tags \
    --resources sir-0e54a519c9EXAMPLE i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

PowerShell

Untuk menandai permintaan Instans Spot atau Instance Spot yang ada

Gunakan New-EC2Tagcmdlet. Contoh berikut menambahkan tag `purpose=test` ke permintaan Instans Spot yang ada dan Instance Spot.

```
New-EC2Tag `
    -Resource sir-0e54a519c9EXAMPLE, i-1234567890abcdef0 `
    -Tag @{Key="purpose"; Value="test"}
```

Melihat tanda permintaan Instans Spot

Console

Untuk melihat tag permintaan Instans Spot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Instans Spot Anda dan pilih tab Tanda.

AWS CLI

Untuk mendeskripsikan tag permintaan Instans Spot

Gunakan describe-spot-instance-requestsperintah untuk melihat konfigurasi permintaan Instans Spot yang ditentukan, yang mencakup tag apa pun yang ditentukan untuk permintaan tersebut.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-0e54a519c9EXAMPLE \
    --query "SpotInstanceRequests[*].Tags"
```

Berikut ini adalah output contoh.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

PowerShell

Untuk mendeskripsikan tag permintaan Instans Spot

Gunakan Get-EC2SpotInstanceRequestcmdlet.

```
(Get-EC2SpotInstanceRequest `
    -SpotInstanceRequestId sir-0e54a519c9EXAMPLE).Tags
```

Berikut ini adalah output contoh.

```
Key         Value
---         -----
Environment Production
Department  101
```

Membatalkan permintaan Instans Spot

Jika Anda tidak lagi menginginkan permintaan Instans Spot, Anda dapat membatalkannya. Anda hanya dapat membatalkan permintaan Instans Spot yang `open`, `active`, atau `disabled`.

- Permintaan Instans Spot Anda adalah `open` saat permintaan Anda belum dipenuhi dan belum ada instans yang diluncurkan.
- Permintaan Instans Spot Anda adalah `active` saat permintaan Anda telah dipenuhi sehingga Instans Spot telah diluncurkan.
- Permintaan Instans Spot Anda adalah `disabled` saat Anda menghentikan Instans Spot Anda.

Jika permintaan Instans Spot Anda adalah `active` dan memiliki Instans Spot terkait yang sedang berjalan, membatalkan permintaan tidak akan menghentikan instans tersebut. Untuk informasi selengkapnya tentang pengakhiran Instans Spot, lihat Menghentikan Instans Spot.

Console

Untuk membatalkan permintaan Instans Spot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Instans Spot.
4. Pilih Tindakan, Batalkan permintaan.
5. (Opsional) Jika Anda telah selesai menggunakan Instans Spot terkait, Anda dapat mengakhirinya. Dalam kotak dialog Batalkan permintaan Spot, pilih Akhiri instans, lalu pilih Konfirmasi.

AWS CLI

Untuk membatalkan permintaan Instans Spot

Gunakan perintah berikut cancel-spot-instance-requests.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-
ids sir-0e54a519c9EXAMPLE
```

PowerShell

Untuk membatalkan permintaan Instans Spot

Gunakan Stop-EC2SpotInstanceRequestcmdlet.

```
Stop-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE
```

Mengelola Instans Spot Anda

Amazon EC2 meluncurkan Instans Spot saat kapasitas tersedia. Instans Spot berjalan hingga diinterupsi atau Anda mengakhirinya sendiri.

Daftar Isi

- Temukan Instans Spot Anda
- Temukan instance yang diluncurkan oleh permintaan tertentu
- Menghentikan Instans Spot
- Memulai Instans Spot
- Menghentikan Instans Spot

Temukan Instans Spot Anda

Instans Spot muncul di halaman Instans di konsol, bersama dengan Instans Sesuai Permintaan. Gunakan prosedur berikut untuk menemukan Instans Spot Anda.

Console

Untuk menemukan Instans Spot Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Untuk menemukan semua Instans Spot, di panel pencarian, pilih Instance lifecycle=spot.
4. Untuk memverifikasi bahwa instance adalah Instans Spot, pilih instance, pilih tab Detail, dan periksa nilai Siklus Hidup. Nilai untuk Instans Spot adalah `spot` dan nilai untuk Instans On-Demand adalah`normal`.

AWS CLI

Untuk menemukan Instans Spot Anda

Gunakan perintah describe-instance berikut.

```
aws ec2 describe-instances --filters "Name=instance-lifecycle,Values=spot"
```

Untuk menentukan apakah sebuah instance adalah Instans Spot

Gunakan perintah describe-instance berikut.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Jika outputnya`spot`, instance adalah Instans Spot. Jika tidak ada output, instans adalah Instans On-Demand.

PowerShell

Untuk menemukan Instans Spot Anda

Gunakan Get-EC2Instancecmdlet.

```
Get-EC2Instance -Filter @{Name="instance-lifecycle"; Values="spot"}
```

Untuk menentukan apakah sebuah instance adalah Instans Spot

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.InstanceLifecycle
```

Jika outputnya`Spot`, instance adalah Instans Spot. Jika tidak ada output, instans adalah Instans On-Demand.

Temukan instance yang diluncurkan oleh permintaan tertentu

Gunakan prosedur berikut untuk menemukan Instans Spot yang diluncurkan dari permintaan Instance Spot atau Armada Spot tertentu.

Console

Untuk menemukan Instans Spot untuk permintaan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot. Daftar ini berisi permintaan Instans Spot dan permintaan Armada Spot.
3. Jika permintaan Instans Spot terpenuhi, Kapasitas adalah ID dari Instans Spot. Untuk Armada Spot, Kapasitas menunjukkan jumlah permintaan kapasitas yang telah terpenuhi. Untuk melihat instance di Armada Spot, pilih panah perluas, atau pilih armada dan pilih Instans. IDs
4. Untuk Armada Spot, Kapasitas menunjukkan berapa banyak kapasitas yang diminta terpenuhi. Untuk melihat instans di Armada Spot, pilih ID armada untuk membuka halaman detailnya dan cari panel Instans. IDs

AWS CLI

Untuk menemukan Instans Spot untuk permintaan

Gunakan perintah berikut describe-spot-instance-requests.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-0e54a519c9EXAMPLE \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

Berikut ini adalah output contoh:

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
    }
]
```

PowerShell

Untuk menemukan Instans Spot untuk permintaan

Gunakan Get-EC2SpotInstanceRequestcmdlet.

```
(Get-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE).InstanceId
```

Menghentikan Instans Spot

Jika Anda tidak memerlukan Instans Spot sekarang, tetapi Anda ingin memulai ulang nanti tanpa kehilangan data yang disimpan dalam volume Amazon EBS, Anda dapat menghentikannya. Langkah-langkah untuk menghentikan Instans Spot serupa dengan langkah-langkah untuk menghentikan Instans Sesuai Permintaan.

> **Note**
>
> Saat Instans Spot dihentikan, Anda dapat memodifikasi beberapa atribut instans, tetapi tidak untuk tipe instansnya.
> Kami tidak mengenakan biaya penggunaan untuk Instans Spot yang dihentikan, atau biaya transfer data, tetapi kami mengenakan biaya penyimpanan untuk setiap volume Amazon EBS.

Batasan

- Anda hanya dapat menghentikan Instans Spot jika Instans Spot diluncurkan dari Permintaan Instans Spot `persistent`.
- Anda tidak dapat menghentikan Instans Spot jika permintaan Instans Spot yang terkait dibatalkan. Ketika permintaan Instans Spot dibatalkan, Anda hanya dapat mengakhiri Instans Spot.
- Anda tidak dapat menghentikan Instans Spot jika instans itu adalah bagian dari armada atau grup peluncuran, atau grup Zona Ketersediaan.

Console

Untuk menghentikan Instance Spot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih Instans Spot. Jika Anda tidak menyimpan ID instance dari Instance Spot, lihatthe section called “Temukan Instans Spot Anda”.

4. Pilih Status instans, Hentikan instans.
5. Ketika diminta konfirmasi, pilih Berhenti.

AWS CLI

Untuk menghentikan Instance Spot

Gunakan perintah stop-instance untuk menghentikan Instans Spot Anda secara manual.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk menghentikan Instance Spot

Gunakan Stop-EC2Instancecmdlet.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

Memulai Instans Spot

Anda dapat memulai Instans Spot yang sebelumnya Anda hentikan.

Prasyarat

Anda hanya dapat memulai Instans Spot jika:

- Anda menghentikan Instans Spot secara manual.
- Instans Spot adalah instans yang didukung EBS.
- Kapasitas Instans Spot tersedia.
- Harga Spot lebih rendah dari harga maksimum Anda.

Batasan

- Anda tidak dapat memulai Instans Spot jika instans itu adalah bagian dari armada atau grup peluncuran, atau grup Zona Ketersediaan.

Langkah-langkah untuk memulai Instans Spot serupa dengan langkah-langkah untuk memulai Instans Sesuai Permintaan.

Console

Untuk memulai Instance Spot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih Instans Spot. Jika Anda tidak menyimpan ID instance dari Instance Spot, lihatthe section called “Temukan Instans Spot Anda”.
4. Pilih Status instans, Mulai instans.

AWS CLI

Untuk memulai Instance Spot

Gunakan perintah start-instance untuk memulai Instans Spot Anda secara manual.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk memulai Instance Spot

Gunakan Start-EC2Instancecmdlet.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Menghentikan Instans Spot

Warning

Mengakhiri sebuah instance bersifat permanen dan ireversibel.
Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan.

Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Jika Anda mengakhiri Instans Spot yang sedang berjalan atau berhenti yang diluncurkan oleh permintaan Spot persisten, permintaan Instans Spot akan beralih ke status `open` sehingga Instans Spot baru dapat diluncurkan. Untuk memastikan bahwa tidak ada instans Spot baru yang diluncurkan, maka Anda harus terlebih dahulu membatalkan permintaan Instans Spot.

Jika Anda membatalkan permintaan Instans Spot `active` yang memiliki Instans Spot berjalan, maka Instans Spot yang berjalan itu tidak akan berhenti secara otomatis; Anda harus secara manual mengakhiri Instans Spot tersebut.

Jika Anda membatalkan permintaan Instans Spot `disabled` yang memiliki Instans Spot yang berhenti, maka Instans Spot yang berhenti akan secara otomatis diakhiri oleh layanan Amazon EC2 Spot. Mungkin ada jeda pendek antara saat Anda membatalkan permintaan Instans Spot dan ketika layanan Spot mengakhiri Instans Spot.

Untuk informasi selengkapnya, lihat Membatalkan permintaan Instans Spot.

Console

Untuk menghentikan Instans Spot secara manual

1. Sebelum Anda mengakhiri sebuah instans, pastikan bahwa Anda tidak akan kehilangan data apa pun dengan memeriksa apakah volume Amazon EBS Anda tidak akan dihapus pada saat pengakhiran, dan apakah Anda telah menyalin semua data yang Anda perlukan dari volume penyimpanan instans Anda ke penyimpanan persisten, seperti sebagai Amazon EBS atau Amazon S3.
2. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
3. Di panel navigasi, pilih Instans.
4. Pilih Instans Spot. Jika Anda tidak menyimpan ID instance dari Instance Spot, lihatthe section called “Temukan Instans Spot Anda”.
5. Pilih Instance state, Terminate (delete) instance.
6. Pilih Hentikan (hapus) saat diminta konfirmasi.

AWS CLI

Untuk menghentikan Instans Spot secara manual

Gunakan perintah terminate-instance untuk menghentikan Instans Spot Anda secara manual.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

PowerShell

Untuk menghentikan Instans Spot secara manual

Gunakan Remove-EC2Instancecmdlet.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Interupsi Instans Spot

Anda dapat meluncurkan Instans Spot pada kapasitas EC2 cadangan untuk mendapatkan diskon besar, dengan syarat mengembalikan kapasitas itu saat Amazon EC2 membutuhkannya kembali. Saat Amazon EC2 mengklaim kembali Instans Spot, kami menyebut peristiwa ini sebagai interupsi Instans Spot.

Permintaan untuk Instans Spot dapat sangat bervariasi dari waktu ke waktu, dan ketersediaan Instans Spot juga dapat sangat bervariasi tergantung pada berapa banyak instans EC2 yang tidak terpakai yang tersedia. Selalu ada kemungkinan Instans Spot Anda akan diinterupsi. Berikut ini adalah kemungkinan alasan Amazon EC2 menginterupsi Instans Spot Anda:

Kapasitas

Amazon EC2 dapat mengganggu menginterupsi Instans Spot Anda saat membutuhkannya kembali. EC2 mengeklaim kembali instans Anda terutama untuk menggunakan kembali kapasitas, tetapi dapat juga terjadi karena alasan lain seperti pemeliharaan host atau penghentian penggunaan perangkat keras.

Harga

Harga Spot lebih tinggi dari harga maksimum Anda.

Anda dapat menentukan harga maksimum dalam permintaan Spot Anda. Jika Anda menentukan harga maksimum, instans Anda akan lebih sering diinterupsi daripada jika Anda memilih untuk tidak nenentukannya.

Batasan

Jika permintaan Spot Anda menyertakan batasan seperti grup peluncuran atau grup Zona Ketersediaan, Instans Spot diakhiri sebagai grup saat batasan tidak dapat lagi dipenuhi.

Saat Amazon EC2 menyela Instans Spot, Instans Spot akan menghentikan, menghentikan, atau hibernasi instance, tergantung pada perilaku interupsi yang Anda tentukan saat membuat permintaan Spot.

Daftar Isi

- Perilaku interupsi Instance Spot
- Bersiaplah untuk interupsi Spot Instance
- Memulai interupsi Instans Spot
- Pemberitahuan interupsi Instans Spot
- Menemukan Instans Spot yang diinterupsi
- Menentukan apakah Amazon EC2 mengakhiri Instans Spot
- Penagihan untuk Instans Spot yang diinterupsi

Perilaku interupsi Instance Spot

Saat membuat permintaan Spot, Anda dapat menentukan perilaku interupsi. Berikut ini adalah kemungkinan perilaku interupsi:

- Menghentikan
- Hibernasi
- Mengakhiri

Perilaku defaultnya adalah Amazon EC2 menghentikan Instans Spot saat terputus.

Menghentikan Instans Spot yang terinterupsi

Anda dapat menentukan bahwa Amazon EC2 akan menghentikan Instans Spot Anda ketika instans diinterupsi. Tipe permintaan Instans Spot harus `persistent`. Anda tidak dapat menentukan grup

peluncuran dalam permintaan Instans Spot. Untuk Armada EC2 atau Armada Spot, jenis permintaan harus`maintain`.

Pertimbangan-pertimbangan

- Hanya Amazon EC2 yang dapat memulai ulang Instans Spot yang berhenti karena diinterupsi.
- Untuk Instans Spot yang diluncurkan oleh permintaan Instans Spot `persistent`: Amazon EC2 memulai ulang instans yang dihentikan ketika kapasitas tersedia di Zona Ketersediaan yang sama dan untuk tipe instans yang sama dengan instans yang dihentikan (spesifikasi peluncuran yang sama harus digunakan).
- Saat Instans Spot dihentikan, Anda dapat memodifikasi beberapa atribut instans, tetapi tidak untuk tipe instansnya. Jika Anda melepaskan atau menghapus volume EBS, volume tersebut tidak akan dilampirkan saat Instans Spot dimulai. Jika Anda melepaskan volume root dan Amazon EC2 mencoba memulai Instans Spot, instans akan gagal dimulai dan Amazon EC2 akan mengakhiri instans yang berhenti.
- Anda dapat mengakhiri Instans Spot saat instans berhenti.
- Jika Anda membatalkan permintaan Instans Spot, Armada EC2, atau Armada Spot, Amazon EC2 akan mengakhiri semua Instans Spot terkait yang berhenti.
- Saat Instans Spot yang diinterupsi dihentikan, Anda hanya dikenai biaya untuk volume EBS, yang dipertahankan. Dengan Armada EC2 dan Armada Spot, jika Anda memiliki banyak instans yang dihentikan, Anda dapat melebihi batas jumlah volume EBS untuk akun Anda. Untuk informasi selengkapnya tentang cara penagihan saat Instans Spot diinterupsi, lihat Penagihan untuk Instans Spot yang diinterupsi.
- Pastikan Anda terbiasa dengan implikasi berhentinya sebuah instans. Untuk informasi tentang apa yang terjadi saat sebuah instans berhenti, lihat Perbedaan antara status instance.

Menghibernasi Instans Spot yang diinterupsi

Anda dapat menentukan bahwa Amazon EC2 akan menghibernasi Instans Spot Anda ketika instans diinterupsi. Untuk informasi selengkapnya, lihat Hibernasi instans Amazon EC2 Anda.

Amazon EC2 kini menawarkan pengalaman hibernasi yang sama untuk Instans Spot seperti yang saat ini tersedia untuk Instans Sesuai Permintaan. Layanan ini menawarkan dukungan yang lebih luas, yang sekarang mendukung hal-hal berikut ini untuk hibernasi Instans Spot:

- Lebih didukung AMIs
- Lebih banyak keluarga instans yang didukung

- Hibernasi yang diprakarsai pengguna

Mengakhiri Instans Spot yang diinterupsi

Saat menginterupsi Instans Spot, Amazon EC2 mengakhiri instans secara default, kecuali Anda menentukan perilaku interupsi berbeda, seperti berhenti atau hibernasi. Untuk informasi selengkapnya, lihat Mengakhiri instans Amazon EC2.

Bersiaplah untuk interupsi Spot Instance

Permintaan untuk Instans Spot dapat sangat bervariasi dari waktu ke waktu, dan ketersediaan Instans Spot juga dapat sangat bervariasi tergantung pada berapa banyak instans EC2 tidak terpakai yang tersedia. Selalu ada kemungkinan Instans Spot Anda akan diinterupsi. Oleh karena itu, Anda harus memastikan bahwa aplikasi Anda siap menghadapi interupsi Instans Spot.

Kami merekomendasikan Anda untuk mengikuti praktik terbaik ini sehingga Anda siap menghadapi interupsi Instans Spot.

- Buat permintaan Spot menggunakan grup Auto Scaling. Jika Instans Spot Anda diinterupsi, grup Auto Scaling akan secara otomatis meluncurkan instans pengganti. Untuk informasi selengkapnya, lihat Grup Auto Scaling dengan beberapa tipe instans dan opsi pembelian dalam Panduan Pengguna Amazon EC2 Auto Scaling.
- Pastikan instans Anda siap digunakan segera setelah permintaan dipenuhi dengan menggunakan Amazon Machine Image (AMI) yang berisi konfigurasi perangkat lunak yang diperlukan. Anda juga dapat menggunakan data pengguna untuk menjalankan perintah saat memulai.
- Data pada volume penyimpanan instans hilang saat instans dihentikan atau diakhiri. Cadangkan semua data penting pada volume penyimpanan instans ke penyimpanan yang lebih persisten, seperti Amazon S3, Amazon EBS, atau Amazon DynamoDB.
- Simpan data penting secara teratur di tempat yang tidak terpengaruh jika Instans Spot diakhiri. Misalnya, Anda dapat menggunakan Amazon S3, Amazon EBS, atau DynamoDB.
- Bagilah pekerjaan menjadi tugas-tugas kecil (menggunakan Grid, Hadoop, atau arsitektur berbasis antrean) atau gunakan titik pemeriksaan sehingga Anda dapat sering menyimpan pekerjaan.
- Amazon EC2 memancarkan sinyal rekomendasi penyeimbangan kembali ke Instans Spot saat instans berisiko tinggi mengalami interupsi. Anda dapat mengandalkan rekomendasi penyeimbangan kembali untuk secara proaktif mengelola interupsi Instans Spot tanpa harus menunggu pemberitahuan interupsi Instans Spot dua menit. Untuk informasi selengkapnya, lihat Rekomendasi penyeimbangan ulang instans EC2.

- Gunakan pemberitahuan interupsi Instans Spot dua menit untuk memantau status Instans Spot Anda. Untuk informasi selengkapnya, lihat Pemberitahuan interupsi Instans Spot.
- Meskipun kami berusaha semaksimal mungkin untuk memberikan peringatan ini, ada kemungkinan Instans Spot Anda diinterupsi sebelum peringatan tersebut datang. Uji aplikasi Anda untuk memastikan bahwa aplikasi tersebut menangani interupsi instans yang tidak terduga dengan baik, meskipun Anda memantau sinyal rekomendasi penyeimbangan kembali dan pemberitahuan interupsi. Anda dapat melakukan ini dengan menjalankan aplikasi menggunakan Instans Sesuai Permintaan, kemudian mengakhiri sendiri instans sesuai permintaan itu.
- Jalankan eksperimen injeksi kesalahan terkontrol AWS Fault Injection Service untuk menguji bagaimana aplikasi Anda merespons saat Instans Spot Anda terganggu. Untuk informasi selengkapnya, lihat Tutorial: Uji interupsi Instans Spot menggunakan AWS FIS dalam di Panduan Pengguna AWS Fault Injection Service .

Memulai interupsi Instans Spot

Anda dapat memilih permintaan Instans Spot atau permintaan Armada Spot di konsol Amazon EC2 dan memulai interupsi sehingga Anda dapat menguji bagaimana aplikasi di Instans Spot menangani interupsi. Saat Anda memulai interupsi Instans Spot, Amazon EC2 memberi tahu Anda bahwa Instans Spot Anda akan diinterupsi dalam dua menit, dan kemudian, setelah dua menit, instans akan diinterupsi.

Layanan dasar yang melakukan interupsi Instans Spot adalah AWS Fault Injection Service (AWS FIS). Untuk informasi tentang AWS FIS, lihat AWS Fault Injection Service.

> **Note**
>
> Perilaku interupsi adalah `terminate`, `stop`, dan `hibernate`. Jika Anda mengatur perilaku interupsi ke `hibernate`, saat Anda memulai interupsi Instans Spot, proses hibernasi akan segera dimulai.

Memulai interupsi Instans Spot didukung di semua Wilayah AWS kecuali Asia Pasifik (Jakarta), Asia Pasifik (Osaka), Tiongkok (Beijing), Tiongkok (Ningxia), dan Timur Tengah (UEA).

Daftar Isi

- Memulai interupsi Instans Spot
- Verifikasi interupsi Instans Spot

- Kuota

Memulai interupsi Instans Spot

Anda dapat menggunakan konsol EC2 untuk memulai interupsi Instans Spot dengan cepat. Ketika Anda memilih permintaan Instans Spot, Anda dapat memulai interupsi satu Instans Spot. Ketika Anda memilih permintaan Armada Spot, Anda dapat memulai interupsi banyak Instans Spot sekaligus.

Untuk eksperimen lanjutan lainnya untuk menguji interupsi Instans Spot, Anda dapat membuat eksperimen sendiri menggunakan konsol. AWS FIS

Untuk memulai interupsi satu Instans Spot dalam satu permintaan Instans Spot menggunakan konsol EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Instans Spot, lalu pilih Tindakan, Mulai interupsi. Anda tidak dapat memilih banyak permintaan Instans Spot untuk memulai interupsi.
4. Di kotak dialog Mulai interupsi Instans Spot, pada Akses layanan, gunakan peran default, atau pilih peran yang sudah ada. Untuk memilih peran yang sudah ada, pilih Gunakan peran layanan yang ada, lalu untuk Peran IAM, pilih peran yang akan digunakan.
5. Saat Anda siap untuk memulai interupsi Instans Spot, pilih Mulai interupsi.

Untuk memulai interupsi satu atau lebih Instans Spot dalam satu permintaan Armada Spot menggunakan konsol EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot, lalu pilih Tindakan, Mulai interupsi. Anda tidak dapat memilih banyak permintaan Armada Spot untuk memulai interupsi.
4. Dalam kotak dialog Tentukan jumlah Instans Spot, untuk Jumlah instans yang akan diinterupsi, masukkan jumlah Instans Spot yang akan diinterupsi, lalu pilih Konfirmasi.

> **Note**
>
> Jumlahnya tidak dapat melebihi jumlah Instans Spot di armada atau kuota Anda untuk jumlah Instans Spot yang AWS FIS dapat diinterupsi per percobaan.

5. Di kotak dialog Mulai interupsi Instans Spot, pada Akses layanan, gunakan peran default, atau pilih peran yang sudah ada. Untuk memilih peran yang sudah ada, pilih Gunakan peran layanan yang ada, lalu untuk Peran IAM, pilih peran yang akan digunakan.
6. Saat Anda siap untuk memulai interupsi Instans Spot, pilih Mulai interupsi.

Untuk membuat eksperimen lanjutan untuk menguji interupsi Instans Spot menggunakan konsol AWS FIS

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari panel navigasi, pilih Permintaan Spot.
3. Pilih Tindakan, Buat eksperimen lanjutan.

   AWS FIS Konsol terbuka. Untuk informasi selengkapnya, lihat Tutorial: Uji interupsi Instans Spot menggunakan AWS FIS dalam di Panduan Pengguna AWS Fault Injection Service .

Verifikasi interupsi Instans Spot

Setelah Anda memulai interupsi, berikut ini yang akan terjadi:

- Instans Spot menerima rekomendasi penyeimbangan kembali instans.
- Pemberitahuan interupsi Instans Spot dikeluarkan dua menit sebelum AWS FIS menginterupsi instans Anda.
- Setelah dua menit, Instans Spot akan diinterupsi.
- Instance Spot yang dihentikan oleh AWS FIS tetap berhenti sampai Anda memulai ulang.

Untuk memverifikasi bahwa instans diinterupsi setelah Anda memulai interupsi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari panel navigasi, buka Permintaan Spot dan Instans di tab atau jendela peramban yang terpisah.

3. Untuk Permintaan Spot, pilih permintaan Instans Spot atau permintaan Armada Spot. Status awal adalah `fulfilled`. Setelah instans diinterupsi, status berubah sebagai berikut, tergantung pada perilaku interupsi:
   - `terminate` – Status berubah menjadi `instance-terminated-by-experiment`.
   - `stop` – Status berubah menjadi `marked-for-stop-by-experiment`, kemudian `instance-stopped-by-experiment`.
4. Untuk Instans, pilih Instans Spot. Status awal adalah `Running`. Dua menit setelah Anda menerima pemberitahuan diinterupsi Instans Spot, status berubah sebagai berikut, tergantung pada perilaku interupsi:
   - `stop` – Status berubah menjadi `Stopping`, kemudian `Stopped`.
   - `terminate` – Status berubah menjadi `Shutting-down`, kemudian `Terminated`.

Kuota

Anda Akun AWS memiliki kuota default berikut untuk jumlah Instans Spot yang AWS FIS dapat mengganggu per percobaan.

Nama	Default	Dapat disesuaikan	Deskripsi
Target SpotInstances untuk aws:ec2: send-spot-instance-interruptions	Setiap Wilayah yang didukung: 5	Ya	Jumlah maksimum Instans Spot yang aws:ec2: send-spot-instance-interruptions dapat menargetkan saat Anda mengidentifikasi target menggunakan tag, per percobaan.

Anda dapat meminta penambahan kuota. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota di Panduan Pengguna Kuota Layanan.

Untuk melihat semua kuota AWS FIS, buka konsol Service Quotas. Pada panel navigasi, pilih Layanan AWS dan pilih AWS Fault Injection Service. Anda juga dapat melihat semua kuota untuk AWS Fault Injection Service di Panduan Pengguna AWS Fault Injection Service .

Pemberitahuan interupsi Instans Spot

Pemberitahuan interupsi Instans Spot adalah peringatan yang dikeluarkan dua menit sebelum Amazon EC2 menghentikan atau mengakhiri Instans Spot Anda. Jika Anda menentukan hibernasi sebagai perilaku interupsi, Anda akan menerima pemberitahuan interupsi, tetapi Anda tidak menerima peringatan dua menit karena proses hibernasi langsung dimulai.

Cara terbaik agar Anda dapat menangani interupsi Instans Spot dengan baik adalah dengan merancang aplikasi Anda agar toleran terhadap kesalahan. Untuk melakukannya, Anda dapat memanfaatkan pemberitahuan interupsi Instans Spot. Kami menyarankan Anda untuk memeriksa pemberitahuan interupsi ini setiap 5 detik.

Pemberitahuan interupsi tersedia sebagai EventBridge peristiwa dan sebagai item dalam metadata instance pada Instans Spot. Pemberitahuan interupsi dipancarkan dengan upaya yang terbaik.

Kejadian EC2 Spot Instance Interruption Warning

Saat akan menginterupsi Instans Spot Anda, Amazon EC2 memancarkan peristiwa dua menit sebelum interupsi sebenarnya (kecuali untuk hibernasi, yang mendapatkan pemberitahuan interupsi, tetapi tidak dua menit sebelumnya, karena hibernasi langsung dimulai). Acara ini dapat dideteksi oleh Amazon EventBridge. Untuk informasi selengkapnya tentang EventBridge peristiwa, lihat Panduan EventBridge Pengguna Amazon. Untuk contoh terperinci yang akan memandu Anda tentang cara membuat dan menggunakan aturan peristiwa, lihat Memanfaatkan Notifikasi Interupsi Instans Spot Amazon EC2.

Berikut ini adalah contoh peristiwa untuk interupsi Instans Spot. Nilai yang mungkin untuk `instance-action` adalah `hibernate`, `stop`, dan `terminate`.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
```

```
}
```

> **Note**
>
> Format ARN dari peristiwa interupsi Instans Spot adalah. `arn:aws:ec2:`*`availability-zone`*`:instance/`*`instance-id`* Format ini berbeda dari format ARN sumber daya EC2.

instance-action

Item `instance-action` menentukan tindakan dan perkiraan waktu, dalam UTC, kapan tindakan akan terjadi.

Jika Instans Spot Anda ditandai untuk dihentikan atau diakhiri oleh Amazon EC2, item `instance-action` akan ada di metadata instans Anda. Jika tidak, item itu tidak ada. Anda dapat mengambil Instance Metadata Service Version 2 (IMDSv2) sebagai berikut. `instance-action`

Linux

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

Contoh output berikut menunjukkan waktu saat instans ini akan dihentikan.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

Output contoh berikut menunjukkan waktu saat instans ini akan diakhiri.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Jika Amazon EC2 tidak bersiap untuk menghentikan atau mengakhiri instans, atau jika Anda sendiri mengakhiri instans, `instance-action` tidak ada dalam metadata instans dan Anda menerima kesalahan HTTP 404 saat Anda mencoba untuk mengambilnya kembali.

termination-time

`termination-time`Item menentukan perkiraan waktu dalam UTC kapan instance akan menerima sinyal shutdown.

> **Note**
>
> Item ini dipertahankan untuk kompatibilitas mundur; Anda seharusnya menggunakan `instance-action`.

Jika Instans Spot ditandai untuk dihentikan oleh Amazon EC2 (baik karena gangguan Instans Spot di mana perilaku interupsi disetel `keterminate`, atau karena pembatalan permintaan Instans Spot persisten), `termination-time` item tersebut ada dalam metadata instans Anda. Jika tidak, item itu tidak ada. Anda dapat mengambil `termination-time` menggunakan IMDSv2 sebagai berikut.

Linux

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo termination_scheduled; fi
```

Windows

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

Berikut ini adalah output contoh.

```
2015-01-05T18:02:00Z
```

Jika Amazon EC2 tidak bersiap untuk menghentikan instance (baik karena tidak ada gangguan Instans Spot atau karena perilaku interupsi Anda disetel ke `stop` atau`hibernate`), atau jika Anda

menghentikan Instans Spot sendiri, `termination-time` item tersebut tidak ada dalam metadata instans (sehingga Anda menerima kesalahan HTTP 404) atau berisi nilai yang bukan nilai waktu.

Jika Amazon EC2 gagal untuk mengakhiri instans, status permintaan diatur ke `fulfilled`. Nilai `termination-time` tetap dalam metadata instans dengan perkiraan waktu semula, yang sekarang sudah berlalu.

Menemukan Instans Spot yang diinterupsi

Saat Anda mendeskripsikan instans EC2 Anda, hasilnya menyertakan Instans Spot Anda. Siklus hidup instans dari instans Spot adalah `spot`. Status instans dari Instans Spot bisa berupa `stopped` atau `terminated`, tergantung pada perilaku interupsi yang Anda konfigurasikan. Untuk instans Spot hibernasi, status instans adalah `stopped`.

Untuk detail tambahan tentang alasan interupsi, periksa kode status permintaan Spot. Untuk informasi selengkapnya, lihat the section called “Mendapatkan status permintaan Instans Spot”.

Console

Untuk menemukan Instance Spot yang terputus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Terapkan filter berikut: Siklus hidup instans=spot.
4. Terapkan filter Status instans=berhenti atau Status instans=diakhiri tergantung pada perilaku interupsi yang Anda konfigurasikan.
5. Untuk setiap Instans Spot, di tab Detail, pada Detail instans, temukan Pesan transisi status. Kode berikut menunjukkan bahwa Instans Spot diinterupsi.
   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`

AWS CLI

Untuk menemukan Instans Spot yang terputus

Gunakan perintah describe-instance dengan opsi. `--filters` Untuk mencantumkan hanya instance IDs dalam output, sertakan `--query` opsi.

Jika perilaku interupsi adalah untuk menghentikan Instans Spot, gunakan contoh berikut:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot \
              Name=instance-state-name,Values=terminated \
              Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Jika perilaku interupsi adalah menghentikan Instans Spot, gunakan contoh berikut:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot \
              Name=instance-state-name,Values=stopped \
              Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

PowerShell

Untuk menemukan Instans Spot yang terputus

Gunakan Get-EC2Instancecmdlet.

Jika perilaku interupsi adalah untuk menghentikan Instans Spot, gunakan contoh berikut:

```
(Get-EC2Instance `
    -Filter @{Key="instance-lifecycle"; Values="spot"} `
            @{Key="instance-state-name"; Values="terminated"} `
            @{Key="state-reason-code";
 Values="Server.SpotInstanceTermination"}).Instances.InstanceId
```

Jika perilaku interupsi adalah menghentikan Instans Spot, gunakan contoh berikut:

```
(Get-EC2Instance `
    -Filter @{Key="instance-lifecycle"; Values="spot"} `
            @{Key="instance-state-name"; Values="stopped"} `
            @{Key="state-reason-code";
 Values="Server.SpotInstanceTermination"}).Instances.InstanceId
```

Menentukan apakah Amazon EC2 mengakhiri Instans Spot

Instans Spot berjalan hingga Amazon EC2 menghentikannya sebagai respons terhadap gangguan Instans Spot, atau hingga Anda menghentikannya sendiri. Untuk informasi selengkapnya, lihat the section called “Perilaku interupsi”.

Setelah Instans Spot dihentikan, Anda dapat menggunakan AWS CloudTrail untuk melihat apakah Amazon EC2 menghentikannya. Jika CloudTrail log menyertakan a`BidEvictedEvent`, ini menunjukkan bahwa Amazon EC2 menghentikan Instans Spot. Jika sebaliknya Anda melihat `TerminateInstances` peristiwa, ini menunjukkan bahwa pengguna menghentikan Instans Spot.

Atau, jika Anda ingin menerima pemberitahuan bahwa Amazon EC2 akan mengganggu Instans Spot Anda, gunakan Amazon EventBridge untuk menanggapi peristiwa Peringatan Gangguan Instans Spot EC2.

Untuk melihat BidEvictedEvent acara di CloudTrail

1. Buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pada panel navigasi, pilih Riwayat peristiwa.
3. Dari daftar filter, pilih Nama acara, lalu di bidang filter di sebelah kanan, masukkan**`BidEvictedEvent`**.
4. (Opsional) Pilih rentang waktu.
5. Jika daftar tidak kosong, pilih BidEvictedEventdari entri yang dihasilkan untuk membuka halaman detailnya. Anda dapat menemukan informasi tentang Instans Spot di panel Catatan peristiwa, termasuk ID Instans Spot. Berikut ini adalah contoh catatan acara.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "ec2.amazonaws.com"
    },
    "eventTime": "2016-08-16T22:30:00Z",
    "eventSource": "ec2.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "sourceIPAddress": "ec2.amazonaws.com",
    "eventName": "BidEvictedEvent",
    "awsRegion": "us-east-2",
    "eventID": "d27a6096-807b-4bd0-8c20-a33a83375054",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "RequestParameters": null,
    "ResponseElements": null,
    "serviceEventDetails": {
        "instanceIdSet": [
          "i-1eb2ac8eEXAMPLE"
```

```
        ]
    }
}
```

6. Jika Anda tidak menemukan entri untuk `BidEvictedEvent` acara tersebut, masukkan **`TerminateInstances`** sebagai nama acara. Untuk informasi selengkapnya tentang catatan acara`TerminateInstances`, lihatthe section called “Contoh acara Amazon EC2 API”.

Penagihan untuk Instans Spot yang diinterupsi

Ketika Instans Spot terputus, Anda dikenakan biaya misalnya dan penggunaan volume EBS, dan Anda mungkin dikenakan biaya lain, sebagai berikut.

Penggunaan instans

Siapa yang menginterupsi Instans Spot	Sistem operasi	Interupsi dalam satu jam pertama	Interupsi dalam berapa pun jam setelah satu jam pertama
Jika Anda menghentikan atau mengakhiri Instans Spot	Windows dan Linux (tidak termasuk SUSE)	Dikenai biaya untuk detik yang digunakan	Dikenai biaya untuk detik yang digunakan
	SEGAR	Dikenai biaya selama satu jam penuh meskipun Anda menggunakan sebagian jam	Dikenai biaya selama satu jam penuh yang digunakan, dan dikenai biaya untuk sebagian jam yang diinterupsi
Jika Amazon EC2 menginterupsi Instans Spot	Windows dan Linux (tidak termasuk SUSE)	Tidak dikenai biaya	Dikenai biaya untuk detik yang digunakan
	SEGAR	Tidak dikenai biaya	Dikenai biaya selama satu jam penuh yang digunakan, tetapi tidak

Siapa yang menginterupsi Instans Spot	Sistem operasi	Interupsi dalam satu jam pertama	Interupsi dalam berapa pun jam setelah satu jam pertama
			dikenai biaya untuk sebagian jam yang diinterupsi

Penggunaan volume EBS

Saat Instans Spot yang diinterupsi dihentikan, Anda hanya dikenai biaya untuk volume EBS, yang dipertahankan.

Dengan Armada EC2 dan Armada Spot, jika Anda memiliki banyak instans yang dihentikan, Anda dapat melebihi batas jumlah volume EBS untuk akun Anda.

Rekomendasi penyeimbangan ulang instans EC2

Rekomendasi penyeimbangan kembali instans EC2 adalah sinyal yang memberi tahu Anda saat Instans Spot berada pada risiko interupsi yang tinggi. Sinyal dapat tiba lebih cepat daripada pemberitahuan interupsi Instans Spot dua menit, yang memberi Anda kesempatan untuk mengelola Instans Spot secara proaktif. Anda dapat memutuskan untuk menyeimbangkan kembali beban kerja Anda ke Instans Spot baru atau lama yang tidak berisiko tinggi mengalami interupsi.

Amazon EC2 tidak selalu dapat mengirim sinyal rekomendasi penyeimbangan kembali sebelum pemberitahuan interupsi Instans Spot dua menit. Oleh karena itu, sinyal rekomendasi penyeimbangan kembali dapat tiba bersama dengan pemberitahuan interupsi dua menit.

Rekomendasi penyeimbangan ulang tersedia sebagai EventBridge peristiwa dan sebagai item dalam metadata instance pada Instans Spot. Peristiwa dipancarkan atas dasar upaya terbaik.

> **Note**
>
> Rekomendasi penyeimbangan kembali hanya didukung untuk Instans Spot yang diluncurkan setelah 5 November 2020 00:00 UTC.

Daftar Isi

- Menyeimbangkan kembali tindakan yang dapat Anda lakukan
- Pantau sinyal rekomendasi penyeimbangan kembali
- Layanan yang menggunakan sinyal rekomendasi penyeimbangan kembali

Menyeimbangkan kembali tindakan yang dapat Anda lakukan

Berikut adalah beberapa kemungkinan tindakan penyeimbangan ulang yang dapat Anda lakukan:

Pematian terkendali

Saat Anda menerima sinyal rekomendasi penyeimbangan ulang untuk Instans Spot, Anda dapat memulai prosedur pematian instans Anda, yang mungkin termasuk memastikan bahwa proses telah selesai sebelum menghentikannya. Misalnya, Anda dapat mengunggah log sistem atau aplikasi ke Amazon Simple Storage Service (Amazon S3), Anda dapat mematikan pekerja Amazon SQS, atau Anda dapat menyelesaikan penghapusan pendaftaran dari Sistem Nama Domain (DNS). Anda juga dapat menyimpan pekerjaan Anda di penyimpanan eksternal dan melanjutkannya di lain waktu.

Mencegah pekerjaan baru dijadwalkan

Saat Anda menerima sinyal rekomendasi penyeimbangan kembali untuk Instans Spot, Anda dapat mencegah pekerjaan baru dijadwalkan pada instans tersebut, sambil terus menggunakan instans tersebut hingga pekerjaan yang dijadwalkan selesai.

Luncurkan instans pengganti baru secara proaktif

Anda dapat mengonfigurasi grup Auto Scaling, Armada EC2, atau Armada Spot untuk secara otomatis meluncurkan Instans Spot pengganti ketika sinyal rekomendasi penyeimbangan kembali dipancarkan. Untuk informasi selengkapnya, lihat Menggunakan Penyeimbangan Kembali Kapasitas untuk menangani interupsi Spot Amazon EC2 di Panduan Pengguna Penskalaan Otomatis Amazon EC2, dan dalam panduan pengguna ini. Gunakan Rebalancing Kapasitas di Armada EC2 dan Armada Spot untuk mengganti Instans Spot yang berisiko

Pantau sinyal rekomendasi penyeimbangan kembali

Anda dapat memantau sinyal rekomendasi penyeimbangan kembali sehingga Anda dapat mengambil tindakan yang ditentukan di bagian sebelumnya ketika sinyal dipancarkan. Sinyal rekomendasi penyeimbangan ulang tersedia sebagai peristiwa yang dikirim ke Amazon EventBridge (sebelumnya dikenal sebagai Amazon CloudWatch Events) dan sebagai metadata instans pada Instans Spot.

Pantau sinyal rekomendasi penyeimbangan kembali:

- Gunakan Amazon EventBridge
- Gunakan metadata instans

Gunakan Amazon EventBridge

Ketika sinyal rekomendasi penyeimbangan kembali dipancarkan untuk Instans Spot, peristiwa untuk sinyal dikirim ke Amazon. EventBridge Jika EventBridge mendeteksi pola peristiwa yang cocok dengan pola yang ditentukan dalam aturan, EventBridge memanggil target (atau target) yang ditentukan dalam aturan.

Berikut adalah contoh peristiwa untuk sinyal rekomendasi penyeimbangan kembali.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Bidang berikut membentuk pola peristiwa yang ditentukan dalam aturan:

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Mengidentifikasi bahwa peristiwa itu adalah peristiwa rekomendasi penyeimbangan kembali

`"source": "aws.ec2"`

Mengidentifikasi bahwa peristiwa tersebut itu dari Amazon EC2

Buat EventBridge aturan

Anda dapat menulis EventBridge aturan dan mengotomatiskan tindakan apa yang harus diambil ketika pola acara cocok dengan aturan.

Contoh berikut membuat EventBridge aturan untuk mengirim email, pesan teks, atau pemberitahuan push seluler setiap kali Amazon EC2 memancarkan sinyal rekomendasi penyeimbangan ulang. Sinyal dipancarkan sebagai peristiwa `EC2 Instance Rebalance Recommendation`, yang memicu tindakan yang ditentukan oleh aturan.

Sebelum membuat EventBridge aturan, Anda harus membuat topik Amazon SNS untuk email, pesan teks, atau pemberitahuan push seluler.

Untuk membuat EventBridge aturan untuk acara rekomendasi penyeimbangan ulang

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Pilih Buat aturan.
3. Untuk Tentukan detail aturan, lakukan hal berikut:
   a. Masukkan Nama untuk aturan tersebut dan, secara opsional, deskripsi.

      Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus peristiwa yang sama.
   b. Untuk Bus peristiwa, pilih default. Saat layanan AWS di akun Anda membuat peristiwa, layanan tersebut akan selalu masuk ke bus peristiwa default akun.
   c. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
   d. Pilih Selanjutnya.
4. Untuk Pola peristiwa build, lakukan hal berikut ini:
   a. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.
   b. Untuk Pola peristiwa, untuk contoh ini Anda akan menentukan pola peristiwa berikut agar cocok dengan peristiwa `EC2 Instance Rebalance Recommendation`, lalu pilih Simpan.

      ```
      {
       "source": ["aws.ec2"],
       "detail-type": ["EC2 Instance Rebalance Recommendation"]
      }
      ```

      Untuk menambahkan pola peristiwa, Anda dapat menggunakan templat dengan memilih formulir pola peristiwa, atau menentukan pola Anda sendiri dengan memilih Pola kustom (editor JSON), sebagai berikut:

i. Untuk menggunakan templat untuk membuat pola peristiwa, lakukan hal berikut:

A. Pilih Formulir pola peristiwa.

B. Untuk Sumber peristiwa, pilih Layanan AWS .

C. Untuk Layanan AWS , pilih Armada Spot EC2.

D. Untuk Tipe peristiwa, pilih Rekomendasi Penyeimbangan Kembali Instans EC2.

E. Untuk menyesuaikan templat, pilih Edit pola dan buat perubahan Anda agar sesuai dengan contoh pola peristiwa.

ii. (Alternatif) Untuk menentukan pola peristiwa khusus, lakukan hal berikut:

A. Pilih Pola kustom (editor JSON).

B. Dalam kotak Pola peristiwa, tambahkan pola peristiwa untuk contoh ini.

c. Pilih Selanjutnya.

5. Untuk Pilih target, lakukan hal berikut:

a. Untuk Tipe Target, pilih Layanan AWS .

b. Untuk Memilih target, pilih topik SNS untuk mengirim email, pesan teks, atau notifikasi push seluler saat peristiwa tersebut terjadi.

c. Untuk Topik, pilih topik yang ada. Anda harus terlebih dahulu membuat topik Amazon SNS menggunakan konsol Amazon SNS. Untuk informasi selengkapnya, lihat Menggunakan Amazon SNS untuk pesan application-to-person (A2P) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

d. (Opsional) Pada Pengaturan tambahan, Anda dapat mengonfigurasi pengaturan tambahan secara opsional. Untuk informasi selengkapnya, lihat Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa (langkah 16) di Panduan EventBridge Pengguna Amazon.

e. Pilih Selanjutnya.

6. (Opsional) Untuk Tanda, Anda dapat secara opsional menetapkan satu atau beberapa tanda ke aturan, lalu pilih Berikutnya.

7. Untuk Tinjau dan buat, lakukan hal berikut:

a. Tinjau detail aturan dan modifikasi seperlunya.

b. Pilih Buat aturan.

Untuk informasi selengkapnya, lihat EventBridge aturan Amazon dan pola EventBridge peristiwa Amazon di Panduan EventBridge Pengguna Amazon

Gunakan metadata instans

Kategori metadata instans `events/recommendations/rebalance` memberikan perkiraan waktu, dalam UTC, kapan sinyal rekomendasi penyeimbangan kembali dipancarkan untuk Instans Spot.

Kami menyarankan Anda untuk memeriksa sinyal rekomendasi penyeimbangan kembali setiap 5 detik agar Anda tidak melewatkan kesempatan untuk menjalankan rekomendasi penyeimbangan kembali.

Jika Instans Spot menerima rekomendasi penyeimbangan kembali, waktu sinyal dipancarkan ada dalam metadata instans. Anda dapat mengambil waktu saat sinyal itu dipancarkan sebagai berikut.

IMDSv2

Linux

Jalankan perintah berikut dari instance Linux Anda.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/events/
recommendations/rebalance
```

Berikut ini adalah contoh output, yang menunjukkan waktu, dalam UTC, saat sinyal rekomendasi penyeimbangan kembali dipancarkan untuk Instans Spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Jika sinyal belum dipancarkan untuk instans itu, `events/recommendations/rebalance` tidak ada dan Anda akan menerima kesalahan HTTP 404 ketika Anda mencoba untuk mengambilnya kembali.

Layanan yang menggunakan sinyal rekomendasi penyeimbangan kembali

Amazon EC2 Auto Scaling, Armada EC2, dan Armada Spot menggunakan sinyal rekomendasi penyeimbangan kembali untuk memudahkan Anda mempertahankan ketersediaan beban kerja dengan secara proaktif menambah armada Anda dengan Instans Spot baru sebelum instans yang berjalan menerima pemberitahuan interupsi Instans Spot dua menit. Anda dapat meminta layanan ini untuk memantau dan secara proaktif merespons perubahan yang memengaruhi ketersediaan Instans Spot Anda. Untuk informasi selengkapnya, lihat berikut ini:

- Gunakan Penyeimbangan Kembali Kapasitas untuk menangani interupsi Amazon EC2 Spot di Panduan Pengguna Amazon EC2 Auto Scaling
- Gunakan Rebalancing Kapasitas di Armada EC2 dan Armada Spot untuk mengganti Instans Spot yang berisikodalam topik Armada EC2 dan Armada Spot di panduan pengguna ini

Skor penempatan Spot

Fitur skor penempatan Spot dapat merekomendasikan AWS Wilayah atau Zona Ketersediaan berdasarkan persyaratan kapasitas Spot Anda. Kapasitas spot berfluktuasi, dan Anda tidak dapat memastikan bahwa Anda akan selalu mendapatkan kapasitas yang Anda butuhkan. Skor penempatan Spot menunjukkan seberapa besar kemungkinan permintaan Spot akan berhasil di suatu Wilayah atau Zona Ketersediaan.

> **Note**
>
> Skor penempatan Spot tidak memberikan jaminan apa pun dalam hal kapasitas yang tersedia atau risiko interupsi. Skor penempatan Spot hanya berfungsi sebagai rekomendasi.

Kasus penggunaan

Anda dapat menggunakan fitur skor penempatan Spot untuk hal-hal berikut:

- Untuk merelokasi dan menskalakan kapasitas komputasi Spot di Wilayah yang berbeda, sesuai kebutuhan, sebagai respons terhadap peningkatan kebutuhan kapasitas atau penurunan kapasitas yang tersedia di Wilayah saat ini.
- Untuk mengidentifikasi Zona Ketersediaan yang paling optimal untuk menjalankan beban kerja Zona Ketersediaan Tunggal.
- Untuk menyimulasikan kebutuhan kapasitas Spot di masa mendatang sehingga Anda dapat memilih Wilayah yang optimal untuk perluasan beban kerja berbasis Spot Anda.
- Untuk menemukan kombinasi tipe instans yang optimal untuk memenuhi kebutuhan kapasitas Spot Anda.

Daftar Isi

- Batasan
- Biaya
- Cara kerja skor penempatan Spot
- Izin yang diperlukan untuk skor penempatan Spot
- Hitung skor penempatan Spot

Batasan

- Batas kapasitas target — Batas kapasitas target skor penempatan Spot Anda didasarkan pada penggunaan Spot terbaru Anda, sambil memperhitungkan potensi pertumbuhan penggunaan. Jika Anda tidak memiliki penggunaan Spot terbaru, kami memberi Anda batas default rendah yang selaras dengan batas permintaan Spot Anda.
- Batas konfigurasi permintaan — Kami dapat membatasi jumlah konfigurasi permintaan baru dalam jangka waktu 24 jam jika kami mendeteksi pola yang tidak terkait dengan tujuan penggunaan fitur skor penempatan Spot. Jika Anda mencapai batas, Anda dapat mencoba kembali konfigurasi permintaan yang telah Anda gunakan, tetapi Anda tidak dapat menentukan konfigurasi permintaan baru hingga periode 24 jam berikutnya.
- Jumlah minimum tipe instans — Jika Anda menentukan tipe instans, Anda harus menentukan setidaknya tiga tipe instans yang berbeda; jika tidak, Amazon EC2 akan menampilkan skor penempatan Spot rendah. Demikian pula, jika Anda menentukan atribut instans, atribut itu harus menyelesaikan setidaknya tiga tipe instans yang berbeda. Tipe instans dianggap berbeda jika mereka memiliki nama yang berbeda. Misalnya, m5.8xlarge, m5a.8xlarge, dan m5.12xlarge, semua dianggap berbeda.

Biaya

Tidak ada biaya tambahan karena menggunakan fitur skor penempatan Spot.

Cara kerja skor penempatan Spot

Saat menggunakan fitur skor penempatan Spot, pertama-tama tentukan kebutuhan komputasi untuk Instans Spot Anda, lalu Amazon EC2 akan menampilkan skor 10 Wilayah teratas atau Zona Ketersediaan tempat permintaan Spot Anda kemungkinan berhasil. Setiap Wilayah atau Zona Ketersediaan dinilai pada skala 1 hingga 10, dengan 10 menunjukkan bahwa permintaan Spot Anda sangat mungkin berhasil, dan 1 menunjukkan bahwa permintaan Spot Anda tidak mungkin berhasil.

Untuk menggunakan fitur skor penempatan Spot, ikuti langkah-langkah berikut:

- Langkah 1: Tentukan kebutuhan Spot Anda
- Langkah 2: Filter respons skor penempatan Spot
- Langkah 3: Tinjau rekomendasi
- Langkah 4: Gunakan rekomendasi

Langkah 1: Tentukan kebutuhan Spot Anda

Pertama, tentukan kapasitas Spot target yang Anda inginkan dan kebutuhan komputasi Anda, sebagai berikut:

1. Tentukan kapasitas Spot target, dan unit kapasitas target opsional.

   Anda dapat menentukan kapasitas Spot target yang Anda inginkan dalam hal jumlah instance atau vCPUs, atau dalam hal jumlah memori di MiB. Untuk menentukan kapasitas target dalam jumlah v CPUs atau jumlah memori, Anda harus menentukan unit kapasitas target sebagai `vcpu` atau`memory-mib`. Jika tidak, default ditentukan ke jumlah instans.

   Dengan menentukan kapasitas target Anda dalam hal jumlah v CPUs atau jumlah memori, Anda dapat menggunakan unit ini saat menghitung total kapasitas. Misalnya, jika Anda ingin menggunakan campuran instance dengan ukuran berbeda, Anda dapat menentukan kapasitas target sebagai jumlah total vCPUs. Fitur skor penempatan Spot kemudian mempertimbangkan setiap jenis instance dalam permintaan dengan jumlah vCPUs, dan menghitung jumlah total v CPUs daripada jumlah total instance saat menjumlahkan kapasitas target.

   Misalnya, Anda menentukan total kapasitas target 30 vCPUs, dan daftar tipe instans Anda terdiri dari c5.xlarge (4 vCPUs), m5.2xlarge (8 v), dan r5.large (2 vCPUs). CPUs Untuk mencapai total 30 vCPUs, Anda bisa mendapatkan campuran 2 c5.xlarge (2* 4 v), 2 m5.2xlarge (2* 8 vCPUs), dan 3 r5.large (3* 2 v). CPUs CPUs
2. Tentukan tipe instans atau atribut instans.

   Anda dapat menentukan tipe instans yang akan digunakan, atau Anda dapat menentukan atribut instans yang Anda perlukan untuk kebutuhan komputasi, lalu biarkan Amazon EC2 mengidentifikasi tipe instans yang memiliki atribut tersebut. Pemilihan ini dikenal sebagai pemilihan tipe instans berbasis atribut.

   Anda tidak dapat menentukan tipe instans sekaligus atribut instans dalam permintaan skor penempatan Spot yang sama.

   Jika Anda menentukan tipe instans, Anda harus menentukan setidaknya tiga tipe instans yang berbeda, jika tidak, Amazon EC2 akan mengembalikan skor penempatan Spot rendah. Demikian pula, jika Anda menentukan atribut instans, atribut itu harus menyelesaikan setidaknya tiga tipe instans yang berbeda.

Untuk contoh berbagai cara menentukan kebutuhan Spot Anda, lihat Contoh konfigurasi.

Langkah 2: Filter respons skor penempatan Spot

Amazon EC2 menghitung skor penempatan Spot untuk setiap Wilayah atau Zona Ketersediaan, dan menampilkan 10 Wilayah teratas atau 10 Zona Ketersediaan teratas di mana permintaan Spot Anda kemungkinan akan berhasil. Defaultnya adalah menampilkan daftar Wilayah dengan skornya. Jika berencana untuk meluncurkan semua kapasitas Spot Anda ke dalam satu Zona Ketersediaan, lebih baik Anda meminta daftar Zona Ketersediaan dengan skornya.

Anda dapat menentukan filter Wilayah untuk mempersempit Wilayah yang akan ditampilkan dalam respons.

Anda dapat menggabungkan filter Wilayah dan permintaan Zona Ketersediaan dengan skornya. Dengan cara ini, Zona Ketersediaan dengan skornya dibatasi untuk Wilayah yang telah Anda filter. Untuk menemukan Zona Ketersediaan dengan skor tertinggi di suatu Wilayah, tentukan hanya Wilayah tersebut, dan responsnya akan menampilkan daftar skor dari semua Zona Ketersediaan di Wilayah tersebut.

Langkah 3: Tinjau rekomendasi

Skor penempatan Spot untuk setiap Wilayah atau Zona Ketersediaan dihitung berdasarkan kapasitas target, komposisi tipe instans, tren penggunaan Spot historis dan saat ini, serta waktu permintaan. Karena kapasitas Spot terus berfluktuasi, permintaan skor penempatan Spot yang sama dapat menghasilkan skor yang berbeda ketika dihitung pada waktu yang berbeda.

Wilayah dan Zona Ketersediaan diberi skor pada skala 1 hingga 10. Skor 10 menunjukkan bahwa permintaan Spot Anda sangat mungkin—tetapi tidak dijamin—akan berhasil. Skor 1 menunjukkan bahwa permintaan Spot Anda tidak mungkin berhasil. Skor yang sama mungkin ditampilkan untuk Wilayah atau Zona Ketersediaan yang berbeda.

Jika skor rendah ditampilkan, Anda dapat mengedit kebutuhan komputasi Anda dan menghitung ulang skor. Anda juga dapat meminta rekomendasi skor penempatan Spot untuk kebutuhan komputasi yang sama pada waktu yang berbeda dalam sehari.

Langkah 4: Gunakan rekomendasi

Skor penempatan Spot hanya relevan jika permintaan Spot Anda memiliki konfigurasi yang persis sama dengan konfigurasi skor penempatan Spot (kapasitas target, unit kapasitas target, dan tipe instans atau atribut instans), dan dikonfigurasi untuk menggunakan strategi alokasi `capacity-optimized`. Jika tidak, kemungkinan mendapatkan kapasitas Spot yang tersedia tidak akan selaras dengan skor.

Meskipun skor penempatan Spot berfungsi sebagai pedoman, dan tidak ada skor yang menjamin bahwa permintaan Spot Anda akan terpenuhi sepenuhnya atau sebagian, Anda dapat menggunakan informasi berikut untuk mendapatkan hasil terbaik:

- Gunakan konfigurasi yang sama — Skor penempatan Spot hanya relevan jika konfigurasi permintaan Spot (kapasitas target, unit kapasitas target, dan tipe instans atau atribut instans) di grup Auto Scaling, Armada EC2, atau Armada Spot Anda sama dengan yang Anda masukkan untuk mendapatkan skor penempatan Spot.

  Jika Anda menggunakan pemilihan tipe instans berdasarkan atribut dalam permintaan skor penempatan Spot, Anda dapat menggunakan pemilihan tipe instans berdasarkan atribut untuk mengonfigurasi grup Auto Scaling, Armada EC2, atau Armada Spot. Untuk informasi selengkapnya, lihat Membuat grup instance campuran menggunakan pemilihan tipe instans berbasis atribut dan. Tentukan atribut untuk pemilihan tipe contoh untuk Armada EC2 atau Armada Spot

  > **Note**
  >
  > Jika Anda menentukan kapasitas target berdasarkan jumlah vCPU atau jumlah memori, dan Anda menentukan tipe instans dalam konfigurasi skor penempatan Spot, perhatikan bahwa saat ini Anda tidak dapat membuat konfigurasi ini di grup Auto Scaling, Armada EC2, atau Armada Spot. Namun, Anda harus secara manual mengatur pembobotan instans dengan menggunakan parameter `WeightedCapacity`.

- Gunakan strategi alokasi **`capacity-optimized`** — Skor berapa pun mengasumsikan bahwa permintaan armada Anda akan dikonfigurasi untuk menggunakan semua Zona Ketersediaan (untuk meminta kapasitas di seluruh Wilayah) atau satu Zona Ketersediaan (jika meminta kapasitas dalam satu Zona Ketersediaan) dan strategi alokasi Spot `capacity-optimized` untuk permintaan Anda agar kapasitas Spot berhasil. Jika Anda menggunakan strategi alokasi lain, seperti `lowest-price`, kemungkinan mendapatkan kapasitas Spot yang tersedia tidak akan selaras dengan skor.
- Segera bertindak berdasarkan skor — Rekomendasi skor penempatan Spot mencerminkan kapasitas Spot yang tersedia pada saat permintaan, dan konfigurasi yang sama dapat menghasilkan skor yang berbeda bila dihitung pada waktu yang berbeda karena fluktuasi kapasitas Spot. Meskipun skor 10 berarti permintaan kapasitas Spot Anda sangat mungkin—tetapi tidak dijamin—berhasil, untuk hasil terbaik kami sarankan Anda segera bertindak berdasarkan skor.

Kami juga menyarankan Anda untuk mendapatkan skor baru setiap kali Anda mencoba permintaan kapasitas.

Izin yang diperlukan untuk skor penempatan Spot

Secara default, identitas IAM (pengguna, peran, atau grup) tidak memiliki izin untuk digunakan. the section called “Skor penempatan Spot” Untuk mengizinkan identitas IAM menggunakan skor penempatan Spot, Anda harus membuat kebijakan IAM yang memberikan izin untuk menggunakan tindakan EC2 API. `ec2:GetSpotPlacementScores` Anda kemudian lampirkan kebijakan ke identitas IAM yang memerlukan izin ini.

Berikut ini adalah contoh kebijakan IAM yang memberikan izin untuk menggunakan tindakan EC2 API `ec2:GetSpotPlacementScores`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Untuk informasi tentang pembuatan kebijakan IAM, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Pengguna yang dikelola di IAM melalui penyedia identitas:

Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Hitung skor penempatan Spot

Anda dapat menghitung skor penempatan Spot berdasarkan kapasitas target dan persyaratan komputasi. Untuk informasi selengkapnya, lihat the section called “Cara kerja skor penempatan Spot”.

Izin yang diperlukan

Pastikan Anda memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat the section called “Izin yang diperlukan”.

Opsi

- Hitung menggunakan atribut instance
- Hitung menggunakan tipe instance
- Hitung menggunakan AWS CLI

Mencari solusi otomatis? Alih-alih mengikuti langkah-langkah manual dalam panduan pengguna ini, Anda dapat membuat dasbor pelacak skor penempatan Spot yang secara otomatis menangkap dan menyimpan skor di Amazon. CloudWatch Untuk informasi selengkapnya, lihat Panduan untuk Membangun Dasbor Pelacak Skor Penempatan Spot di AWS.

Hitung menggunakan atribut instance

Untuk menghitung skor penempatan Spot dengan menentukan atribut instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.

3. Pilih panah bawah di sebelah Minta Instans Spot dan pilih Hitung Skor Penempatan Spot.
4. Pilih Masukkan persyaratan.
5. Untuk kapasitas Target, masukkan kapasitas yang Anda inginkan dalam hal jumlah instance atau v CPUs, atau jumlah memori (MiB).
6. Untuk Persyaratan tipe instans, untuk menentukan kebutuhan komputasi Anda dan agar Amazon EC2 dapat mengidentifikasi tipe instans yang optimal untuk kebutuhan ini, pilih Tentukan atribut instans yang sesuai dengan kebutuhan komputasi Anda.
7. Untuk v CPUs, masukkan jumlah minimum dan maksimum yang diinginkan vCPUs. Untuk menentukan tidak ada batas, pilih No minimum, No maximum, atau keduanya.
8. Untuk Memori (GiB), masukkan jumlah memori minimum dan maksimum yang diinginkan. Untuk menentukan tanpa batasan, pilih Tanpa minimum, Tanpa maksimum, atau keduanya.
9. Untuk Arsitektur CPU, pilih arsitektur instans yang diperlukan.
10. (Opsional) Untuk Atribut instans tambahan, Anda dapat secara opsional menentukan satu atau lebih atribut untuk mengekspresikan kebutuhan komputasi Anda secara lebih mendetail. Setiap atribut tambahan menambahkan batasan lebih lanjut ke permintaan Anda. Anda dapat menghilangkan atribut tambahan; ketika dihilangkan, nilai default digunakan. Untuk deskripsi setiap atribut dan nilai defaultnya, lihat get-spot-placement-scores.
11. (Opsional) Untuk menampilkan tipe instans dengan atribut tertentu, perluas Pratinjau tipe instans yang cocok. Untuk mengecualikan tipe instans agar tidak digunakan dalam evaluasi penempatan Anda, pilih instans, lalu pilih Kecualikan tipe instans yang dipilih.
12. Pilih Muat skor penempatan, dan tinjau hasilnya.
13. (Opsional) Untuk menampilkan skor penempatan Spot untuk Wilayah tertentu, di Wilayah untuk dievaluasi, pilih Wilayah yang akan dievaluasi, lalu pilih Hitung skor penempatan.
14. (Opsional) Untuk menampilkan skor penempatan Spot untuk Availability Zones di Region yang ditampilkan, pilih kotak centang Berikan skor penempatan per Availability Zone. Daftar Zona Ketersediaan yang dinilai akan bermanfaat jika Anda berencana untuk meluncurkan semua kapasitas Spot Anda ke dalam satu Zona Ketersediaan.
15. (Opsional) Untuk mengedit kebutuhan komputasi Anda dan mendapatkan skor penempatan baru, pilih Edit, buat penyesuaian yang diperlukan, lalu pilih Hitung skor penempatan.

Hitung menggunakan tipe instance

Untuk menghitung skor penempatan Spot dengan menentukan tipe instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih panah bawah di sebelah Minta Instans Spot dan pilih Hitung Skor Penempatan Spot.
4. Pilih Masukkan persyaratan.
5. Untuk kapasitas Target, masukkan kapasitas yang Anda inginkan dalam hal jumlah instance atau v CPUs, atau jumlah memori (MiB).
6. Untuk Persyaratan tipe instans, untuk menentukan tipe instans yang akan digunakan, pilih Pilih tipe instans secara manual.
7. Pilih Pilih tipe instans, pilih tipe instans yang akan digunakan, lalu pilih Pilih. Untuk menemukan tipe instans dengan cepat, Anda dapat menggunakan bilah filter untuk memfilter tipe instans berdasarkan properti yang berbeda.
8. Pilih Muat skor penempatan, dan tinjau hasilnya.
9. (Opsional) Untuk menampilkan skor penempatan Spot untuk Wilayah tertentu, di Wilayah untuk dievaluasi, pilih Wilayah yang akan dievaluasi, lalu pilih Hitung skor penempatan.
10. (Opsional) Untuk menampilkan skor penempatan Spot untuk Availability Zones di Region yang ditampilkan, pilih kotak centang Berikan skor penempatan per Availability Zone. Daftar Zona Ketersediaan yang dinilai akan bermanfaat jika Anda berencana untuk meluncurkan semua kapasitas Spot Anda ke dalam satu Zona Ketersediaan.
11. (Opsional) Untuk mengedit daftar tipe instans dan mendapatkan skor penempatan baru, pilih Edit, buat penyesuaian yang diperlukan, lalu pilih Hitung skor penempatan.

Hitung menggunakan AWS CLI

Hitung skor penempatan Spot

1. (Opsional) Untuk menghasilkan semua parameter yang mungkin yang dapat ditentukan untuk konfigurasi skor penempatan Spot, gunakan get-spot-placement-scoresperintah dan `--generate-cli-skeleton` parameter.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
```

```
    --generate-cli-skeleton
```

Berikut ini adalah output contoh.

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
```

```
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
```

```
}
```

2. Buat file konfigurasi JSON menggunakan output dari langkah sebelumnya, dan konfigurasikan sebagai berikut:

   a. Untuk`TargetCapacity`, masukkan kapasitas Spot yang Anda inginkan dalam hal jumlah instans atau vCPUs, atau jumlah memori (MiB).

   b. Untuk `TargetCapacityUnitType`, masukkan unit untuk kapasitas target. Jika Anda menghilangkan parameter ini, defaultnya adalah `units`.

      Nilai yang valid: `units` (yang diterjemahkan ke jumlah contoh) | `vcpu` | `memory-mib`

   c. Untuk `SingleAvailabilityZone`, tentukan `true` untuk respons yang menampilkan daftar Zona Ketersediaan dengan skornya. Daftar Zona Ketersediaan yang dinilai akan bermanfaat jika Anda berencana untuk meluncurkan semua kapasitas Spot Anda ke dalam satu Zona Ketersediaan. Jika Anda menghilangkan parameter ini, parameter defaultnya adalah `false`, dan respons akan menampilkan daftar Wilayah dengan skornya.

   d. (Opsional) Untuk `RegionNames`, tentukan Wilayah yang akan digunakan sebagai filter. Anda harus menentukan kode Wilayah, misalnya, `us-east-1`.

      Dengan filter Wilayah, respons hanya menampilkan Wilayah yang Anda tentukan. Jika Anda menentukan `true` untuk `SingleAvailabilityZone`, respons hanya menampilkan Zona Ketersediaan di Wilayah yang ditentukan.

   e. Anda dapat memasukkan salah satu `InstanceTypes` atau `InstanceRequirements`, tetapi tidak keduanya dalam konfigurasi yang sama.

      Tentukan salah satu dari berikut ini dalam konfigurasi JSON Anda:

      - Untuk menentukan daftar tipe instans, tentukan tipe instans dalam parameter `InstanceTypes`. Tentukan setidaknya tiga tipe instans yang berbeda. Jika Anda hanya menentukan satu atau dua tipe instans, skor penempatan Spot menampilkan skor rendah. Untuk daftar tipe instans, lihat Tipe Instans Amazon EC2.
      - Untuk menentukan atribut instans sehingga Amazon EC2 akan mengidentifikasi tipe instans yang cocok dengan atribut tersebut, tentukan atribut yang terletak di struktur `InstanceRequirements`.

        Anda harus memberikan nilai untuk `VCpuCount`, `MemoryMiB`, dan `CpuManufacturers`. Anda dapat menghilangkan atribut lainnya; saat dihilangkan, nilai default digunakan. Untuk deskripsi setiap atribut dan nilai defaultnya, lihat get-spot-placement-scores.

Untuk contoh konfigurasi, lihat Contoh konfigurasi.

3. Untuk mendapatkan skor penempatan Spot untuk persyaratan yang Anda tentukan dalam file JSON, gunakan get-spot-placement-scoresperintah, dan tentukan nama dan jalur ke file JSON Anda dengan menggunakan parameter. `--cli-input-json`

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Contoh keluaran jika `SingleAvailabilityZone` disetel ke `true` — daftar Skor Availability Zones dikembalikan.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1",
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3",
        "Score": 6
    },
   ...
```

Contoh konfigurasi

Saat menggunakan AWS CLI, Anda dapat menggunakan contoh konfigurasi berikut.

Contoh konfigurasi

- Contoh: Tentukan tipe instans dan kapasitas target
- Contoh: Tentukan tipe instans, dan kapasitas target dalam hal memori
- Contoh: Tentukan atribut untuk pemilihan tipe instans berdasarkan atribut
- Contoh: Tentukan atribut untuk pemilihan tipe instans berdasarkan atribut dan tampilkan daftar Zona Ketersediaan dengan skornya

Contoh: Tentukan tipe instans dan kapasitas target

Contoh konfigurasi berikut menentukan tiga tipe instans yang berbeda dan kapasitas Spot target adalah 500 Instans Spot.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

Contoh: Tentukan tipe instans, dan kapasitas target dalam hal memori

Contoh konfigurasi berikut menentukan tiga tipe instans yang berbeda dan kapasitas Spot target 500.000 MiB memori, di mana jumlah Instans Spot yang akan diluncurkan harus menyediakan total 500.000 MiB memori.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Contoh: Tentukan atribut untuk pemilihan tipe instans berdasarkan atribut

Contoh konfigurasi berikut dikonfigurasi untuk pemilihan tipe instans berdasarkan atribut, dan diikuti dengan penjelasan teks tentang contoh konfigurasi.

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Untuk menggunakan pemilihan instans berdasarkan atribut, Anda harus menyertakan struktur `InstanceRequirementsWithMetadata` dalam konfigurasi Anda, dan menentukan atribut yang diinginkan untuk Instans Spot.

Pada contoh sebelumnya, atribut instans yang diperlukan ditentukan berikut ini:

- `ArchitectureTypes` — Tipe arsitektur dari tipe instans harus `arm64`.
- `VirtualizationTypes` — Tipe virtualisasi dari tipe instans harus `hvm`.
- `VCpuCount`— Jenis instance harus memiliki minimal 1 dan maksimal 12 vCPUs.
- `MemoryMiB` — Tipe instans harus memiliki memori minimal 512 MiB. Dengan menghilangkan parameter `Max`, Anda menunjukkan bahwa tidak ada batas maksimum.

Perhatikan bahwa ada beberapa atribut opsional lain yang dapat Anda tentukan. Untuk daftar atribut, lihat get-spot-placement-scores.

`TargetCapacityUnitType`

Parameter `TargetCapacityUnitType` menentukan unit untuk kapasitas target. Dalam contoh, kapasitas target adalah `5000` dan tipe unit kapasitas target adalah`vcpu`, yang bersama-sama menentukan kapasitas target yang diinginkan 5000 vCPUs, di mana jumlah Instans Spot yang akan diluncurkan harus memberikan total 5000 vCPUs.

Contoh: Tentukan atribut untuk pemilihan tipe instans berdasarkan atribut dan tampilkan daftar Zona Ketersediaan dengan skornya

Contoh konfigurasi berikut dikonfigurasi untuk pemilihan tipe instans berdasarkan atribut. Dengan menentukan `"SingleAvailabilityZone": true`, respons akan menampilkan daftar Zona Ketersediaan dengan skornya.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Lacak biaya Instans Spot Anda menggunakan umpan data Instans Spot

Untuk membantu Anda memahami biaya untuk Instans Spot Anda, Amazon EC2 menyediakan umpan data yang menjelaskan penggunaan dan harga Instans Spot Anda. Umpan data ini dikirim ke bucket Amazon S3 yang Anda tentukan saat Anda berlangganan umpan data.

File umpan data tiba di bucket Anda biasanya sekali dalam satu jam. Jika Anda tidak menjalankan Instans Spot selama jam tertentu, Anda tidak menerima file data feed untuk jam itu.

Setiap jam penggunaan Instans Spot biasanya tercakup dalam satu file data. File-file ini dikompresi (gzip) sebelum dikirim ke bucket Anda. Amazon EC2 dapat menulis banyak file selama jam

penggunaan tertentu di mana file berukuran besar (misalnya, ketika konten file untuk satu jam melebihi 50 MB sebelum kompresi).

> **Note**
>
> Anda hanya dapat membuat satu feed data Instance Spot per Akun AWS.

Umpan data Instans Spot didukung di semua AWS Wilayah kecuali China (Beijing), Tiongkok (Ningxia) AWS GovCloud , (AS), dan Wilayah yang dinonaktifkan secara default.

Daftar Isi

- Nama dan format file umpan data
- Persyaratan bucket Amazon S3
- Berlangganan ke umpan data Instans Spot Anda
- Melihat data di umpan data Anda
- Hapus umpan data Instans Spot Anda

Nama dan format file umpan data

Nama file feed data Instans Spot menggunakan format berikut (dengan tanggal dan jam dalam UTC):

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Misalnya, jika nama bucket Anda adalah **amzn-s3-demo-bucket** dan prefiks Anda adalah **my-prefix**, nama file Anda mirip dengan yang berikut ini:

```
amzn-s3-demo-bucket.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Untuk informasi selengkapnya tentang nama bucket, lihat Aturan penamaan bucket di Panduan Pengguna Amazon S3.

File data feed instans Spot dibatasi tab. Setiap baris dalam file data sesuai dengan satu jam instans dan berisi bidang yang tercantum dalam tabel berikut.

Bidang	Deskripsi
`Timestamp`	Stempel waktu yang digunakan untuk menentukan harga yang dikenakan untuk penggunaan instans ini.
`UsageType`	Tipe penggunaan dan tipe instans yang dikenai biaya. Untuk Instans Spot, `m1.small` bidang ini diatur ke `SpotUsage` . Untuk semua tipe instans lainnya, bidang ini diatur ke `SpotUsage:` {instance-type}. Sebagai conto,.`SpotUsage:c1.medium`
`Operation`	Produk yang ditagihkan. Untuk Instans Spot Linux, bidang ini diatur ke `RunInstances` . Untuk Instans Spot Windows, bidang ini diatur ke `RunInstances:0002` . Penggunaan spot dikelompokkan menurut Zona Ketersediaan.
`InstanceID`	ID Instans Spot yang menghasilkan penggunaan instans ini.
`MyBidID`	ID untuk permintaan Instans Spot yang menghasilkan penggunaan instans ini.
`MyMaxPrice`	Harga maksimum yang ditentukan untuk permintaan Spot ini.
`MarketPrice`	Harga Spot pada waktu yang ditentukan di bidang `Timestamp` .
`Charge`	Harga yang dikenakan untuk penggunaan instans ini.
`Version`	Versi umpan data. Versi yang memungkinkan adalah versi 1.0.

Persyaratan bucket Amazon S3

Saat Anda berlangganan umpan data, Anda harus menentukan bucket Amazon S3 untuk menyimpan file umpan data tersebut.

Sebelum Anda memilih bucket Amazon S3 untuk umpan data, pertimbangkan hal berikut:

- Anda harus memiliki izin FULL_CONTROL ke bucket. Jika Anda adalah pemilik bucket, Anda memiliki izin ini secara default. Jika tidak, pemilik ember harus memberikan izin Akun AWS ini kepada Anda.
- Saat Anda berlangganan umpan data, izin ini digunakan untuk memperbarui bucket ACL untuk memberikan izin akun FULL_CONTROL umpan AWS data. Akun umpan AWS data menulis file umpan data ke bucket. Jika akun Anda tidak memiliki izin yang diperlukan, file data feed tidak dapat ditulis ke bucket. Untuk informasi selengkapnya, lihat Log yang dikirim ke Amazon S3 di Panduan Pengguna Amazon CloudWatch Logs.

  Jika Anda memperbarui ACL dan menghapus izin untuk akun umpan AWS data, file umpan data tidak dapat ditulis ke bucket. Anda harus berlangganan kembali umpan data untuk menerima file data umpan.
- Setiap file umpan data memiliki ACL-nya sendiri (terpisah dari ACL untuk bucket). Pemilik bucket memiliki izin FULL_CONTROL ke file data. Akun umpan AWS data memiliki izin baca dan tulis.
- Jika Anda menghapus langganan umpan data, Amazon EC2 tidak menghapus izin baca dan tulis untuk akun umpan AWS data di bucket atau file data. Anda harus menghapus izin ini sendiri.
- Jika Anda mengenkripsi bucket Amazon S3 menggunakan enkripsi sisi server dengan AWS KMS kunci yang disimpan AWS Key Management Service di (SSE-KMS), Anda harus menggunakan kunci yang dikelola pelanggan. Untuk informasi selengkapnya, lihat enkripsi sisi server bucket Amazon S3 di Panduan Pengguna Amazon Logs. CloudWatch

Berlangganan ke umpan data Instans Spot Anda

Anda dapat berlangganan feed data Instans Spot kapan saja. Anda tidak dapat menyelesaikan tugas ini menggunakan konsol Amazon EC2.

Jika Anda mendapatkan kesalahan karena bucket tidak memiliki izin yang cukup, lihat artikel berikut untuk informasi pemecahan masalah: Memecahkan masalah umpan data untuk Instans Spot.

AWS CLI

Untuk berlangganan umpan data Anda

Gunakan perintah create-spot-datafeed-subscription.

Untuk menentukan bucket dengan awalan, gunakan contoh berikut:

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket \
```

```
    --prefix my-prefix
```

Untuk menentukan bucket tanpa awalan, gunakan contoh berikut:

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket
```

PowerShell

Untuk berlangganan umpan data Anda

Gunakan New-EC2SpotDatafeedSubscriptioncmdlet.

Untuk menentukan bucket dengan awalan, gunakan contoh berikut:

```
New-EC2SpotDatafeedSubscription `
    -Bucket amzn-s3-demo-bucket `
    -Prefix my-prefix
```

Untuk menentukan bucket tanpa awalan, gunakan contoh berikut:

```
New-EC2SpotDatafeedSubscription `
    -Bucket amzn-s3-demo-bucket
```

Melihat data di umpan data Anda

Di Konsol Manajemen AWS, terbuka AWS CloudShell. Gunakan perintah s3 sync berikut untuk mendapatkan file.gz dari bucket S3 untuk umpan data Anda dan simpan di folder yang Anda tentukan.

```
aws s3 sync s3://amzn-s3-demo-bucket ./data-feed
```

Untuk menampilkan isi file .gz, ubah ke folder tempat Anda menyimpan konten bucket S3.

```
cd data-feed
```

Gunakan perintah ls untuk melihat nama-nama file. Gunakan perintah zcat dengan nama file untuk menampilkan konten file terkompresi. Hal berikut menunjukkan contoh perintah.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

Berikut ini adalah output contoh.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Hapus umpan data Instans Spot Anda

Setelah selesai dengan umpan data Spot Instance, Anda dapat menghapusnya.

AWS CLI

Untuk menghapus umpan data Anda

Gunakan perintah delete-spot-datafeed-subscription.

```
aws ec2 delete-spot-datafeed-subscription
```

PowerShell

Untuk menghapus umpan data Anda

Gunakan Remove-EC2SpotDatafeedSubscriptioncmdlet.

```
Remove-EC2SpotDatafeedSubscription
```

Peran tertaut layanan untuk permintaan Instans Spot

Amazon EC2 menggunakan peran tertaut layanan untuk izin yang diperlukan untuk memanggil layanan AWS lain atas nama Anda. Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke sebuah. Layanan AWS Peran terkait layanan menyediakan cara aman untuk mendelegasikan izin Layanan AWS karena hanya layanan tertaut yang dapat mengambil peran terkait layanan. Untuk informasi selengkapnya, lihat Peran terkait layanan di Panduan Pengguna IAM.

Amazon EC2 menggunakan peran terkait layanan bernama AWSServiceRoleForEC2Spot untuk meluncurkan dan mengelola Instans Spot atas nama Anda.

Izin diberikan oleh AWSServiceRoleForEC2Spot

Amazon EC2 menggunakan AWSServiceRoleForEC2Spot untuk menyelesaikan tindakan berikut:

- `ec2:DescribeInstances` – Menjelaskan Instans Spot
- `ec2:StopInstances` – Menghentikan Instans Spot
- `ec2:StartInstances` – Memulai Instans Spot

Membuat peran tertaut layanan

Dalam sebagian besar situasi, Anda tidak perlu membuat peran tertaut layanan secara manual. Amazon EC2 membuat peran terkait layanan AWSServiceRoleForEC2Spot saat pertama kali Anda meminta Instans Spot menggunakan konsol.

Jika Anda memiliki permintaan Instans Spot aktif sebelum Oktober 2017, saat Amazon EC2 mulai mendukung peran terkait layanan ini, Amazon EC2 membuat peran Spot di AWSService RoleFor EC2 akun Anda. AWS Untuk informasi selengkapnya, lihat Peran Baru Muncul di Akun Saya dalam Panduan Pengguna IAM.

Jika Anda menggunakan AWS CLI atau API untuk meminta Instance Spot, Anda harus terlebih dahulu memastikan bahwa peran ini ada.

Untuk membuat AWSServiceRoleForEC2Spot menggunakan konsol

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran.
3. Pilih Buat peran.
4. Di halaman Pilih tipe entitas tepercaya, pilih EC2, EC2 - Instans Spot, Berikutnya: Izin.
5. Di halaman berikutnya, pilih Berikutnya: Tinjau.
6. Di halaman Tinjau, pilih Buat peran.

Untuk membuat AWSServiceRoleForEC2Spot menggunakan AWS CLI

Gunakan perintah create-service-linked-role sebagai berikut.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Jika Anda tidak perlu lagi menggunakan Instans Spot, sebaiknya hapus peran AWSServiceRoleForEC2Spot. Setelah peran ini dihapus dari akun Anda, Amazon EC2 akan membuat peran lagi jika Anda meminta Instans Spot.

Berikan akses ke kunci terkelola pelanggan untuk digunakan dengan snapshot terenkripsi AMIs dan EBS

Jika Anda menentukan AMI terenkripsi atau snapshot Amazon EBS terenkripsi untuk Instans Spot Anda dan Anda menggunakan kunci yang dikelola pelanggan untuk enkripsi, Anda harus memberikan AWSService RoleFor EC2 izin peran Spot untuk menggunakan kunci yang dikelola pelanggan sehingga Amazon EC2 dapat meluncurkan Instans Spot atas nama Anda. Untuk melakukannya, Anda harus menambahkan pemberian izin ke kunci yang dikelola pelanggan, seperti yang ditunjukkan dalam prosedur berikut.

Ketika memberikan izin, pemberian izin merupakan alternatif dari kebijakan kunci. Untuk informasi selengkapnya, lihat Menggunakan Pemberian Izin dan Menggunakan Kebijakan Kunci di AWS KMS dalam Panduan Developer AWS Key Management Service .

Untuk memberikan izin peran AWSServiceRoleForEC2Spot untuk menggunakan kunci terkelola pelanggan

- Gunakan perintah create-grant untuk menambahkan hibah ke kunci yang dikelola pelanggan dan untuk menentukan prinsipal (peran terkait layanan AWSServiceRoleForEC2Spot) yang diberi izin untuk melakukan operasi yang diizinkan hibah. Kunci yang dikelola pelanggan ditentukan oleh parameter `key-id` dan ARN kunci yang dikelola pelanggan. Prinsipal ditentukan oleh `grantee-principal` parameter dan ARN dari peran terkait layanan AWSServiceRoleForEC2Spot.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spot.amazonaws.com/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Kuota Instans Spot

Ada kuota untuk jumlah Instans Spot yang berjalan dan permintaan Instans Spot yang tertunda per Akun AWS per Wilayah. Setelah permintaan Instans Spot tertunda terpenuhi, permintaan tidak lagi dihitung terhadap kuota karena instans yang sedang berjalan dihitung terhadap kuota.

Kuota Instans Spot dikelola berdasarkan jumlah unit pemrosesan pusat virtual (vCPUs) yang digunakan oleh Instans Spot yang sedang berjalan atau akan digunakan sambil menunggu pemenuhan permintaan Instans Spot terbuka. Jika Anda menghentikan Instans Spot tetapi tidak membatalkan permintaan Instans Spot, permintaan tersebut diperhitungkan dalam kuota vCPU Instans Spot Anda hingga Amazon EC2 mendeteksi pengakhiran Instans Spot dan menutup permintaan.

Kami menyediakan jenis kuota berikut untuk Instans Spot.

Nama	Default	Dapat disesuaikan
Semua Permintaan Instans Spot DL	0	Ya
Semua Permintaan Instans F Spot	0	Ya
Semua Permintaan Instans Spot G dan VT	0	Ya
Semua Permintaan Instans Spot Inf	0	Ya
Semua Permintaan Instans Spot P	0	Ya
Semua Permintaan Instans Spot Standar (A, C, D, H, I, M, R, T, Z)	5	Ya
Semua Permintaan Instans Spot Trn	0	Ya
Semua Permintaan Instans Spot X	0	Ya

Meskipun Amazon EC2 secara otomatis menyesuaikan kuota Instans Spot berdasarkan penggunaan, Anda dapat meminta peningkatan kuota jika perlu. Misalnya, jika Anda ingin meluncurkan lebih banyak Instans Spot daripada yang diizinkan kuota Anda saat ini, Anda dapat meminta peningkatan kuota. Anda juga dapat meminta peningkatan kuota jika Anda mengirimkan permintaan Instans Spot dan Anda menerima kesalahan `Max spot instance count exceeded`.

Untuk meminta kenaikan kuota, gunakan konsol Kuota Layanan yang dijelaskan di Kuota EC2 layanan Amazon.

Anda dapat meluncurkan kombinasi tipe instans apa pun yang memenuhi kebutuhan aplikasi Anda yang berubah. Misalnya, dengan kuota Semua Permintaan Instans Spot Standar 256 vCPUs, Anda dapat meminta 32 Instans `m5.2xlarge` Spot (32 x 8 vCPUs) atau 16 Instans `c5.4xlarge` Spot (16 x 16 v). CPUs

Dengan integrasi CloudWatch metrik Amazon, Anda dapat memantau penggunaan EC2 terhadap kuota Anda. Anda juga dapat mengonfigurasi alarm untuk memperingatkan saat sudah mendekati kuota. Untuk informasi selengkapnya, lihat Service Quotas dan CloudWatch alarm Amazon di Panduan Pengguna Service Quotas di Panduan Pengguna Amazon. CloudWatch

Host Khusus Amazon EC

Host Khusus Amazon EC2 adalah server fisik yang sepenuhnya didedikasikan untuk Anda gunakan. Anda dapat memilih untuk berbagi kapasitas instans dengan AWS akun lain. Untuk informasi selengkapnya, lihat Berbagi Host Khusus Amazon EC2 lintas akun.

Host Khusus memberikan visibilitas dan kontrol atas penempatan instans dan mendukung afinitas host. Ini berarti Anda dapat meluncurkan dan menjalankan instance pada host tertentu, dan Anda dapat memastikan bahwa instance hanya berjalan pada host tertentu. Untuk informasi selengkapnya, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.

Tuan Rumah Khusus menyediakan dukungan Bring Your Own License (BYOL) yang komprehensif. Mereka memungkinkan Anda untuk menggunakan lisensi perangkat lunak per-soket, per-core, atau per-VM yang ada, termasuk Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, atau lisensi perangkat lunak lain yang terikat pada, soket, atau inti fisik VMs, tunduk pada persyaratan lisensi Anda.

Jika Anda memerlukan instans Anda untuk berjalan pada perangkat keras khusus, tetapi Anda tidak memerlukan visibilitas atau kontrol atas penempatan instans, dan Anda tidak perlu menggunakan lisensi perangkat lunak per-soket atau per-inti, Anda dapat mempertimbangkan untuk menggunakan Instans Khusus sebagai gantinya. Instans Khusus dan Host Khusus keduanya dapat digunakan untuk meluncurkan instans Amazon EC2 ke server fisik khusus. Tidak ada perbedaan performa, keamanan, atau fisik di antara Instans Khusus dan instans pada Host Khusus. Namun, ada beberapa perbedaan utama di antara mereka. Tabel berikut menyoroti beberapa perbedaan utama antara Instans Khusus dan Host Khusus:

	Host Khusus	Instans Khusus
Server fisik khusus	Server fisik dengan kapasitas instans yang sepenuhnya didedikasikan untuk Anda gunakan.	Server fisik yang didedikasikan untuk satu akun pelanggan.
Pembagian kapasitas instans	Dapat berbagi kapasitas instans dengan akun lain.	Tidak didukung
Penagihan	Tagihan per host	Tagihan per instans
Visibilitas soket, inti, dan ID host	Memberikan visibilitas dalam jumlah soket dan inti fisik	Tidak ada visibilitas
Afinitas host dan instans	Memungkinkan Anda melakukan deployment instans Anda secara konsisten ke server fisik yang sama seiring waktu	Tidak didukung
Penempatan instans tertarget	Memberikan visibilitas dan kontrol tambahan atas cara penempatan instans di server fisik	Tidak didukung
Pemulihan instans otomatis	Didukung. Untuk informasi selengkapnya, lihat Pemulihan Host Khusus Amazon EC2.	Didukung
Bawa Lisensi Sendiri (BYOL)	Didukung	Dukungan parsial*
Reservasi Kapasitas	Tidak didukung	Didukung

* Microsoft SQL Server dengan License Mobility melalui Jaminan Perangkat Lunak, sedangkan lisensi Windows Virtual Desktop Access (VDA) dapat digunakan dengan Instans Khusus.

Untuk informasi selengkapnya tentang metadata instans, lihat Instans EC2 Khusus Amazon.

Larangan Host Khusus

Sebelum Anda mengalokasikan Host Khusus, perhatikan batasan dan larangan berikut:

- Untuk menjalankan RHEL dan SUSE Linux pada Host Khusus, Anda harus membawa sendiri. AMIs Anda tidak dapat menggunakan RHEL dan SUSE Linux AMIs yang ditawarkan oleh AWS atau yang tersedia AWS Marketplace dengan Host Khusus. Untuk informasi selengkapnya tentang cara membuat AMI Anda sendiri, lihatBawa lisensi perangkat lunak Anda sendiri ke Host Khusus Amazon EC2.

  Pembatasan ini tidak berlaku untuk host yang dialokasikan untuk instans memori tinggi (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, dan `u-24tb1.metal`). RHEL dan SUSE Linux AMIs yang ditawarkan oleh AWS atau yang tersedia di AWS Marketplace dapat digunakan dengan host ini.
- Ada batasan jumlah menjalankan Host Khusus per keluarga instans per akun AWS per Wilayah. Kuota hanya berlaku untuk menjalankan instans. Jika instans Anda tertunda, berhenti, atau dihentikan, instans tersebut tidak akan dihitung ke dalam kuota Anda. Untuk melihat kuota akun Anda, atau meminta peningkatan kuota, gunakan konsol Kuota Layanan.
- Grup Auto Scaling didukung saat menggunakan templat peluncuran yang menentukan grup sumber daya host. Untuk informasi selengkapnya, lihat Membuat template peluncuran menggunakan setelan lanjutan di Panduan Pengguna Amazon EC2 Auto Scaling.
- Instans Amazon RDS tidak didukung.
- Tingkat Penggunaan AWS Gratis tidak tersedia untuk Host Khusus.
- Kontrol penempatan instans mengacu pada pengelolaan peluncuran instans ke Host Khusus. Anda tidak dapat meluncurkan Host Khusus ke dalam grup penempatan.
- Jika Anda mengalokasikan host untuk tipe instans tervirtualisasi, Anda tidak dapat mengubah tipe instans menjadi tipe `.metal` instans setelah host dialokasikan. Misalnya, jika Anda mengalokasikan host untuk tipe instans `m5.large`, Anda tidak dapat mengubah tipe instans menjadi `m5.metal`.

  Demikian pula, jika Anda mengalokasikan host untuk tipe `.metal` instans, Anda tidak dapat memodifikasi tipe instans menjadi tipe instans virtual setelah host dialokasikan. Misalnya, jika Anda mengalokasikan host untuk tipe instans `m5.metal`, Anda tidak dapat mengubah tipe instans menjadi `m5.large`.

Daftar Isi

- Harga dan penagihan Host Khusus Amazon EC2
- Konfigurasi kapasitas instans Host Khusus Amazon EC2
- Instans T3 Burstable di Host Khusus Amazon EC2
- Bawa lisensi perangkat lunak Anda sendiri ke Host Khusus Amazon EC2
- Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host
- Alokasikan Host Khusus Amazon EC2 untuk digunakan di akun Anda
- Luncurkan instans Amazon EC2 di Host Khusus Amazon EC2
- Luncurkan instans Amazon EC2 ke grup sumber daya host
- Ubah pengaturan penempatan otomatis untuk Host Khusus Amazon EC2 yang ada
- Ubah jenis instans yang didukung untuk Host Khusus Amazon EC2 yang sudah ada
- Ubah penyewaan dan afinitas Host Khusus Amazon EC2 untuk instans Amazon EC2
- Rilis Host Khusus Amazon EC2
- Bermigrasi ke Host Khusus Amazon EC2 berbasis Nitro
- Beli Reservasi Tuan Rumah Khusus untuk diskon tagihan Host Khusus
- Berbagi Host Khusus Amazon EC2 lintas akun
- Host Khusus Amazon EC2 di AWS Outposts
- Pemulihan Host Khusus Amazon EC2
- Pemeliharaan host untuk Host Khusus Amazon EC2
- Pantau status Host Khusus Amazon EC2 Anda
- Lacak perubahan konfigurasi Host Khusus Amazon EC2 menggunakan AWS Config

Harga dan penagihan Host Khusus Amazon EC2

Harga untuk Host Khusus bervariasi menurut opsi pembayaran.

Opsi pembayaran

- Host Khusus Sesuai Permintaan
- Reservasi Host Khusus
- Savings Plans
- Harga untuk Windows Server pada Host Khusus

Host Khusus Sesuai Permintaan

Penagihan Sesuai Permintaan secara otomatis diaktifkan saat Anda mengalokasikan Host Khusus ke akun Anda.

Harga Sesuai Permintaan untuk Host Khusus bervariasi menurut keluarga instans dan Wilayah. Anda membayar per detik (dengan minimal 60 detik) untuk Host Khusus yang aktif, terlepas dari jumlah atau ukuran instans yang Anda pilih untuk diluncurkan. Untuk informasi selengkapnya tentang harga Sesuai Permintaan, lihat Harga Sesuai Permintaan Host Khusus Amazon EC2.

Anda dapat melepas Host Khusus Sesuai Permintaan kapan saja untuk berhenti mengakumulasi biayanya. Untuk informasi tentang pelepasan Host Khusus, lihat Rilis Host Khusus Amazon EC2.

Reservasi Host Khusus

Reservasi Host Khusus memberikan diskon penagihan dibandingkan dengan menjalankan Host Khusus Sesuai Permintaan. Reservasi tersedia dalam tiga opsi pembayaran:

- Tanpa Uang Muka—Reservasi Tanpa Uang Muka memberi Anda diskon untuk penggunaan Host Khusus selama jangka waktu tertentu dan tidak memerlukan pembayaran di muka. Tersedia dalam jangka waktu satu tahun dan tiga tahun. Hanya beberapa keluarga instans yang mendukung jangka waktu tiga tahun untuk Reservasi Tanpa Uang Muka.
- Sebagian Di Muka—Sebagian dari reservasi harus dibayar di muka dan sisa jam dalam jangka waktu tersebut ditagih dengan tarif yang didiskon. Tersedia dalam jangka waktu satu tahun dan tiga tahun.
- Lunas di Muka—Memberikan harga efektif terendah. Tersedia dalam jangka waktu satu tahun dan tiga tahun serta mencakup seluruh biaya selama jangka waktu itu di muka, tanpa biaya tambahan di masa mendatang.

Anda harus memiliki Host Khusus yang aktif di akun Anda sebelum dapat membeli reservasi. Setiap reservasi dapat mencakup satu host atau lebih yang mendukung keluarga instans yang sama dalam satu Zona Ketersediaan. Reservasi diterapkan ke keluarga instans di host, bukan ukuran instans. Jika Anda memiliki tiga Host Khusus dengan ukuran instans berbeda (`m4.xlarge`, `m4.medium`, dan `m4.large`) Anda dapat mengaitkan satu reservasi `m4` dengan semua Host Khusus tersebut. Keluarga instans dan Zona Ketersediaan reservasi harus cocok dengan Host Khusus yang ingin Anda kaitkan dengannya.

Saat reservasi dikaitkan dengan Host Khusus, Host Khusus tidak dapat dilepaskan hingga jangka waktu reservasi berakhir.

Untuk informasi selengkapnya tentang harga reservasi, lihat Harga Host Khusus Amazon EC2.

Savings Plans

Savings Plans adalah model penetapan harga fleksibel yang menawarkan penghematan signifikan atas Instans Sesuai Permintaan. Dengan Savings Plans, Anda membuat komitmen dengan jumlah penggunaan yang konsisten, dalam USD per jam, selama jangka waktu satu atau tiga tahun. Ini memberi Anda fleksibilitas untuk menggunakan Host Khusus yang paling sesuai dengan kebutuhan Anda dan terus menghemat uang, daripada membuat komitmen untuk Host Khusus tertentu. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Savings Plans.

> **Note**
>
> Savings Plans tidak didukung dengan Host Khusus `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, dan `u-24tb1.metal`.

Harga untuk Windows Server pada Host Khusus

Tunduk pada persyaratan lisensi Microsoft, Anda dapat membawa lisensi Windows Server dan SQL Server yang ada ke Host Khusus. Tidak ada biaya tambahan untuk penggunaan perangkat lunak jika Anda memilih untuk membawa lisensi Anda sendiri.

Selain itu, Anda juga dapat menggunakan Windows Server AMIs yang disediakan oleh Amazon untuk menjalankan versi terbaru Windows Server pada Host Khusus. Ini umum untuk skenario di mana Anda memiliki lisensi SQL Server yang memenuhi syarat untuk dijalankan di Host Khusus, tetapi memerlukan Windows Server untuk menjalankan beban kerja SQL Server. Windows Server AMIs yang disediakan oleh Amazon hanya didukung pada jenis instans generasi saat ini. Untuk informasi selengkapnya, lihat Harga Host Khusus Amazon EC2.

Konfigurasi kapasitas instans Host Khusus Amazon EC2

Host Khusus mendukung konfigurasi yang berbeda (inti fisik, soket, dan VCPUs) yang memungkinkan Anda menjalankan instance dari keluarga dan ukuran yang berbeda.

Saat mengalokasikan Host Khusus di akun, Anda dapat memilih konfigurasi yang mendukung baik satu tipe instans maupun beberapa tipe instans dalam keluarga instans yang sama. Jumlah instans yang dapat Anda jalankan di host tergantung pada konfigurasi yang Anda pilih.

Daftar Isi

- Dukungan tipe instans tunggal
- Dukungan tipe banyak instans

Dukungan tipe instans tunggal

Anda dapat mengalokasikan Host Khusus yang hanya mendukung satu tipe instans. Dengan konfigurasi ini, setiap instans yang Anda luncurkan di Host Khusus harus memiliki tipe instans yang sama, yang Anda tentukan saat mengalokasikan host.

Misalnya, Anda dapat mengalokasikan host yang hanya mendukung tipe `m5.4xlarge` instans. Dalam hal ini, Anda hanya dapat menjalankan `m5.4xlarge` instans di host tersebut.

Jumlah instans yang dapat Anda luncurkan ke host bergantung pada jumlah inti fisik yang disediakan oleh host, dan jumlah inti yang dikonsumsi oleh tipe instans yang ditentukan. Misalnya, jika Anda mengalokasikan host untuk `m5.4xlarge` instans, host menyediakan 48 core fisik, dan setiap `m5.4xlarge` instans mengkonsumsi 8 core fisik. Ini berarti Anda dapat meluncurkan hingga 6 instans pada host tersebut (48 core fisik/8 core per instans = 6 instans).

Dukungan tipe banyak instans

Anda dapat mengalokasikan Host Khusus yang mendukung banyak tipe instans dalam keluarga instans yang sama. Ini memungkinkan Anda menjalankan tipe instans yang berbeda pada host yang sama, selama mereka berada dalam keluarga instans yang sama dan host memiliki kapasitas instans yang memadai.

Misalnya, Anda dapat mengalokasikan host yang mendukung berbagai tipe instans dalam keluarga `R5` instans. Dalam hal ini, Anda dapat meluncurkan kombinasi jenis `R5` instans tertentu, seperti `r5.larger5.xlarge`,`r5.2xlarge`,, dan`r5.4xlarge`, pada host tersebut, dalam kapasitas inti fisik host.

Keluarga instans berikut mendukung Host Khusus dengan dukungan beberapa tipe instans:

- Tujuan umum: A1 | M5 | M5n | M6i | M7i | T3
- Komputasi dioptimalkan: C5 | C5n | C6i | C7i
- Memori dioptimalkan: R5 | R5n | R6i | R7i

Jumlah instans yang dapat Anda jalankan di host bergantung pada jumlah core fisik yang disediakan oleh host, dan jumlah core yang dikonsumsi oleh setiap tipe instans yang Anda jalankan di

host. Misalnya, jika Anda mengalokasikan R5 host, yang menyediakan 48 core fisik, dan Anda menjalankan dua `r5.2xlarge` instance (4 core x 2 instance) dan tiga `r5.4xlarge` instance (8 core x 3 instance), instance tersebut mengkonsumsi total 32 core, dan Anda mungkin dapat menjalankan kombinasi R5 instance tertentu selama mereka berada dalam 16 core yang tersisa.

Namun, untuk setiap keluarga instance, ada batasan jumlah instance yang dapat dijalankan untuk setiap jenis instance. Misalnya, Host R5 Khusus mendukung maksimal 2 `r5.8xlarge` instans, yang menggunakan 32 inti fisik. Dalam hal ini, R5 contoh tambahan dari tipe yang lebih kecil kemudian dapat digunakan untuk mengisi host ke kapasitas inti. Untuk jumlah tipe instans yang didukung untuk setiap keluarga instans, lihat Tabel Konfigurasi Host Khusus.

Tabel berikut menunjukkan contoh kombinasi tipe instans:

Keluarga instans	Contoh kombinasi tipe instance	
R5	• Contoh 1: 4 x `r5.4xlarge` + 4 x `r5.2xlarge` • Contoh 2: 1 x `r5.12xlarge` + 1 x `r5.4xlarge` + 1 x `r5.2xlarge` + 5 x `r5.xlarge` + 2 x `r5.large`	
C5	• Contoh 1: 1 x `c5.9xlarge` + 2 x `c5.4xlarge` + 1 x `c5.xlarge` • Contoh 2: 4 x `c5.4xlarge` + 1 x `c5.xlarge` + 2 x `c5.large`	
M5	• Contoh 1: 4 x `m5.4xlarge` + 4 x `m5.2xlarge` • Contoh 2: 1 x `m5.12xlarge` + 1 x `m5.4xlarge` + 1 x `m5.2xlarge` + 5 x `m5.xlarge` + 2 x `m5.large`	

Pertimbangan-pertimbangan

Ingatlah hal-hal berikut ini saat bekerja dengan Host Khusus yang mendukung banyak tipe instans:

- Menggunakan beberapa jenis instance pada host yang sama hanya dimungkinkan dalam keluarga instance yang sama.
- Saat mencampur jenis instance, untuk memaksimalkan pemanfaatan host, sebaiknya luncurkan tipe instans yang lebih besar terlebih dahulu diikuti dengan tipe instans yang lebih kecil.
  - Bergantung pada kombinasi dan urutan peluncuran jenis instans pada Host Khusus, secara fisik tidak mungkin memaksimalkan pemanfaatan host. Saat mencampur jenis instance pada host, beberapa kapasitas mungkin tersedia di host tetapi tidak dapat digunakan. Misalnya, Anda mungkin melihat 16 v CPUs tersedia di host r5n tetapi mungkin tidak dapat meluncurkan instance 4xlarge pada host meskipun r5n.4xlarge berjalan pada 16 v. CPUs

> **Note**
>
> Jika Anda mengaktifkan Host Khusus A1 untuk beberapa jenis instans, Anda hanya dapat meluncurkan campuran `a1.xlarge` dan `a1.2xlarge` instance pada host tersebut. Jika Anda meluncurkan `a1.large` instans `a1.medium` atau pada host itu, Anda akan dibatasi untuk meluncurkan hanya lebih banyak jenis instance yang sama di host. Satu `a1.4xlarge` instance mengkonsumsi semua kapasitas pada host. Jika Anda memerlukan host untuk salah satu `a1.medium` atau `a1.large` instans, sebaiknya Anda mengalokasikan host terpisah untuk jenis instans tersebut.

Instans T3 Burstable di Host Khusus Amazon EC2

Host Khusus mendukung instans T3 performa dapat melonjak. Instans T3 menyediakan cara hemat biaya untuk menggunakan perangkat lunak lisensi BYOL Anda yang memenuhi syarat pada perangkat keras khusus. Jejak vCPU yang lebih kecil dari instans T3 memungkinkan Anda untuk mengonsolidasikan beban kerja Anda pada host yang lebih sedikit dan memaksimalkan pemanfaatan lisensi per inti Anda.

Host Khusus T3 paling cocok untuk menjalankan perangkat lunak BYOL dengan pemanfaatan CPU rendah hingga sedang. Beban kerja tersebut termasuk lisensi perangkat lunak per soket, per inti, atau per VM yang memenuhi syarat, seperti Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux, dan Oracle Database. Contoh beban kerja yang cocok untuk Host Khusus T3 adalah basis data kecil dan menengah, desktop virtual, lingkungan pengembangan dan pengujian, repositori kode, dan prototipe produk. Host Khusus T3 tidak direkomendasikan untuk beban kerja dengan pemanfaatan CPU tinggi yang berkelanjutan atau untuk beban kerja yang mengalami lonjakan CPU yang berkorelasi secara bersamaan.

Instans T3 pada Host Khusus menggunakan model kredit yang sama dengan instans T3 pada perangkat keras penghunian bersama. Namun, mereka hanya mendukung mode kredit `standard`; mereka tidak mendukung mode kredit `unlimited`. Dalam mode `standard`, instans T3 di Host Khusus memperoleh, menggunakan, dan mengakumulasikan kredit dengan cara yang sama seperti instans yang dapat melonjak pada perangkat keras penghunian bersama. Mereka memberikan performa CPU dasar dengan kemampuan untuk melonjak di atas level acuan. Untuk melonjak di atas batas dasar, instans menggunakan kredit yang telah diakumulasikan dalam saldo kredit CPU. Ketika kredit akumulasi habis, pemanfaatan CPU diturunkan ke tingkat acuan. Untuk informasi selengkapnya tentang mode `standard`, lihat Cara kerja instans performa yang dapat melonjak standar.

Host Khusus T3 mendukung semua fitur yang ditawarkan oleh Host Khusus Amazon EC2, termasuk banyak ukuran instans pada satu host, grup sumber daya Host, dan BYOL.

Ukuran dan konfigurasi instans T3 yang didukung

Host Khusus T3 menjalankan instans T3 tujuan umum yang dapat melonjak, yang berbagi sumber daya CPU host dengan menyediakan performa CPU dasar dan kemampuan untuk melonjak ke tingkat yang lebih tinggi bila diperlukan. Hal ini memungkinkan Host Khusus T3, yang memiliki 48 inti, untuk mendukung hingga maksimum 192 instans per host. Untuk memanfaatkan sumber daya host secara efisien dan memberikan kinerja instans terbaik, algoritme penempatan instans Amazon EC2 secara otomatis menghitung jumlah instans dan kombinasi ukuran instans yang didukung yang dapat diluncurkan di host.

Host Khusus T3 mendukung beberapa tipe instans pada host yang sama. Semua ukuran instans T3 didukung pada Host Khusus. Anda dapat menjalankan berbagai kombinasi instans T3 hingga batas CPU host.

Tabel berikut mencantumkan tipe instans yang didukung, merangkum kinerja setiap tipe instans, dan menunjukkan jumlah maksimum instans dari setiap ukuran yang dapat diluncurkan.

Tipe insta	v CPUs	Memori (GiB)	Pemanfaatan CPU acuan per vCPU	Bandwidth lonjakan jaringan (Gbps)	Bandwidth lonjakan Amazon EBS (Mbps)	Jumlah maksimum instans per Host Khusus
t3.na	2	0,5	5%	5	Hingga 2.085	192

Tipe insta	v CPUs	Memori (GiB)	Pemanfaatan CPU acuan per vCPU	Bandwidth lonjakan jaringan (Gbps)	Bandwidth lonjakan Amazon EBS (Mbps)	Jumlah maksimum instans per Host Khusus
t3.m	2	1	10%	5	Hingga 2.085	192
t3.sn	2	2	20%	5	Hingga 2.085	192
t3.m	2	4	20%	5	Hingga 2.085	192
t3.la	2	8	30%	5	2,780	96
t3.xl	4	16	40%	5	2,780	48
t3.2x e	8	32	40%	5	2,780	24

Pantau pemanfaatan CPU untuk Host Khusus T3

Anda dapat menggunakan CloudWatch metrik `DedicatedHostCPUUtilization` Amazon untuk memantau pemanfaatan vCPU dari Host Khusus. Metrik tersedia di namespace `EC2` dan dimensi `Per-Host-Metrics`. Untuk informasi selengkapnya, lihat Metrik Host Khusus.

Bawa lisensi perangkat lunak Anda sendiri ke Host Khusus Amazon EC2

Host Khusus memungkinkan Anda menggunakan lisensi perangkat lunak per soket, per inti, atau per VM yang ada. Saat Anda membawa lisensi Anda sendiri, Anda bertanggung jawab untuk mengelola lisensi Anda sendiri. Namun, Amazon EC2 memiliki fitur yang membantu Anda menjaga kepatuhan lisensi, seperti afinitas instans dan penempatan tertarget.

Ini adalah langkah umum yang harus diikuti untuk membawa gambar mesin berlisensi volume Anda sendiri ke Amazon EC2.

1. Verifikasi bahwa persyaratan lisensi yang mengontrol penggunaan gambar mesin Anda mengizinkan penggunaan dalam lingkungan cloud tervirtualisasi. Untuk informasi selengkapnya tentang Lisensi Microsoft, lihat Amazon Web Services dan Microsoft Licensing.

2. Setelah Anda memverifikasi bahwa gambar mesin Anda dapat digunakan dalam Amazon EC2, impor gambar menggunakan VM Import/Export. Untuk informasi tentang cara mengimpor gambar mesin Anda, lihat Panduan Import/Export Pengguna VM.
3. Setelah Anda mengimpor gambar mesin, Anda dapat meluncurkan instans darinya ke Host Khusus yang aktif di akun Anda.
4. Saat Anda menjalankan instans ini, bergantung pada sistem operasi, Anda mungkin diminta untuk mengaktifkan instans ini di server KMS Anda sendiri (misalnya, Windows Server atau Windows SQL Server). Anda tidak dapat mengaktifkan AMI Windows yang diimpor pada server Amazon Windows KMS.

> **Note**
>
> Untuk melacak bagaimana gambar Anda digunakan AWS, aktifkan perekaman host AWS Config. Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi ke Host Khusus dan menggunakan output sebagai sumber data untuk pelaporan lisensi. Untuk informasi selengkapnya, lihat Lacak perubahan konfigurasi Host Khusus Amazon EC2 menggunakan AWS Config.

Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host

Kontrol penempatan untuk Host Khusus terjadi pada level instans dan level host.

Penempatan otomatis

Penempatan otomatis dikonfigurasi di tingkat host. Ini memungkinkan Anda untuk mengelola apakah instans yang Anda luncurkan diluncurkan ke host tertentu, atau ke host mana pun yang tersedia yang memiliki konfigurasi yang cocok.

Ketika penempatan otomatis dinonaktifkan untuk Host Khusus, ia hanya menerima peluncuran instance penyewaan host yang menentukan ID host uniknya. Ini adalah pengaturan default untuk Host Khusus baru.

Ketika penempatan otomatis diaktifkan untuk Host Khusus, ia menerima peluncuran instans penyewaan host yang tidak ditargetkan yang cocok dengan konfigurasi tipe instance-nya.

Saat meluncurkan sebuah instans, Anda perlu mengonfigurasi penghuniannya. Meluncurkan sebuah instans ke Host Khusus tanpa memberikan `HostId` yang spesifik memungkinkannya untuk

diluncurkan pada Host Khusus yang memiliki penempatan otomatis yang diaktifkan dan yang cocok dengan tipe instansnya.

Afinitas host

Afinitas host dikonfigurasi pada tingkat instans. Ini menetapkan hubungan peluncuran antara sebuah instans dan Host Khusus.

Saat afinitas ditetapkan ke `Host`, sebuah instans yang diluncurkan ke host tertentu selalu dimulai ulang di host yang sama jika dihentikan. Ini berlaku untuk peluncuran tertarget dan tidak tertarget.

Saat afinitas diatur ke `Default`, dan Anda menghentikan serta memulai ulang instans, instans ini dapat dimulai ulang di semua host yang tersedia. Namun, ia mencoba untuk meluncurkan kembali ke Host Khusus terakhir yang dijalankannya (dengan upaya terbaik).

Alokasikan Host Khusus Amazon EC2 untuk digunakan di akun Anda

Untuk mulai menggunakan Host Khusus, Anda harus terlebih dahulu mengalokasikannya di akun Anda. Setelah Anda mengalokasikan Host Khusus, kapasitas Host Khusus akan segera tersedia di akun Anda dan Anda dapat mulai meluncurkan instans ke Host Khusus.

Saat mengalokasikan Host Khusus di akun, Anda dapat memilih konfigurasi yang mendukung baik satu tipe instans maupun beberapa tipe instans dalam keluarga instans yang sama. Jumlah instans yang dapat Anda jalankan di host tergantung pada konfigurasi yang Anda pilih. Untuk informasi selengkapnya, lihat Konfigurasi kapasitas instans Host Khusus Amazon EC2.

Console

Untuk mengalokasikan Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus lalu pilih Alokasi Host Khusus.
3. Di keluarga instans, pilih keluarga instans untuk Host Khusus.
4. Tentukan apakah Host Khusus mendukung banyak ukuran instans dalam keluarga instans yang dipilih, atau hanya tipe instans tertentu. Lakukan salah satu dari berikut ini.

   - Untuk mengonfigurasi Host Khusus agar mendukung banyak tipe instans dalam keluarga instans yang dipilih, pada Dukung beberapa tipe instans, pilih Aktifkan. Dengan mengaktifkannya, Anda akan dapat meluncurkan ukuran instans yang berbeda dari keluarga instans yang sama ke Host Khusus. Misalnya, jika Anda memilih keluarga instans

m5 dan memilih opsi ini, Anda dapat meluncurkan instans m5.xlarge dan m5.4xlarge ke Host Khusus.

- Untuk mengonfigurasi Host Khusus agar mendukung satu tipe instans dalam keluarga instans yang dipilih, hapus Dukung beberapa tipe instans, lalu untuk Tipe instans, pilih tipe instans yang akan didukung. Dengan demikian, Anda akan dapat meluncurkan satu tipe instans pada Host Khusus. Misalnya, jika Anda memilih opsi ini dan menentukan m5.4xlarge sebagai tipe instans yang didukung, Anda hanya dapat meluncurkan instans m5.4xlarge ke Host Khusus.

5. Untuk Zona Ketersediaan, pilih Zona Ketersediaan untuk mengalokasikan Host Khusus.
6. Agar Host Khusus dapat menerima peluncuran instans tidak tertarget yang cocok dengan tipe instansnya, di Penempatan otomatis instans, pilih Aktifkan. Untuk informasi selengkapnya tentang penempatan otomatis, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.
7. Untuk mengaktifkan pemulihan host untuk Host Khusus, pada Pemulihan host, pilih Aktifkan. Untuk informasi selengkapnya, lihat Pemulihan Host Khusus Amazon EC2.
8. Untuk Kuantitas, masukkan jumlah Host Khusus yang akan dialokasikan.
9. (Opsional) Pilih Tambahkan tanda baru dan masukkan kunci tanda dan nilai tanda.
10. Pilih Alokasikan.

AWS CLI

Untuk mengalokasikan Host Khusus

Gunakan perintah allocate-hosts. Contoh berikut mengalokasikan Host Khusus yang mendukung beberapa jenis instans dari keluarga m5 instance di us-east-1a Availability Zone. Ini juga memungkinkan pemulihan host dan menonaktifkan penempatan otomatis.

```
aws ec2 allocate-hosts \
    --instance-family "m5" \
    --availability-zone "us-east-1a" \
    --auto-placement "off" \
    --host-recovery "on" \
    --quantity 1
```

Contoh berikut mengalokasikan Host Khusus yang mendukung peluncuran instans yang tidak ditargetkan di Availability Zone yang ditentukan, mengaktifkan pemulihan host, dan mengaktifkan penempatan otomatis.

```
aws ec2 allocate-hosts \
    --instance-type "m5.large" \
    --availability-zone "eu-west-1a" \
    --auto-placement "on" \
    --host-recovery "on" \
    --quantity 1
```

PowerShell

Untuk mengalokasikan Host Khusus

Gunakan New-EC2Hostcmdlet. Contoh berikut mengalokasikan Host Khusus yang mendukung beberapa jenis instans dari keluarga `m5` instance di `us-east-1a` Availability Zone. Host juga mengaktifkan pemulihan host dan penempatan otomatis dinonaktifkan.

```
New-EC2Host `
    -InstanceFamily m5 `
    -AvailabilityZone us-east-1a `
    -AutoPlacement Off `
    -HostRecovery On `
    -Quantity 1
```

Contoh berikut mengalokasikan Host Khusus yang mendukung peluncuran instans yang tidak ditargetkan di Availability Zone yang ditentukan dan memungkinkan pemulihan host.

```
New-EC2Host `
    -InstanceType m5.large `
    -AvailabilityZone eu-west-1a `
    -AutoPlacement On `
    -HostRecovery On `
    -Quantity 1
```

Luncurkan instans Amazon EC2 di Host Khusus Amazon EC2

Setelah Anda mengalokasikan Host Khusus, Anda dapat meluncurkan instans ke dalamnya. Anda tidak dapat meluncurkan instans dengan penghunian `host` jika Anda tidak memiliki Host Khusus aktif dengan kapasitas ketersediaan yang cukup untuk tipe instans yang Anda luncurkan.

Pertimbangan-pertimbangan

- AMI SQL Server, SUSE, dan RHEL yang disediakan oleh Amazon EC2 tidak dapat digunakan dengan Host Khusus.
- Untuk Host Khusus yang mendukung banyak ukuran instans, kami menyarankan Anda untuk meluncurkan ukuran instans yang lebih besar terlebih dahulu, kemudian mengisi kapasitas instans yang tersisa dengan ukuran instans yang lebih kecil, sesuai kebutuhan.
- Sebelum Anda meluncurkan instans Anda, perhatikan batasannya. Untuk informasi selengkapnya, lihat Larangan Host Khusus.

Console

Untuk meluncurkan sebuah instans ke Host Khusus tertentu dari halaman Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Host Khusus di panel navigasi.
3. Di halaman Host Khusus, pilih host dan pilih Tindakan, Luncurkan Instans ke host.
4. Di bagian Gambar Aplikasi dan OS, pilih AMI dari daftar.
5. Di bagian tipe instans, pilih tipe instans yang akan diluncurkan.

> **Note**
>
> Jika Host Khusus mendukung satu tipe instans saja, tipe instans yang didukung akan dipilih secara default dan tidak dapat diubah.
> Jika Host Khusus mendukung banyak tipe instans, Anda harus memilih tipe instans dalam keluarga instans yang didukung berdasarkan kapasitas instans yang tersedia pada Host Khusus. Kami menyarankan Anda untuk meluncurkan ukuran instans yang lebih besar terlebih dahulu, kemudian mengisi kapasitas instans yang tersisa dengan ukuran instans yang lebih kecil, sesuai kebutuhan.

6. Di bagian Key pair, pilih key pair untuk diasosiasikan dengan instans.
7. Di bagian Detail lanjutan, untuk Afinitas sewa, pilih salah satu dari berikut ini:
   - Mati - Afinitas host dinonaktifkan. Instance diluncurkan ke host yang ditentukan, tetapi tidak dijamin untuk memulai ulang pada Host Khusus yang sama jika dihentikan.

- ID Host Khusus - Afinitas host diaktifkan. Jika dihentikan, instance selalu restart pada host yang ditentukan ini jika memiliki kapasitas. Jika host tidak memiliki kapasitas, instance tidak dapat dimulai ulang; Anda harus membangun afinitas dengan host yang berbeda.

Untuk informasi selengkapnya tentang Afinitas, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.

> **Note**
>
> Opsi Penghunian dan Host telah dikonfigurasi sebelumnya berdasarkan host yang Anda pilih.

8. Konfigurasikan opsi instans yang tersisa sesuai kebutuhan. Untuk informasi selengkapnya, lihat Referensi untuk parameter konfigurasi EC2 instans Amazon.
9. Pilih Luncurkan instans.

Untuk meluncurkan sebuah instans ke Host Khusus menggunakan Wizard Peluncuran Instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, Luncurkan instans.
3. Di bagian Gambar Aplikasi dan OS, pilih AMI dari daftar.
4. Di bagian tipe instans, pilih tipe instans yang akan diluncurkan.
5. Di bagian Key pair, pilih key pair untuk diasosiasikan dengan instans.
6. Di bagian Detail lanjutan, lakukan hal berikut:
   a. Untuk Penghunian, pilih Host Khusus.
   b. Untuk Target host berdasarkan, pilih ID Host.
   c. Untuk ID host Target, pilih host yang akan meluncurkan instans.
   d. Untuk afinitas Tenancy, pilih salah satu dari berikut ini:
      - Mati - Afinitas host dinonaktifkan. Instance diluncurkan ke host yang ditentukan, tetapi tidak dijamin untuk memulai ulang pada Host Khusus yang sama jika dihentikan.
      - ID Host Khusus - Afinitas host diaktifkan. Jika dihentikan, instance selalu restart pada host yang ditentukan ini jika memiliki kapasitas. Jika host tidak memiliki kapasitas,

instance tidak dapat dimulai ulang; Anda harus membangun afinitas dengan host yang berbeda.

Untuk informasi selengkapnya tentang Afinitas, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.

7. Konfigurasikan opsi instans yang tersisa sesuai kebutuhan. Untuk informasi selengkapnya, lihat Referensi untuk parameter konfigurasi EC2 instans Amazon.
8. Pilih Luncurkan instans.

AWS CLI

Untuk meluncurkan sebuah instans ke Host Khusus

Gunakan perintah run-instance dan tentukan afinitas instance, penyewaan, dan host dalam opsi. `--placement`

Untuk meluncurkan ke Host Khusus tertentu dengan afinitas host (instance selalu dimulai ulang pada host yang sama jika dihentikan):

```
--placement Affinity=host,Tenancy=host,HostId=h-07879acf49EXAMPLE
```

Untuk memulai ke Host Khusus tertentu tanpa afinitas host (instance dapat dimulai ulang pada host mana pun yang tersedia):

```
--placement Tenancy=host,HostId=h-07879acf49EXAMPLE
```

Untuk meluncurkan ke Host Khusus yang tersedia dengan penempatan otomatis diaktifkan dan jenis instans yang cocok:

```
--placement Tenancy=host
```

PowerShell

Untuk meluncurkan sebuah instans ke Host Khusus

Gunakan New-EC2Instancecmdlet dan tentukan afinitas instance, penyewaan, dan host dalam parameter. `-Placement`

Untuk meluncurkan ke Host Khusus tertentu dengan afinitas host (instance selalu dimulai ulang pada host yang sama jika dihentikan):

```
-Placement_Affinity host `
-Placement_Tenancy host `
-Placement_HostId h-07879acf49EXAMPLE
```

Untuk memulai ke Host Khusus tertentu tanpa afinitas host (instance dapat dimulai ulang pada host mana pun yang tersedia):

```
-Placement_Tenancy host `
-Placement_HostId h-07879acf49EXAMPLE
```

Untuk meluncurkan ke Host Khusus yang tersedia dengan penempatan otomatis diaktifkan dan jenis instans yang cocok:

```
-Placement_Tenancy host
```

Luncurkan instans Amazon EC2 ke grup sumber daya host

Host Khusus juga terintegrasi dengan AWS License Manager. Dengan License Manager, Anda dapat membuat grup sumber daya host, yang merupakan kumpulan Host Khusus yang dikelola sebagai satu entitas. Saat membuat grup sumber daya host, Anda menentukan preferensi pengelolaan host, seperti alokasi otomatis dan lepas otomatis, untuk Host Khusus. Ini memungkinkan Anda meluncurkan instans ke Host Khusus tanpa mengalokasikan dan mengelola host tersebut secara manual. Untuk informasi selengkapnya, lihat Grup Sumber Daya Host di Panduan Pengguna AWS License Manager .

Saat Anda meluncurkan instans ke dalam grup sumber daya host yang memiliki Host Khusus dengan kapasitas instans yang tersedia, Amazon EC2 meluncurkan instans ke host tersebut. Jika grup sumber daya host tidak memiliki host dengan kapasitas instans yang tersedia, Amazon EC2 secara otomatis mengalokasikan host baru di grup sumber daya host, lalu meluncurkan instans tersebut ke host tersebut. Untuk informasi selengkapnya, lihat Grup Sumber Daya Host di Panduan Pengguna AWS License Manager .

Persyaratan dan batasan

- Anda harus mengaitkan konfigurasi lisensi berbasis inti atau soket dengan AMI.

- Anda tidak dapat menggunakan AMI SQL SQL Server, SUSE, atau RHEL yang disediakan oleh Amazon EC2 dengan Host Khusus.
- Anda tidak dapat menargetkan host tertentu dengan memilih ID host, dan Anda tidak dapat mengaktifkan afinitas instans saat meluncurkan sebuah instans ke dalam grup sumber daya host.

Console

Untuk meluncurkan sebuah instans ke dalam grup sumber daya host

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, Luncurkan instans.
3. Di bagian Gambar Aplikasi dan OS, pilih AMI dari daftar.
4. Di bagian tipe instans, pilih tipe instans yang akan diluncurkan.
5. Di bagian Key pair, pilih key pair untuk diasosiasikan dengan instans.
6. Di bagian Detail lanjutan, lakukan hal berikut:

   a. Untuk Penghunian, pilih Host Khusus.

   b. Untuk Host target oleh, pilih Grup sumber daya host.

   c. Untuk Grup sumber daya host penghunian, pilih grup sumber daya host di mana instans akan diluncurkan.

   d. Untuk Afinitas penghunian, lakukan salah satu hal berikut ini:

      - Pilih Nonaktif — Instans diluncurkan ke host yang ditentukan, tetapi tidak ada jaminan bahwa instans akan dimulai ulang pada Host Khusus yang sama jika dihentikan.
      - Pilih ID Host Khusus — Jika dihentikan, instans selalu dimulai ulang di host spesifik ini.

      Untuk informasi selengkapnya tentang Afinitas, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.
7. Konfigurasikan opsi instans yang tersisa sesuai kebutuhan. Untuk informasi selengkapnya, lihat Referensi untuk parameter konfigurasi EC2 instans Amazon.
8. Pilih Luncurkan instans.

AWS CLI

Untuk meluncurkan sebuah instans ke dalam grup sumber daya host

Gunakan perintah run-instans. Dalam `--placement` opsi, hilangkan penyewaan dan tentukan ARN dari grup sumber daya host.

```
--placement HostResourceGroupArn=arn:aws:resource-groups:us-
east-2:123456789012:group/my-resource-group
```

PowerShell

Untuk meluncurkan sebuah instans ke dalam grup sumber daya host

Gunakan New-EC2Instancecmdlet. Dalam `-Placement` parameter, hilangkan penyewaan dan tentukan ARN dari grup sumber daya host.

```
-Placement_HostResourceGroupArn arn:aws:resource-groups:us-
east-2:123456789012:group/my-resource-group
```

Ubah pengaturan penempatan otomatis untuk Host Khusus Amazon EC2 yang ada

Anda dapat mengubah pengaturan penempatan otomatis Host Khusus setelah Anda mengalokasikannya ke akun Anda AWS .

Console

Untuk memodifikasi penempatan otomatis Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Pilih host dan pilih Tindakan, Ubah host.
4. Untuk Penempatan otomatis instans, pilih Aktifkan untuk mengaktifkan penempatan otomatis, atau kosongkan Aktifkan untuk menonaktifkan penempatan otomatis. Untuk informasi selengkapnya, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.
5. Pilih Simpan.

AWS CLI

Untuk memodifikasi penempatan otomatis Host Khusus

Gunakan perintah modify-hosts.

```
aws ec2 modify-hosts \
    --auto-placement on \
    --host-ids h-012a3456b7890cdef
```

PowerShell

Untuk memodifikasi penempatan otomatis Host Khusus

Gunakan Edit-EC2Hostcmdlet.

```
Edit-EC2Host `
    -AutoPlacement 1 `
    -HostId h-012a3456b7890cdef
```

Ubah jenis instans yang didukung untuk Host Khusus Amazon EC2 yang sudah ada

Anda dapat memodifikasi Host Khusus untuk mengubah tipe instans yang didukungnya. Jika saat ini mendukung satu tipe instans, Anda dapat memodifikasinya untuk mendukung beberapa tipe instans dalam keluarga instans itu. Demikian pula, jika saat ini mendukung beberapa tipe instans, Anda dapat memodifikasinya untuk mendukung tipe instans tertentu saja.

Untuk mengubah Host Khusus agar mendukung banyak tipe instans, Anda harus terlebih dahulu menghentikan semua instans yang berjalan di host. Modifikasi membutuhkan waktu sekitar 10 menit untuk selesai. Transisi Host Khusus ke status `pending` saat modifikasi sedang berlangsung. Anda tidak dapat memulai instans yang berhenti atau meluncurkan instans baru pada Host Khusus saat berada di status `pending`.

Untuk mengubah Host Khusus yang mendukung banyak tipe instans agar hanya mendukung satu tipe instans, host tidak boleh memiliki instans yang sedang berjalan, atau instans yang sedang berjalan harus dari tipe instans yang Anda inginkan agar didukung oleh host. Misalnya, untuk mengubah host yang mendukung beberapa tipe instans di keluarga instans `m5` untuk mendukung instans `m5.large` saja, Host Khusus tidak boleh memiliki instans yang berjalan, atau hanya boleh memiliki instans `m5.large` yang berjalan di atasnya.

Jika Anda mengalokasikan host untuk tipe instans tervirtualisasi, Anda tidak dapat mengubah tipe instans menjadi tipe `.metal` instans setelah host dialokasikan. Misalnya, jika Anda mengalokasikan host untuk tipe instans `m5.large`, Anda tidak dapat mengubah tipe instans menjadi `m5.metal`. Demikian pula, jika Anda mengalokasikan host untuk tipe `.metal` instans, Anda tidak dapat

memodifikasi tipe instans menjadi tipe instans virtual setelah host dialokasikan. Misalnya, jika Anda mengalokasikan host untuk tipe instans `m5.metal`, Anda tidak dapat mengubah tipe instans menjadi `m5.large`.

Console

Untuk mengubah tipe instans yang didukung untuk Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel Navigasi, pilih Host Khusus.
3. Pilih Host Khusus untuk memodifikasi dan pilih Tindakan, Ubah host.
4. Lakukan salah satu hal berikut, tergantung pada konfigurasi Host Khusus saat ini:
   - Jika Host Khusus saat ini mendukung tipe instans tertentu, Dukung beberapa tipe instans tidak diaktifkan, dan Tipe instans mencantumkan tipe instans yang didukung. Untuk mengubah host agar mendukung banyak tipe dalam keluarga instans saat ini, pada Dukungan beberapa tipe instans, pilih Aktifkan.

     Anda harus terlebih dahulu menghentikan semua instans yang berjalan pada host sebelum memodifikasinya untuk mendukung banyak tipe instans.
   - Jika Host Khusus saat ini mendukung beberapa tipe instans dalam sebuah keluarga instans, Diaktifkan dipilih untuk Mendukung beberapa tipe instans. Untuk memodifikasi host agar mendukung tipe instans tertentu, pada Dukungan beberapa tipe instans, hapus Aktifkan, lalu pada Tipe instans, pilih tipe instans tertentu yang akan didukung.

     Anda tidak dapat mengubah keluarga instans yang didukung oleh Host Khusus.
5. Pilih Simpan.

AWS CLI

Untuk mengubah tipe instans yang didukung untuk Host Khusus

Gunakan perintah modify-hosts.

Contoh berikut memodifikasi Host Khusus untuk mendukung beberapa jenis instans dalam keluarga `m5` instance.

```
aws ec2 modify-hosts \
```

```
    --instance-family m5 \
    --host-ids h-012a3456b7890cdef
```

Contoh berikut memodifikasi Host Khusus untuk mendukung `m5.xlarge` instance saja.

```
aws ec2 modify-hosts \
    --instance-type m5.xlarge \
    --instance-family --host-ids h-012a3456b7890cdef
```

PowerShell

Untuk mengubah tipe instans yang didukung untuk Host Khusus

Gunakan Edit-EC2Hostcmdlet.

Contoh berikut memodifikasi Host Khusus untuk mendukung beberapa jenis instans dalam keluarga `m5` instance.

```
Edit-EC2Host `
    -InstanceFamily m5 `
    -HostId h-012a3456b7890cdef
```

Contoh berikut memodifikasi Host Khusus untuk mendukung `m5.xlarge` instance saja.

```
Edit-EC2Host `
    -InstanceType m5.xlarge `
    -HostId h-012a3456b7890cdef
```

Ubah penyewaan dan afinitas Host Khusus Amazon EC2 untuk instans Amazon EC2

Anda dapat mengubah penghunian instans setelah Anda meluncurkannya. Anda juga dapat mengubah afinitas instans Anda untuk menargetkan host tertentu atau mengizinkannya diluncurkan pada host khusus apa pun yang tersedia dengan atribut yang cocok di akun Anda. Untuk mengubah penghunian atau afinitas instans, instans tersebut harus ada dalam status `stopped`.

Detail sistem operasi instans Anda, dan apakah SQL Server diinstal, memengaruhi konversi apa yang didukung. Untuk informasi selengkapnya tentang jalur konversi penghunian yang tersedia untuk instans Anda, lihat Konversi penghunia di Panduan Pengguna Manajer Lisensi.

> **Note**
>
> Untuk instans T3, Anda harus meluncurkan instans pada Host Khusus untuk menggunakan penyewaan `host`. Untuk instans T3, Anda tidak dapat mengubah penghunian dari `host` ke `dedicated` atau `default`. Percobaan mengubah salah satu penghunian yang tidak didukung ini dapat mengakibatkan kode kesalahan `InvalidRequest`.

Console

Untuk memodifikasi penghunian atau afinitas instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Instans dan pilih instans yang akan dimodifikasi.
3. Pilih Status instans, Berhenti.
4. Dengan instans yang dipilih, pilih Tindakan, Pengaturan instans, Modifikasi penempatan instans.
5. Pada halaman Modify instance placement, konfigurasikan hal berikut:
   - Penghunian—Pilih salah satu dari berikut:
     - Jalankan instans perangkat keras khusus — Meluncurkan instans sebagai Instans Khusus. Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.
     - Meluncurkan instans pada Host Khusus — Meluncurkan instans ke Host Khusus dengan afinitas yang dapat dikonfigurasi.
   - Afinitas—Pilih salah satu dari berikut:
     - Instans ini dapat berjalan di salah satu host saya—Instans ini diluncurkan ke Host Khusus mana pun yang tersedia di akun Anda yang mendukung tipe instansnya.
     - Instans ini hanya dapat berjalan di host yang dipilih—Instans ini hanya dapat berjalan di Host Khusus yang dipilih untuk Host Target.
   - Target Host—Pilih Host Khusus tempat instans harus dijalankan. Jika tidak ada host target yang terdaftar, Anda mungkin tidak memiliki Host Khusus yang tersedia dan kompatibel di akun Anda.

   Untuk informasi selengkapnya, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.

6. Pilih Simpan.

AWS CLI

Untuk mengubah tenancy atau afinitas instance

Gunakan perintah modify-instance-placement. Contoh berikut mengubah afinitas instance yang ditentukan dari `default` untuk, `host`dan menentukan Host Khusus yang terkait dengan instans.

```
aws ec2 modify-instance-placement \
    --instance-id i-1234567890abcdef0 \
    --affinity host \
    --tenancy host \
    --host-id h-012a3456b7890cdef
```

PowerShell

Untuk memodifikasi penghunian atau afinitas instans

Gunakan Edit-EC2InstancePlacementcmdlet. Contoh berikut mengubah afinitas instans yang ditetapkan dari `default` menjadi `host`, dan menetapkan Host Khusus yang mempunyai afinitas dengan instans.

```
Edit-EC2InstancePlacement `
    -InstanceId i-1234567890abcdef0 `
    -Affinity host `
    -Tenancy host `
    -HostId h-012a3456b7890cdef
```

Rilis Host Khusus Amazon EC2

Jika Anda tidak lagi membutuhkan Host Khusus, Anda dapat menghentikan instans yang berjalan di host, mengarahkannya untuk diluncurkan di host yang berbeda, dan kemudian melepaskan host.

Setiap instans yang berjalan di Host Khusus harus dihentikan sebelum Anda dapat merilis host. Instans ini dapat dimigrasikan ke Host Khusus lainnya di akun Anda sehingga Anda dapat terus menggunakannya. Langkah-langkah ini hanya berlaku untuk Host Khusus Sesuai Permintaan.

Console

Untuk merilis Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Di halaman Host Khusus, pilih Host Khusus yang akan dirilis.
4. Pilih Tindakan, Rilis host.
5. Untuk mengonfirmasi, pilih Lepaskan.

AWS CLI

Untuk merilis Host Khusus

Gunakan perintah release-hosts.

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Untuk merilis Host Khusus

Gunakan Remove-EC2Hostcmdlet.

```
Remove-EC2Host -HostId h-012a3456b7890cdef
```

Setelah Anda merilis Host Khusus, Anda tidak dapat menggunakan kembali host atau ID host yang sama, sehingga Anda tidak lagi dikenai tarif penagihan Sesuai Permintaan. Status Host Khusus diubah menjadi `released`, dan Anda tidak dapat meluncurkan instans apa pun ke host itu.

> **Note**
>
> Jika Anda baru saja melepas Host Khusus, mungkin perlu beberapa saat bagi host tersebut untuk tidak diperhitungkan dalam batas Anda. Selama waktu ini, Anda mungkin mengalami kesalahan `LimitExceeded` saat mencoba mengalokasikan Host Khusus baru. Jika ini masalahnya, coba alokasikan host baru lagi setelah beberapa menit.

Instans yang dihentikan masih tersedia untuk digunakan dan terdaftar di halaman Instans. Pengaturan penghunian `host` dipertahankan.

Bermigrasi ke Host Khusus Amazon EC2 berbasis Nitro

Nitro System adalah kumpulan komponen perangkat keras dan perangkat lunak yang dibangun oleh AWS yang memungkinkan performa tinggi, ketersediaan tinggi, dan keamanan tinggi. Host Khusus berbasis Nitro menawarkan kinerja harga yang lebih baik dibandingkan dengan Host Khusus berbasis Xen. Jika Anda memiliki Host Khusus berbasis Xen di akun Anda, kami sarankan Anda memigrasikan beban kerja Anda ke Host Khusus berbasis Nitro. Untuk informasi selengkapnya, lihat AWS Nitro System.

Untuk bermigrasi dari Host Khusus berbasis Xen ke Host Khusus berbasis Nitro, Anda perlu memigrasikan instans berbasis Xen di Host Khusus Anda ke jenis instans berbasis Nitro, mengalokasikan Host Khusus berbasis Nitro baru, dan kemudian memindahkan instans berbasis Nitro yang dimigrasi ke Host Khusus berbasis Nitro baru Anda.

Topik ini memberikan langkah-langkah terperinci untuk bermigrasi dari Host Khusus berbasis Xen ke Host Khusus berbasis Nitro.

Langkah migrasi

- Langkah 1: Identifikasi Host Khusus Berbasis Xen
- Langkah 2: Migrasikan instance berbasis Xen ke tipe instans berbasis Nitro
- Langkah 3: Alokasikan Host Khusus Berbasis Nitro
- Langkah 4: Pindahkan instance yang dimigrasi ke Host Khusus berbasis Nitro baru
- Langkah 5: Lepaskan Host Khusus berbasis Xen yang tidak terpakai

Langkah 1: Identifikasi Host Khusus Berbasis Xen

Host Khusus berikut berbasis Xen dan memenuhi syarat untuk dimigrasikan ke Host Khusus berbasis Nitro.

- Tujuan umum: M3 | M4
- Komputasi dioptimalkan: C3 | C4
- Memori dioptimalkan: R3 | R4 | X1 | X1e
- Penyimpanan dioptimalkan: D2 | H1 | I2 | I3
- Komputasi yang dipercepat: F1 | G3 | P2 | P3

Untuk memeriksa apakah Anda memiliki Host Khusus berbasis Xen di akun Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Di kolom Penelusuran, gunakan filter keluarga Instance untuk mencari Host Khusus berbasis Xen di atas. Misalnya, keluarga Instance = m3.

Langkah 2: Migrasikan instance berbasis Xen ke tipe instans berbasis Nitro

Instans yang berjalan di Host Khusus berbasis Xen juga berbasis Xen. Anda harus memigrasikan instans ini ke tipe instans berbasis Nitro sebelum dapat memindahkannya ke Host Khusus berbasis Nitro.

> **Important**
>
> Sebelum Anda mulai memigrasikan instans Anda, kami sarankan Anda mencadangkan data Anda. Untuk informasi selengkapnya, lihat Membuat snapshot Amazon EBS multi-volume dari instans Amazon EC2.

Untuk menemukan instans yang berjalan di Host Khusus berbasis Xen

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Pilih host berbasis Xen yang ingin Anda migrasikan dan kemudian pilih tab Running instance. Tab mencantumkan semua instance yang berjalan dari host yang dipilih.

Untuk memigrasikan instance Linux, lihat. Perubahan jenis instans Amazon EC2

Untuk memigrasikan instance Windows, lihat. Migrasikan instans Windows EC2 ke tipe instans berbasis Nitro

> **Note**
>
> Pastikan Anda memigrasikan instans ke jenis instans yang cocok dengan Host Khusus berbasis Nitro yang ingin Anda migrasi. Misalnya, jika Anda ingin bermigrasi ke Host Khusus M7i, pastikan Anda memigrasikan instans ke jenis instans M7i.

Langkah 3: Alokasikan Host Khusus Berbasis Nitro

Untuk menemukan Host Khusus Berbasis Nitro yang didukung

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Jenis Instance.
3. Terapkan filter berikut:
   - Hypervisor = nitro
   - Dukungan Host Khusus = benar

Setelah Anda menemukan jenis instans berbasis Nitro yang sesuai, alokasikan Host Khusus baru.

Langkah 4: Pindahkan instance yang dimigrasi ke Host Khusus berbasis Nitro baru

Setelah mengalokasikan Host Khusus berbasis Nitro dan mencapai `available` status, Anda dapat memindahkan instance yang sebelumnya Anda migrasi ke jenis instans berbasis Nitro ke Host Khusus yang baru.

Untuk memindahkan instans Anda ke Host Khusus berbasis Nitro yang baru

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, Instance.
3. Pilih instance yang dimigrasikan dan pilih Tindakan, Pengaturan instans, Ubah penempatan instans.
4. Untuk host khusus Target, pilih Host Khusus berbasis Nitro yang baru, lalu pilih Simpan.
5. Mulai ulang instans. Pilih instance dan pilih Instance state, Start instance.

Langkah 5: Lepaskan Host Khusus berbasis Xen yang tidak terpakai

Setelah Anda memigrasikan beban kerja Anda dari Host Khusus berbasis Xen ke Host Khusus berbasis Nitro yang baru, Anda dapat merilis Host Khusus berbasis Xen jika Anda tidak lagi membutuhkannya.

Beli Reservasi Tuan Rumah Khusus untuk diskon tagihan Host Khusus

Reservasi Tuan Rumah Khusus memberi Anda diskon hingga 70 persen dibandingkan dengan harga Tuan Rumah Khusus Sesuai Permintaan. Anda harus memiliki Dedicated Host aktif yang

dialokasikan di akun Anda sebelum dapat membeli Reservasi Tuan Rumah Terdedikasi. Untuk informasi selengkapnya, lihat Reservasi Host Khusus.

Console

Untuk membeli reservasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Host Khusus, Reservasi Host Khusus, Beli Reservasi Host Khusus.
3. Pada layar Temukan penawaran, lakukan hal berikut:
   a. Untuk keluarga Instans, pilih keluarga instans dari Host Khusus untuk membeli Reservasi Tuan Rumah Khusus.
   b. Untuk opsi Pembayaran, pilih dan konfigurasikan opsi pembayaran pilihan Anda.
4. Pilih Berikutnya.
5. Pilih Host Khusus untuk mengaitkan Reservasi Tuan Rumah Khusus, lalu pilih Berikutnya.
6. (Opsional) Tetapkan tag ke Reservasi Tuan Rumah Khusus.
7. Tinjau pesanan Anda dan pilih Pembelian.

AWS CLI

Untuk membeli reservasi

1. Gunakan describe-host-reservation-offeringsperintah untuk membuat daftar penawaran yang tersedia yang sesuai dengan kebutuhan Anda. Contoh berikut menampilkan daftar penawaran yang mendukung instans di keluarga instans `m4` dan memiliki jangka waktu satu tahun.

   Jangka waktu ditentukan dalam hitungan detik. Jangka waktu satu tahun mencakup 31.536.000 detik, dan jangka waktu tiga tahun mencakup 94.608.000 detik.

   ```
   aws ec2 describe-host-reservation-offerings \
       --filter Name=instance-family,Values=m4 \
       --max-duration 31536000
   ```

   Perintah menampilkan daftar penawaran yang sesuai dengan kriteria Anda. Catat ID penawaran untuk dibeli.

2. Gunakan purchase-host-reservationperintah untuk membeli penawaran dan berikan yang `offeringId` disebutkan di langkah sebelumnya. Contoh berikut membeli reservasi yang ditentukan dan mengaitkannya dengan Host Khusus tertentu yang sudah dialokasikan di AWS akun, dan menerapkan tag dengan kunci `purpose` dan nilai. `production`

```
aws ec2 purchase-host-reservation \
    --offering-id hro-03f707bf363b6b324 \
    --host-id-set h-013abcd2a00cbd123 \
    --tag-specifications 'ResourceType=host-
reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

Untuk membeli reservasi

1. Gunakan Get-EC2HostReservationOfferingcmdlet untuk membuat daftar penawaran yang tersedia yang sesuai dengan kebutuhan Anda. Contoh berikut mencantumkan penawaran yang mendukung instans di keluarga instans `m5` dan memiliki jangka waktu satu tahun.

   Jangka waktu ditentukan dalam hitungan detik. Jangka waktu satu tahun mencakup 31.536.000 detik, dan jangka waktu tiga tahun mencakup 94.608.000 detik.

```
$filter = @{Name="instance-family"; Values="m5"}
Get-EC2HostReservationOffering `
    -Filter $filter `
    -MaxDuration 31536000
```

   Perintah menampilkan daftar penawaran yang sesuai dengan kriteria Anda. Catat ID penawaran untuk dibeli.

2. Gunakan New-EC2HostReservationcmdlet untuk membeli penawaran dan memberikan ID penawaran yang tercantum pada langkah sebelumnya. Contoh berikut membeli reservasi yang ditentukan dan mengaitkannya dengan Host Khusus tertentu yang sudah dialokasikan di AWS akun.

```
New-EC2HostReservation `
    -OfferingId hro-03f707bf363b6b324 `
    -HostIdSet h-013abcd2a00cbd123
```

Berbagi Host Khusus Amazon EC2 lintas akun

Berbagi Host Khusus memungkinkan pemilik Host Khusus untuk berbagi Host Khusus mereka dengan AWS akun lain atau di dalam AWS organisasi. Hal ini memungkinkan Anda untuk membuat dan mengelola Host Khusus secara terpusat, dan berbagi Host Khusus di beberapa AWS akun atau di dalam AWS organisasi Anda.

Dalam model ini, AWS akun yang memiliki Host Khusus (pemilik) membagikannya dengan AWS akun lain (konsumen). Konsumen dapat meluncurkan instans ke Host Khusus yang dibagikan dengan mereka dengan cara yang sama seperti saat meluncurkan instans ke Host Khusus yang mereka alokasikan di akun mereka sendiri. Pemilik bertanggung jawab untuk mengelola Host Khusus dan instans yang mereka luncurkan ke dalamnya. Pemilik tidak dapat memodifikasi instans yang diluncurkan konsumen ke Host Khusus bersama. Konsumen bertanggung jawab untuk mengelola instans yang mereka luncurkan ke Host Khusus yang dibagikan dengan mereka. Konsumen tidak dapat melihat atau memodifikasi instans yang dimiliki oleh konsumen lain atau oleh pemilik Host Khusus, dan mereka tidak dapat memodifikasi Host Khusus yang dibagikan dengan mereka.

Pemilik Host Khusus dapat berbagi Host Khusus dengan:

- AWS Akun spesifik di dalam atau di luar AWS organisasinya
- Unit organisasi di dalam AWS organisasinya
- Seluruh AWS organisasinya

Daftar Isi

- Prasyarat untuk berbagi Host Khusus
- Batasan untuk berbagi Host Khusus
- Layanan terkait
- Berbagi di seluruh Zona Ketersediaan
- Izin Host Khusus Bersama
- Tagihan dan pengukuran
- Batas Host Khusus
- Pemulihan host dan berbagi Host Khusus
- Bagikan Host Khusus Amazon EC2 di seluruh akun AWS
- Membatalkan Bagikan Host Khusus yang dibagikan dengan akun lain AWS

- Lihat Host Khusus Amazon EC2 bersama di akun Anda AWS

Prasyarat untuk berbagi Host Khusus

- Untuk berbagi Host Khusus, Anda harus memilikinya di AWS akun Anda. Anda tidak dapat berbagi Host Khusus yang telah dibagikan dengan Anda.
- Untuk berbagi Host Khusus dengan AWS organisasi Anda atau unit organisasi di AWS organisasi Anda, Anda harus mengaktifkan berbagi dengan AWS Organizations. Untuk informasi selengkapnya, lihat Aktifkan Berbagi dengan AWS Organizations dalam Panduan Pengguna AWS RAM .

Batasan untuk berbagi Host Khusus

Anda tidak dapat membagikan Host Khusus yang telah dialokasikan untuk tipe instans berikut: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, dan `u-24tb1.metal`.

Layanan terkait

AWS Resource Access Manager

Berbagi Host Khusus terintegrasi dengan AWS Resource Access Manager (AWS RAM). AWS RAM adalah layanan yang memungkinkan Anda untuk berbagi AWS sumber daya Anda dengan AWS akun apa pun atau melalui AWS Organizations. Dengan AWS RAM, Anda berbagi sumber daya yang Anda miliki dengan membuat pembagian sumber daya. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan dibagikan. Konsumen dapat berupa AWS akun individu, atau unit organisasi atau seluruh organisasi dari AWS Organizations.

Untuk informasi selengkapnya AWS RAM, lihat Panduan AWS RAM Pengguna.

Berbagi di seluruh Zona Ketersediaan

Untuk memastikan bahwa sumber daya didistribusikan di seluruh Zona Ketersediaan untuk suatu Wilayah, kami secara independen memetakan Zona Ketersediaan ke nama untuk setiap akun . Hal ini dapat menyebabkan perbedaan penamaan Zona Ketersediaan di seluruh akun. Misalnya, Availability Zone `us-east-1a` untuk AWS akun Anda mungkin tidak memiliki lokasi yang sama dengan AWS akun lain. `us-east-1a`

Untuk mengidentifikasi lokasi Host Khusus Anda yang terkait dengan akun Anda, Anda harus menggunakan ID Zona Ketersediaan (AZ ID). ID Availability Zone adalah pengidentifikasi unik

dan konsisten untuk Availability Zone di semua AWS akun. Misalnya, `use1-az1` adalah ID Zona Ketersediaan untuk Wilayah `us-east-1` dan lokasinya sama di setiap akun AWS .

Untuk melihat Availability Zone IDs untuk Availability Zone di akun Anda

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/rumah.
2. Availability Zone IDs untuk Region saat ini ditampilkan di panel ID AZ Anda di sisi kanan layar.

Izin Host Khusus Bersama

Izin untuk pemilik

Pemilik bertanggung jawab untuk mengelola Host Khusus bersama dan instans yang mereka luncurkan ke dalamnya. Pemilik dapat melihat semua instans yang berjalan di Host Khusus bersama, termasuk yang diluncurkan oleh konsumen. Namun, pemilik tidak dapat mengambil tindakan apa pun untuk menjalankan instans yang diluncurkan oleh konsumen.

Izin untuk konsumen

Konsumen bertanggung jawab untuk mengelola instans yang mereka luncurkan ke Host Khusus bersama. Konsumen tidak dapat mengubah Host Khusus bersama dengan cara apa pun, dan mereka tidak dapat melihat atau memodifikasi instans yang diluncurkan oleh konsumen lain atau pemilik Host Khusus.

Tagihan dan pengukuran

Tidak ada biaya tambahan untuk berbagi Host Khusus.

Pemilik ditagih untuk Host Khusus yang mereka bagikan. Konsumen tidak akan ditagih untuk instans yang mereka luncurkan ke Host Khusus bersama.

Reservasi Host Khusus terus memberikan diskon penagihan untuk Host Khusus bersama. Hanya pemilik Host Khusus yang dapat membeli Reservasi Host Khusus untuk Host Khusus bersama yang mereka miliki.

Batas Host Khusus

Host Khusus Bersama dihitung dalam batas Host Khusus pemilik saja. Batas Host Khusus konsumen tidak terpengaruh oleh Host Khusus yang telah dibagikan dengan mereka. Demikian pula, instans

yang diluncurkan konsumen ke Host Khusus bersama tidak diperhitungkan dalam batas instans mereka.

Pemulihan host dan berbagi Host Khusus

Pemulihan host memulihkan instans yang diluncurkan oleh pemilik Host Khusus dan konsumen yang telah membagikannya. Host Khusus pengganti dialokasikan ke akun pemilik. Ini ditambahkan ke sumber daya yang sama dengan Host Khusus asli, dan dibagikan dengan konsumen yang sama.

Untuk informasi selengkapnya, lihat Pemulihan Host Khusus Amazon EC2.

Bagikan Host Khusus Amazon EC2 di seluruh akun AWS

Saat pemilik membagikan Host Khusus, konsumen akan dapat meluncurkan instans di host. Konsumen dapat meluncurkan sebanyak mungkin instans ke host bersama sesuai kapasitas yang tersedia.

> **Important**
>
> Perhatikan bahwa Anda bertanggung jawab untuk memastikan bahwa Anda memiliki hak lisensi yang sesuai untuk membagikan lisensi BYOL apa pun pada Host Khusus Anda.

Jika Anda berbagi Host Khusus dengan penempatan otomatis diaktifkan, perhatikan hal berikut karena dapat menyebabkan penggunaan Host Khusus yang tidak diinginkan:

- Jika konsumen meluncurkan instans dengan penghunian Host Khusus dan mereka tidak memiliki kapasitas pada Host Khusus yang mereka miliki di akun mereka, instans tersebut secara otomatis diluncurkan ke Host Khusus bersama.

Untuk membagikan Host Khusus, Anda harus menambahkannya ke berbagi sumber daya. Berbagi sumber daya adalah AWS RAM sumber daya yang memungkinkan Anda berbagi sumber daya di seluruh AWS akun. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan berbagi dengan mereka. Anda dapat menambahkan Host Khusus ke sumber daya yang ada, atau Anda dapat menambahkannya ke berbagi sumber daya baru.

Jika Anda adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, konsumen di organisasi Anda secara otomatis diberikan akses ke Host Khusus bersama. Jika tidak, konsumen menerima undangan untuk bergabung dengan berbagi sumber daya dan diberikan akses ke Host Khusus bersama setelah menerima undangan.

> **Note**
>
> Setelah Anda membagikan Host Khusus, konsumen mungkin perlu waktu beberapa menit untuk dapat mengaksesnya.

Console

Untuk membagikan Host Khusus yang Anda miliki menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Pilih Host Khusus untuk berbagi dan pilih Tindakan, Bagikan host.
4. Pilih berbagi sumber daya yang ingin ditambahkan Host Khusus dan pilih Bagikan host.

   Butuh beberapa menit bagi konsumen untuk mendapatkan akses ke host bersama.

Untuk berbagi Host Khusus yang Anda miliki menggunakan AWS RAM konsol

Lihat Membuat berbagi sumber daya di Panduan AWS RAM Pengguna.

AWS CLI

Untuk berbagi Host Khusus yang Anda miliki

Gunakan perintah create-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE
```

PowerShell

Untuk berbagi Host Khusus yang Anda miliki

Gunakan cmdlet New- RAMResource Share.

```
New-RAMResourceShare `
    -Name my-resource-share `
```

```
    -ResourceArn arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE
```

Membatalkan Bagikan Host Khusus yang dibagikan dengan akun lain AWS

Pemilik Host Khusus dapat membatalkan pembagian Host Khusus bersama kapan saja. Saat Anda membatalkan berbagi Host Khusus bersama, aturan berikut ini berlaku:

- Konsumen yang dibagikan Host Khusus tidak lagi dapat meluncurkan instans baru ke dalamnya.
- Instans yang dimiliki oleh konsumen yang berjalan pada Host Khusus pada waktu pembatalan pembagian terus berjalan, tetapi dijadwalkan untuk pensiun. Konsumen menerima notifikasi pensiun untuk instans tersebut dan mereka memiliki waktu dua minggu untuk mengambil tindakan atas notifikasi tersebut. Namun, jika Host Khusus dibagikan ulang dengan konsumen dalam periode pemberitahuan pensiun, pensiun instans dibatalkan.

Untuk membatalkan berbagi Host Khusus bersama yang Anda miliki, Anda harus menghapusnya dari berbagi sumber daya.

Console

Untuk membatalkan berbagi Host Khusus bersama yang Anda miliki

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Pilih Host Khusus yang batal dibagikan dan pilih tab Berbagi.
4. Tab Berbagi mencantumkan sumber daya yang telah ditambahkan Host Khusus. Pilih bagian sumber daya untuk menghapus Host Khusus dan pilih Hapus host dari berbagi sumber daya.

Untuk membatalkan berbagi Host Khusus bersama yang Anda miliki menggunakan konsol AWS RAM

Lihat Memperbarui bagian sumber daya di Panduan AWS RAM Pengguna.

AWS CLI

Untuk membatalkan berbagi Host Khusus bersama yang Anda miliki

Gunakan perintah disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
 --resource-arns arn:aws:ec2:us-east-2:123456789012:dedicated-host/h-07879acf49EXAMPLE
```

PowerShell

Untuk membatalkan berbagi Host Khusus bersama yang Anda miliki

Gunakan cmdlet Putus- RAMResource Bagikan.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:dedicated-host/h-07879acf49EXAMPLE"
```

Lihat Host Khusus Amazon EC2 bersama di akun Anda AWS

Anda dapat melihat Host Khusus yang Anda bagikan dengan akun lain, dan Host Khusus yang dibagikan dengan Anda. Jika Anda memiliki Host Khusus, Anda dapat melihat semua instans berjalan di host, termasuk instans yang diluncurkan oleh konsumen. Jika Host Khusus dibagikan dengan Anda, Anda hanya dapat melihat instans yang Anda luncurkan ke host bersama, dan bukan yang diluncurkan oleh konsumen lain.

Pemilik dan konsumen dapat mengidentifikasi Host Khusus bersama menggunakan salah satu metode berikut.

Console

Untuk mengidentifikasi Host Khusus bersama

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus. Layar mencantumkan Host Khusus yang Anda miliki dan Host Khusus yang dibagikan dengan Anda.
3. Kolom Pemilik menunjukkan ID akun AWS dari pemilik Host Khusus.
4. Untuk melihat instance yang berjalan di host, pilih tab Instances.

AWS CLI

Untuk mengidentifikasi Host Khusus bersama

Gunakan perintah describe-host. Perintah tersebut menampilkan Host Khusus yang Anda miliki dan Host Khusus yang dibagikan dengan Anda. Nilai `Owner` adalah ID akun pemilik Host Khusus. `Instances`Daftar ini menjelaskan instance yang berjalan di host.

```
aws ec2 describe-hosts --filter "Name=state,Values=available"
```

PowerShell

Untuk mengidentifikasi Host Khusus bersama

Gunakan Get- EC2host cmdlet. Cmdlet mengembalikan Host Khusus yang Anda miliki dan Host Khusus yang dibagikan dengan Anda. Nilai `Owner` dalam respons adalah ID akun pemilik Host Khusus. `Instances`Daftar ini menjelaskan instance yang berjalan di host.

```
Get-EC2Host -Filter @{Name="state"; Values="available"}
```

Host Khusus Amazon EC2 di AWS Outposts

AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, layanan APIs, dan alat ke tempat Anda. Dengan menyediakan akses lokal ke infrastruktur AWS terkelola, AWS Outposts memungkinkan Anda untuk membangun dan menjalankan aplikasi di tempat menggunakan antarmuka pemrograman yang sama seperti di AWS Wilayah, sambil menggunakan sumber daya komputasi dan penyimpanan lokal untuk latensi yang lebih rendah dan kebutuhan pemrosesan data lokal.

Outpost adalah kumpulan kapasitas AWS komputasi dan penyimpanan yang digunakan di situs pelanggan. AWS mengoperasikan, memantau, dan mengelola kapasitas ini sebagai bagian dari suatu AWS Wilayah.

Anda dapat mengalokasikan Host Khusus di Outposts yang Anda miliki di akun Anda. Ini memudahkan Anda untuk membawa lisensi perangkat lunak dan beban kerja yang ada yang memerlukan server fisik khusus ke AWS Outposts. Anda juga dapat menargetkan aset perangkat keras tertentu di Outpost untuk membantu meminimalkan latensi di antara beban kerja Anda.

Host Khusus memungkinkan Anda untuk menggunakan lisensi perangkat lunak yang memenuhi syarat di Amazon EC2, sehingga Anda mendapatkan fleksibilitas dan efektivitas biaya menggunakan

lisensi Anda sendiri. Lisensi perangkat lunak lain yang terikat pada mesin virtual, soket, atau inti fisik, juga dapat digunakan pada Host Khusus, tunduk pada persyaratan lisensi mereka. Meskipun Outposts selalu menjadi lingkungan penghunian tunggal yang memenuhi syarat untuk beban kerja BYOL, Host Khusus memungkinkan Anda membatasi lisensi yang diperlukan untuk satu host dibandingkan dengan deployment seluruh Outpost.

Selain itu, menggunakan Host Khusus di Outpost memberi Anda fleksibilitas yang lebih besar dalam deployment tipe instans, dan kontrol yang lebih terperinci atas penempatan instans. Anda dapat menargetkan host tertentu untuk peluncuran instans dan menggunakan afinitas host untuk memastikan bahwa instans selalu berjalan pada host tersebut, atau Anda dapat menggunakan penempatan otomatis untuk meluncurkan instans ke host mana pun yang tersedia yang memiliki konfigurasi dan ketersediaan kapasitas yang cocok.

Daftar Isi

- Prasyarat
- Fitur yang didukung
- Pertimbangan
- Mengalokasikan Host Khusus Amazon EC2 di AWS Outposts

Prasyarat

Anda harus menginstal Outpost di situs Anda. Untuk informasi selengkapnya, lihat Membuat Outpost dan memesan kapasitas Outpost di Panduan Pengguna AWS Outposts .

Fitur yang didukung

- Contoh keluarga berikut didukung:
  - Tujuan umum: M5 | M5d | M7i | M8i
  - Komputasi dioptimalkan: C5 | C5d | C7i | C8i
  - Memori dioptimalkan: R5 | R5d | R7i | R8i
  - Penyimpanan dioptimalkan: i3en
  - Komputasi yang dipercepat: G4dn
- Host Khusus di Outposts dapat dikonfigurasi untuk mendukung beberapa ukuran instans. Support untuk beberapa ukuran instans tersedia untuk keluarga instance berikut.
  - Tujuan umum: M5 | M5d | M7i
  - Komputasi dioptimalkan: C5 | C5d | C7i

  - Memori dioptimalkan: R5 | R5d | R7i

  Untuk informasi selengkapnya, lihat Konfigurasi kapasitas instans Host Khusus Amazon EC2.
- Host Khusus di Outposts mendukung penempatan otomatis dan peluncuran instans tertarget. Untuk informasi selengkapnya, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.
- Host Khusus di Outposts mendukung afinitas host. Untuk informasi selengkapnya, lihat Penempatan otomatis Host Khusus Amazon EC2 dan afinitas host.
- Host Khusus di Outposts mendukung berbagi dengan. AWS RAM Untuk informasi selengkapnya, lihat Berbagi Host Khusus Amazon EC2 lintas akun.

Pertimbangan

- Reservasi Host Khusus tidak didukung di Outposts.
- Host grup sumber daya dan tidak AWS License Manager didukung di Outposts.
- Host Khusus di Outposts tidak mendukung instans T3 yang dapat melonjak.
- Host Khusus di Outposts tidak mendukung pemulihan host.
- Pemulihan otomatis yang disederhanakan tidak didukung untuk instance dengan penyewaan Host Khusus di Outposts.

Mengalokasikan Host Khusus Amazon EC2 di AWS Outposts

Anda mengalokasikan dan menggunakan Host Khusus di Outposts dengan cara yang sama dengan Host Khusus di Wilayah AWS .

Prasyarat

Buat subnet pada Outpost. Untuk informasi selengkapnya, lihat Membuat subnet di Panduan Pengguna AWS Outposts .

Untuk mengalokasikan Host Khusus di Outpost, gunakan salah satu metode berikut:

Console

Untuk mengalokasikan Host Khusus di Outpost menggunakan konsol AWS Outposts

1. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.

2. Di panel navigasi, pilih Outposts. Pilih Outpost kemudian pilih Tindakan, Alokasikan Host Khusus.
3. Konfigurasikan Host Khusus sesuai kebutuhan. Untuk informasi selengkapnya, lihat Alokasikan Host Khusus Amazon EC2 untuk digunakan di akun Anda.

> **Note**
>
> Zona Ketersediaan dan ARN Outpost harus diisi sebelumnya dengan Zone Ketersediaan dan ARN dari Outpost yang dipilih.

4. Pilih Alokasikan.

Untuk mengalokasikan Host Khusus di Pos Luar menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus, lalu pilih Alokasi Host Khusus.
3. Untuk Zona Ketersediaan, pilih Zona Ketersediaan yang terkait dengan Outpost.
4. Untuk ARN Outpost masukkan ARN Outpost.
5. Untuk menargetkan aset perangkat keras tertentu di Outpost, pada Menargetkan aset perangkat keras tertentu di Outpost, pilih Aktifkan. Untuk setiap aset perangkat keras yang ditargetkan, pilih Tambahkan ID aset, lalu masukkan ID aset perangkat keras.

> **Note**
>
> Nilai yang Anda tentukan untuk Kuantitas harus sama dengan jumlah aset IDs yang Anda tentukan. Misalnya, jika Anda menentukan 3 aset IDs, maka Kuantitas juga harus 3.

6. Konfigurasikan pengaturan Host Khusus yang tersisa sesuai kebutuhan. Untuk informasi selengkapnya, lihat Alokasikan Host Khusus Amazon EC2 untuk digunakan di akun Anda.
7. Pilih Alokasikan.

AWS CLI

Untuk mengalokasikan Host Khusus di Pos Luar

Gunakan perintah allocate-hosts. Untuk `--availability-zone`, tentukan Zona Ketersediaan yang terkait dengan Outpost. Untuk `--outpost-arn`, tentukan ARN dari Outpost. Secara opsional, untuk`--asset-ids`, tentukan aset perangkat keras Outpost yang akan ditargetkan. IDs

```
aws ec2 allocate-hosts \
    --availability-zone "us-east-1a" \
    --outpost-arn "arn:aws:outposts:us-east-1a:111122223333:outpost/
op-4fe3dc21baEXAMPLE" \
    --asset-ids asset_id \
    --instance-family "m5" \
    --auto-placement "off" \
    --quantity 1
```

PowerShell

Untuk mengalokasikan Host Khusus di Pos Luar

Gunakan New-EC2Hostcmdlet. Tentukan Availability Zone yang terkait dengan Outpost. Secara opsional, untuk`-AssetId`, tentukan aset perangkat keras Outpost yang akan ditargetkan. IDs

```
New-EC2Host `
    -AvailabilityZone "us-east-1a" `
    -OutpostArn "arn:aws:outposts:us-east-1a:111122223333:outpost/
op-4fe3dc21baEXAMPLE" `
    -AssetId asset_id `
    -InstanceFamily "m5" `
    -AutoPlacement "off" `
    -Quantity 1
```

Untuk meluncurkan sebuah instans ke Host Khusus di Outpost

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus. Pilih Host Khusus yang Anda alokasikan pada langkah sebelumnya dan pilih Actions, Launch instans ke host.
3. Konfigurasikan instans sesuai kebutuhan kemudian luncurkan instans. Untuk informasi selengkapnya, lihat Luncurkan instans Amazon EC2 di Host Khusus Amazon EC2.

Pemulihan Host Khusus Amazon EC2

Pemulihan otomatis Host Khusus memulai ulang instans Anda ke host pengganti baru saat kondisi bermasalah tertentu terdeteksi di Host Khusus Anda. Pemulihan host mengurangi kebutuhan akan intervensi manual dan menurunkan beban operasional jika ada kegagalan Host Khusus yang tidak terduga terkait daya sistem atau peristiwa konektivitas jaringan. Masalah Host Khusus lainnya akan memerlukan intervensi manual dalam pemulihannya.

Daftar Isi

- Cara kerja pemulihan Host Khusus Amazon EC2
- Jenis instans Supportyang didukung
- Harga
- Kelola pemulihan Host Khusus Amazon EC2
- Lihat pengaturan pemulihan host untuk Host Khusus Amazon EC2 Anda
- Memulihkan instans yang tidak didukung oleh pemulihan Host Khusus Amazon EC2 secara manual

Cara kerja pemulihan Host Khusus Amazon EC2

Host Khusus dan proses pemulihan grup sumber daya host menggunakan pemeriksaan kondisi tingkat host untuk menilai ketersediaan Host Khusus dan untuk mendeteksi kegagalan sistem dasar. Tipe kegagalan Host Khusus menentukan apakah pemulihan otomatis Host Khusus dimungkinkan. Contoh masalah yang dapat menyebabkan pemeriksaan kondisi tingkat host gagal meliputi:

- Hilangnya konektivitas jaringan
- Hilangnya daya sistem
- Masalah perangkat keras atau perangkat lunak pada host fisik

> **Important**
>
> Pemulihan otomatis Host Khusus tidak terjadi ketika host dijadwalkan pensiun.

Pemulihan otomatis Host Khusus

Ketika daya sistem atau kegagalan konektivitas jaringan terdeteksi pada Host Khusus Anda, pemulihan otomatis Host Khusus dimulai dan Amazon EC2 secara otomatis mengalokasikan Host Khusus pengganti di Zona Ketersediaan yang sama dengan Host Khusus asli. Host Khusus pengganti menerima ID host baru, tetapi mempertahankan atribut yang sama dengan Host Khusus yang asli, termasuk:

- Zona Ketersediaan
- Jenis instans
- Tag
- Pengaturan penempatan otomatis
- Reservasi

Saat Host Khusus pengganti dialokasikan, instans dipulihkan ke Host Khusus pengganti. Instans yang dipulihkan mempertahankan atribut yang sama dengan instans asli, termasuk:

- ID Instans
- Alamat IP privat
- Alamat IP elastic
- Lampiran volume EBS
- Semua metadata instans

Selain itu, integrasi bawaan dengan AWS License Manager mengotomatiskan pelacakan dan pengelolaan lisensi Anda.

> **Note**
>
> AWS Integrasi License Manager hanya didukung di Wilayah di mana AWS License Manager tersedia.

Jika instans memiliki hubungan afinitas host dengan Host Khusus yang terganggu, instans yang dipulihkan membentuk afinitas host dengan Host Khusus pengganti.

Jika semua instans telah dipulihkan ke Host Khusus pengganti, Host Khusus yang terganggu akan dilepas, dan Host Khusus pengganti tersedia untuk digunakan.

Ketika pemulihan host dimulai, pemilik AWS akun diberitahu melalui email dan oleh suatu Dasbor AWS Health acara. Notifikasi kedua dikirimkan setelah pemulihan host berhasil diselesaikan.

Jika Anda menggunakan AWS License Manager untuk melacak lisensi Anda, AWS License Manager mengalokasikan lisensi baru untuk penggantian Host Khusus berdasarkan batas konfigurasi lisensi. Jika konfigurasi lisensi memiliki batas keras yang akan dilanggar sebagai akibat dari pemulihan host, proses pemulihan tidak diperbolehkan dan Anda diberitahu tentang kegagalan pemulihan host melalui pemberitahuan Amazon SNS (jika pengaturan pemberitahuan telah dikonfigurasi untuk License AWS Manager). Jika konfigurasi lisensi memiliki batas lunak yang akan dilanggar sebagai akibat dari pemulihan host, pemulihan diizinkan untuk dilanjutkan dan Anda diberi tahu tentang pelanggaran batas melalui notifikasi Amazon SNS. Untuk informasi selengkapnya, lihat Menggunakan Konfigurasi Lisensi dan Pengaturan di License Manager di Panduan Pengguna AWS License Manager.

Status pemulihan host

Saat kegagalan Host Khusus terdeteksi, Host Khusus yang terganggu memasuki status `under-assessment`, dan semua instance masuk ke status `impaired`. Anda tidak dapat meluncurkan instans ke Host Khusus yang rusak saat berada dalam status `under-assessment`.

Setelah Host Khusus pengganti dialokasikan, host memasuki status `pending`. Statusnya tidak berubah sampai proses pemulihan host selesai. Anda tidak dapat meluncurkan instans ke Host Khusus pengganti saat berada dalam status `pending`. Instans yang dipulihkan pada Host Khusus pengganti tetap berada dalam status `impaired` selama proses pemulihan.

Setelah pemulihan host selesai, Host Khusus pengganti memasuki status `available`, dan instans yang dipulihkan kembali ke status `running`. Anda dapat meluncurkan instans ke Host Khusus pengganti setelah instans berada dalam status `available`. Host Khusus yang mengalami gangguan dilepas secara permanen dan masuk dalam status `released-permanent-failure`.

Jika Host Khusus yang mengalami gangguan memiliki instance yang tidak mendukung pemulihan host, seperti instance dengan volume root penyimpanan instans, Host Khusus tidak akan dirilis. Sebaliknya, host ditandai untuk pensiun dan memasuki status `permanent-failure`.

Skenario tanpa pemulihan otomatis Host Khusus

Pemulihan otomatis Host Khusus tidak terjadi ketika host dijadwalkan pensiun. Anda akan menerima pemberitahuan pensiun di Dasbor AWS Health CloudWatch acara Amazon, dan alamat email pemilik

AWS akun menerima pesan mengenai kegagalan Host Khusus. Ikuti langkah-langkah perbaikan yang dijelaskan dalam notifikasi pensiun dalam jangka waktu yang ditentukan untuk secara manual memulihkan instans pada host yang pensiun.

Instans yang dihentikan tidak dipulihkan ke Host Khusus pengganti. Jika Anda mencoba untuk memulai contoh instans yang berhenti yang menargetkan Host Khusus yang terganggu, instans akan mulai gagal. Kami menyarankan Anda mengubah instans yang dihentikan untuk menargetkan Host Khusus yang berbeda, atau untuk meluncurkan pada Host Khusus apa pun yang tersedia dengan konfigurasi yang cocok dan penempatan otomatis diaktifkan.

Instans dengan penyimpanan instans tidak dipulihkan ke Host Khusus pengganti. Sebagai langkah perbaikan, Host Khusus yang mengalami gangguan ditandai untuk pensiun dan Anda akan menerima notifikasi pensiun setelah pemulihan host selesai. Ikuti langkah-langkah perbaikan yang dijelaskan dalam notifikasi pensiun dalam jangka waktu yang ditentukan untuk secara manual memulihkan instans yang tersisa pada Host Khusus yang terganggu.

Jenis instans Supportyang didukung

Pemulihan host didukung untuk keluarga contoh berikut:

- Tujuan umum: A1 | M3 | M4 | M5 | M5n | M5Zn | M6a | M6g | M6i | T3 | Mac1 | Mac2 | Mac2-M1Ultra | Mac2-m2 | Mac2-M2Pro
- Komputasi dioptimalkan: C3 | C4 | C5 | C5n | C6a | C6g | C6i
- Memori dioptimalkan: R3 | R4 | R5 | R5b | R5n | R6g | R6i | U-6TB1 | U-9TB1 | U-12TB1 | U-18TB1 | U-24TB1 | X1 | X1e | x2IEZN
- Komputasi yang dipercepat: Inf1 | G3 | G5g | P2 | P3

Untuk memulihkan instans yang tidak didukung, lihat Memulihkan instans yang tidak didukung oleh pemulihan Host Khusus Amazon EC2 secara manual.

> **Note**
>
> Pemulihan otomatis Host khusus untuk tipe instans metal yang didukung akan membutuhkan waktu lebih lama untuk mendeteksi dan memulihkan dari tipe instans nonmetal.

Harga

Tidak ada biaya tambahan untuk menggunakan pemulihan host, tetapi biaya Host Khusus yang biasa berlaku. Untuk informasi selengkapnya, lihat Harga Host Khusus Amazon EC2.

Segera setelah pemulihan host dimulai, Anda tidak lagi ditagih untuk Host Khusus yang terganggu. Tagihan untuk Host Khusus pengganti dimulai hanya setelah host masuk dalam status `available`.

Jika Host Khusus yang terganggu ditagih menggunakan tarif Sesuai Permintaan, Host Khusus pengganti juga akan ditagih menggunakan tarif Sesuai Permintaan. Jika Host Khusus yang mengalami gangguan memiliki Reservasi Host Khusus yang aktif, Host Khusus tersebut akan ditransfer ke Host Khusus pengganti.

Kelola pemulihan Host Khusus Amazon EC2

Pemulihan otomatis Host Khusus memulai ulang instans Anda ke host pengganti baru saat kondisi bermasalah tertentu terdeteksi di Host Khusus Anda. Anda dapat mengaktifkan pemulihan host ketika Anda mengalokasikan Host Khusus atau setelah alokasi.

Gunakan prosedur berikut untuk mengaktifkan pemulihan host saat mengalokasikan host.

Console

Untuk mengaktifkan pemulihan host pada alokasi

Saat mengalokasikan Host Khusus menggunakan konsol Amazon EC2, untuk pemulihan Host, pilih Aktifkan. Untuk informasi selengkapnya, lihat Alokasikan Host Khusus Amazon EC2 untuk digunakan di akun Anda.

AWS CLI

Untuk mengaktifkan pemulihan host pada alokasi

Gunakan perintah allocate-hosts.

```
aws ec2 allocate-hosts \
    --instance-type m5.large \
    --availability-zone eu-west-1a \
    --auto-placement on \
    --host-recovery on \
    --quantity 1
```

PowerShell

Untuk mengaktifkan pemulihan host pada alokasi

Gunakan New-EC2Hostcmdlet.

```
New-EC2Host `
    -InstanceType m5.large `
    -AvailabilityZone eu-west-1a `
    -AutoPlacement on `
    -HostRecovery on `
    -Quantity 1
```

Gunakan prosedur berikut untuk mengelola pemulihan host untuk Host Khusus.

Console

Untuk mengelola pemulihan host setelah alokasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Pilih Host Khusus.
4. Pilih Tindakan, Ubah host.
5. Untuk pemulihan Host, pilih atau hapus Aktifkan.
6. Pilih Simpan.

AWS CLI

Untuk mengaktifkan pemulihan host setelah alokasi

Gunakan perintah modify-hosts.

```
aws ec2 modify-hosts \
    --host-recovery on \
    --host-ids h-012a3456b7890cdef
```

Untuk menonaktifkan pemulihan host setelah alokasi

Gunakan perintah modify-hosts dan tentukan `host-recovery` parameter dengan nilai. `off`

```
aws ec2 modify-hosts \
    --host-recovery off \
    --host-ids h-012a3456b7890cdef
```

PowerShell

Untuk mengaktifkan pemulihan host setelah alokasi

Gunakan cmdlet Edit-host.

```
Edit-EC2Host `
    -HostRecovery on `
    -HostId h-012a3456b7890cdef
```

Untuk menonaktifkan pemulihan host setelah alokasi

Gunakan Edit-EC2Hostcmdlet.

```
Edit-EC2Host `
    -HostRecovery off `
    -HostId h-012a3456b7890cdef
```

Lihat pengaturan pemulihan host untuk Host Khusus Amazon EC2 Anda

Anda dapat melihat konfigurasi pemulihan host untuk Host Khusus kapan saja.

Console

Untuk melihat konfigurasi pemulihan host untuk Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Pilih Host Khusus, dan di tab Deskripsi, tinjau bidang Pemulihan Host.

AWS CLI

Untuk melihat konfigurasi pemulihan host untuk Host Khusus

Gunakan perintah describe-host.

```
aws ec2 describe-hosts \
    --host-ids h-012a3456b7890cdef \
    --query Hosts[].HostRecovery
```

Berikut ini adalah output contoh.

```
on
```

PowerShell

Untuk melihat konfigurasi pemulihan host untuk Host Khusus

Gunakan Get-EC2Hostcmdlet.

```
(Get-EC2Host -HostId h-012a3456b7890cdef).Hosts | Select HostRecovery
```

Berikut ini adalah output contoh.

```
HostRecovery
------------
on
```

Memulihkan instans yang tidak didukung oleh pemulihan Host Khusus Amazon EC2 secara manual

Pemulihan host tidak mendukung pemulihan instans yang menggunakan volume penyimpanan instans. Ikuti petunjuk di bawah ini untuk secara manual memulihkan semua instans Anda yang tidak dapat dipulihkan secara otomatis.

> **Warning**
>
> Data pada volume penyimpanan instans hilang saat instans dihentikan, dihibernasi, atau diakhiri. Ini termasuk volume penyimpanan instance yang dilampirkan ke instance yang memiliki volume root EBS. Untuk melindungi data dari volume penyimpanan instans, cadangkan ke penyimpanan persisten sebelum instans dihentikan atau diakhiri.

Memulihkan instans yang didukung EBS secara manual

Untuk instans yang didukung EBS yang tidak dapat dipulihkan secara otomatis, kami menyarankan Anda untuk menghentikan dan memulai instans secara manual untuk memulihkannya ke Host Khusus yang baru. Untuk informasi selengkapnya tentang menghentikan instans Anda, dan tentang perubahan yang terjadi dalam konfigurasi instans Anda saat dihentikan, lihat Hentikan dan mulai instans Amazon EC2.

Pulihkan instance secara manual dengan volume root penyimpanan instance

Untuk contoh dengan volume root penyimpanan instance yang tidak dapat dipulihkan secara otomatis, kami sarankan Anda melakukan hal berikut:

1. Luncurkan instans pengganti pada Host Khusus baru dari AMI terbaru Anda.
2. Migrasikan semua data yang diperlukan ke instans pengganti.
3. Akhiri instans asli pada Host Khusus yang terganggu.

Pemeliharaan host untuk Host Khusus Amazon EC2

Dengan pemeliharaan host, jika Host Khusus mengalami degradasi, kami secara otomatis memigrasikan instans yang berjalan di atasnya ke Host Khusus pengganti yang sehat. Hal ini membantu meminimalkan waktu henti beban kerja Anda, dan menyederhanakan pengelolaan Host Khusus Anda. Pemeliharaan host juga dilakukan untuk pemeliharaan Amazon EC2 terencana dan rutin.

Amazon EC2 mendukung dua jenis pemeliharaan host:

- Pemeliharaan host migrasi langsung — Instans secara otomatis dimigrasikan ke host pengganti dalam waktu 24 jam, tanpa menghentikan dan memulai ulang.
- Pemeliharaan host berbasis reboot - Instans dijadwalkan misalnya reboot peristiwa terjadwal, di mana mereka secara otomatis dihentikan dan dimulai ulang pada host pengganti.

Daftar Isi

- Pemeliharaan host versus pemulihan host
- Pertimbangan-pertimbangan
- Layanan terkait
- Harga

- Cara kerja pemeliharaan host untuk Host Khusus Amazon EC2
- Konfigurasikan pengaturan pemeliharaan host untuk Host Khusus Amazon EC2

Pemeliharaan host versus pemulihan host

Tabel berikut menunjukkan perbedaan utama antara pemulihan host dan pemeliharaan host.

	Pemulihan host	Pemeliharaan host
Keterjangkauan instans	Tidak dapat dijangkau	Dapat dijangkau
Status Host Khusus	`under-assessment`	`permanent-failure`
Grup sumber daya tuan rumah	Didukung	Tidak didukung

Untuk informasi selengkapnya tentang pemulihan host, lihat Pemulihan host.

Pertimbangan-pertimbangan

- Pemeliharaan host tersedia di semua Wilayah AWS, kecuali Wilayah Tiongkok AWS GovCloud (US) Regions dan.
- Pemeliharaan host tidak didukung di AWS Outposts, AWS Local Zones, dan AWS Wavelength Zones.
- Pemeliharaan host tidak dapat diaktifkan atau dinonaktifkan untuk host yang sudah ada dalam grup sumber daya host. Host yang ditambahkan ke grup sumber daya host mempertahankan pengaturan pemeliharaan host-nya. Untuk informasi selengkapnya, lihat Grup sumber daya host.
- Pemeliharaan host tidak didukung dengan jenis instance berikut, karena mereka memiliki volume root penyimpanan instance: C1, C3, D2, I2, M1, M2, M3, R3, dan X1.

Layanan terkait

Host Khusus terintegrasi dengan AWS License Manager —Melacak lisensi di seluruh Host Khusus Amazon EC2 Anda (hanya didukung di Wilayah di mana AWS License Manager tersedia). Untuk informasi selengkapnya, lihat Panduan Pengguna AWS License Manager.

Anda harus memiliki lisensi yang cukup Akun AWS untuk Host Khusus Anda yang baru. Lisensi yang terkait dengan host terdegradasi Anda dirilis saat host dirilis setelah selesainya acara yang dijadwalkan.

Harga

Tidak ada biaya tambahan untuk penggunaan pemeliharaan host, tetapi biaya Host Khusus yang biasa berlaku. Untuk informasi selengkapnya, lihat Harga Host Khusus Amazon EC2.

Segera setelah pemeliharaan host dimulai, Anda tidak lagi ditagih untuk Host Khusus yang terdegradasi. Tagihan untuk Host Khusus pengganti dimulai hanya setelah host masuk dalam status `available`.

Jika Dedicated Host yang terdegradasi ditagih menggunakan tarif On-Demand, Dedicated Host pengganti juga ditagih menggunakan tarif On-Demand. Jika Host Khusus yang terdegradasi memiliki Reservasi Host Khusus yang aktif, Host Khusus tersebut akan ditransfer ke Host Khusus yang baru.

Cara kerja pemeliharaan host untuk Host Khusus Amazon EC2

Ketika degradasi terdeteksi pada Host Khusus yang diaktifkan untuk pemeliharaan host, kami secara otomatis mengalokasikan Host Khusus pengganti di akun Anda. Host Khusus pengganti menerima ID host baru, tetapi mempertahankan atribut yang sama dengan Host Khusus yang asli, termasuk:

- Pengaturan penempatan otomatis
- Zona Ketersediaan
- Asosiasi Reservasi Tuan Rumah Khusus
- Afinitas host
- Pengaturan pemeliharaan host
- Pengaturan pemulihan host
- Tipe instans
- Tag

Setelah host pengganti dialokasikan, kami memigrasikan instance menggunakan pemeliharaan host migrasi langsung atau pemeliharaan host berbasis reboot, tergantung pada instancenya.

Setelah host terdegradasi tidak memiliki instance yang berjalan lagi, host tersebut akan dirilis secara permanen dari akun Anda.

Pemeliharaan host migrasi langsung

Instans yang memerlukan pemeliharaan host migrasi langsung secara otomatis dimigrasikan ke host pengganti dalam waktu 24 jam, tanpa menghentikan dan memulai ulang. Instance yang dimigrasi mempertahankan atribut yang ada, termasuk:

- ID Instans
- Metadata instans
- Lampiran volume Amazon EBS
- Alamat IP elastis dan alamat IP pribadi
- Memori, CPU, dan status jaringan

Beberapa ukuran instans yang lebih besar mungkin mengalami sedikit penurunan kinerja selama migrasi.

Setelah instance dimigrasikan secara otomatis ke host pengganti, kami mengirimkan email dan pemberitahuan AWS Health Dasbor kepada Anda. Pemberitahuan mencakup host terdegradasi dan pengganti, informasi tentang instans yang dimigrasi secara otomatis menggunakan pemeliharaan host migrasi langsung, dan informasi tentang instans yang tersisa. IDs

Pemeliharaan host berbasis reboot

Instans yang memerlukan pemeliharaan host berbasis reboot dijadwalkan misalnya acara terjadwal reboot selama 14 hari sejak tanggal pemberitahuan. Anda dapat terus mengakses instans Anda di Host Khusus yang terdegradasi sebelum acara yang dijadwalkan.

Anda dapat menjadwal ulang acara reboot untuk tanggal yang berada dalam 7 hari dari tanggal dan waktu acara asli. Untuk informasi selengkapnya, lihat Menjadwalkan ulang acara terjadwal untuk instans EC2.

Amazon EC2 secara otomatis menyimpan kapasitas pada host pengganti untuk instans ini. Anda tidak dapat menjalankan instance dalam kapasitas cadangan ini.

Konsol Amazon EC2 menunjukkan kapasitas cadangan sebagai kapasitas yang digunakan. Tampaknya instance berjalan pada host yang terdegradasi dan host pengganti. Namun, instance akan terus berjalan hanya pada host yang terdegradasi hingga dihentikan atau dimigrasikan ke kapasitas cadangan pada host pengganti.

Pada tanggal dan waktu acara yang dijadwalkan, instans secara otomatis dihentikan dan dimulai kembali ke kapasitas cadangan pada host pengganti. Instance yang dimigrasi mempertahankan atribut yang ada, termasuk:

- ID Instans
- Metadata instans
- Lampiran volume Amazon EBS
- Alamat IP elastis dan alamat IP pribadi

Namun, karena instance dihentikan dan dimulai ulang selama migrasi, mereka tidak mempertahankan memori, CPU, dan status jaringan mereka.

Anda juga dapat menghentikan dan memulai ulang instance ini secara manual kapan saja sebelum acara yang dijadwalkan untuk memigrasikannya ke host pengganti atau ke host lain. Anda mungkin perlu memodifikasi afinitas host instans Anda untuk memulai ulang pada host yang berbeda. Jika Anda menghentikan instans sebelum acara yang dijadwalkan, kapasitas cadangan pada host pengganti dilepaskan dan tersedia untuk digunakan.

Status pemeliharaan host

Ketika tuan rumah menjadi terdegradasi, ia memasuki `permanent-failure` negara bagian. Anda tidak dapat meluncurkan instance di Host Khusus yang ada di `permanent-failure` negara bagian.

Setelah host pengganti dialokasikan, host tetap dalam `pending` status hingga instance yang mendukung pemeliharaan host migrasi langsung dimigrasikan secara otomatis dari host yang terdegradasi, dan hingga acara terjadwal dijadwalkan untuk instance yang tersisa. Setelah tugas-tugas ini selesai, host pengganti memasuki `available` negara bagian.

Setelah host pengganti memasuki `available` status, Anda dapat menggunakannya dengan cara yang sama seperti Anda menggunakan host apa pun di akun Anda. Namun, beberapa kapasitas instance pada host pengganti dicadangkan untuk instance yang memerlukan migrasi host berbasis reboot. Anda tidak dapat meluncurkan instans baru ke dalam kapasitas cadangan ini.

Ketika host terdegradasi tidak memiliki instance yang berjalan lagi, host tersebut memasuki `released, permanent-failure` status, dan secara permanen dilepaskan dari akun Anda. Perhatikan bahwa host dan sumber dayanya tetap terlihat di konsol untuk waktu yang singkat.

Migrasi otomatis

Beberapa instance tidak dapat dimigrasi secara otomatis ke host pengganti.

Instans dengan volume root yang didukung EBS

Untuk contoh ini, kami menjadwalkan acara penghentian instance selama 28 hari sejak tanggal pemberitahuan. Pada tanggal dan waktu acara yang dijadwalkan, instance dihentikan. Kami menyarankan Anda berhenti secara manual saat memulai ulang instance pada host pengganti atau pada host yang berbeda. Anda mungkin perlu memodifikasi afinitas host instans Anda untuk memulai ulang pada host yang berbeda.

Instance dengan volume root penyimpanan instance

Untuk contoh ini, kami menjadwalkan acara pensiun instance selama 28 hari sejak tanggal pemberitahuan. Pada tanggal dan waktu acara yang dijadwalkan, instance dihentikan secara permanen. Kami menyarankan Anda meluncurkan instans penggantian secara manual pada host pengganti dan kemudian memigrasikan data yang diperlukan ke instance pengganti sebelum acara yang dijadwalkan.

Contoh berikut memiliki volume root penyimpanan instance: C1, C3, D2, I2, M1, M2, M3, R3, dan X1.

Anda dapat terus mengakses instans Anda di Host Khusus yang terdegradasi sebelum acara yang dijadwalkan.

Konfigurasikan pengaturan pemeliharaan host untuk Host Khusus Amazon EC2

Aktifkan pemeliharaan host untuk memastikan bahwa instans Anda yang berjalan di Host Khusus secara otomatis dipulihkan ke Host Khusus baru selama acara pemeliharaan terjadwal.

Jika Anda menonaktifkan pemeliharaan host, Anda akan menerima notifikasi email untuk mengeluarkan host yang terdegradasi dan memigrasikan instans Anda secara manual ke host lain dalam waktu 28 hari. Host pengganti dialokasikan jika Anda memiliki reservasi Host Khusus. Setelah 28 hari, instans yang berjalan pada host terdegradasi akan diakhiri, dan host dilepaskan secara otomatis.

Console

Untuk mengaktifkan pemeliharaan host untuk Host Khusus Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Pilih Host Dedikasi > Tindakan > Modifikasi host.

4. Pilih aktif di bidang Pemeliharaan host.

Untuk menonaktifkan pemeliharaan host untuk Host Khusus Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Pilih Host Dedikasi > Tindakan > Modifikasi host.
4. Pilih nonaktif di bidang Pemeliharaan host.

AWS CLI

Untuk mengaktifkan pemeliharaan host untuk Host Khusus Anda

Gunakan perintah modify-hosts.

```
aws ec2 modify-hosts \
    --host-maintenance on \
    --host-ids h-0d123456bbf78910d
```

Untuk menonaktifkan pemeliharaan host untuk Host Khusus Anda

Gunakan perintah modify-hosts.

```
aws ec2 modify-hosts \
    --host-maintenance off \
    --host-ids h-0d123456bbf78910d
```

PowerShell

Untuk mengaktifkan pemeliharaan host untuk Host Khusus Anda

Gunakan Edit-EC2Hostcmdlet.

```
Edit-EC2Host `
    -HostMaintenance on `
    -HostId h-0d123456bbf78910d
```

Untuk menonaktifkan pemeliharaan host untuk Host Khusus Anda

Gunakan Edit-EC2Hostcmdlet.

```
Edit-EC2Host `
    -HostMaintenance off `
    -HostId h-0d123456bbf78910d
```

Pantau status Host Khusus Amazon EC2 Anda

Amazon EC2 secara konstan memantau status Host Khusus Anda. Pembaruan dikomunikasikan di konsol Amazon EC2. Anda dapat melihat informasi tentang Host Khusus menggunakan metode berikut ini.

Console

Untuk melihat status Host Khusus

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Host Khusus.
3. Cari Host khusus dalam daftar dan tinjau nilai di kolom Status.

AWS CLI

Untuk melihat status Host Khusus

Gunakan perintah describe-host.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Untuk melihat status Host Khusus

Gunakan Get-EC2Hostcmdlet.

```
Get-EC2Host -HostId h-012a3456b7890cdef
```

Tabel berikut menjelaskan kemungkinan status Host Khusus.

Status	Deskripsi
`available`	AWS belum mendeteksi masalah dengan Host Khusus. Tidak ada pemeliharaan atau perbaikan yang dijadwalkan. Instans dapat diluncurkan ke Host Khusus ini.
`released`	Host Khusus telah dilepas. ID host tidak lagi digunakan. Host yang dilepas tidak dapat digunakan kembali.
`under-assessment`	AWS sedang mengeksplorasi kemungkinan masalah dengan Host Khusus. Jika tindakan harus diambil, Anda akan diberitahu melalui Konsol Manajemen AWS atau email. Instans tidak dapat diluncurkan ke Host Khusus dalam status ini.
`pending`	Host Khusus tidak dapat digunakan untuk peluncuran instans baru. Modifikasi untuk mendukung banyak tipe instans atau pemulihan host sedang berlangsung.
`permanent-failure`	Telah terdeteksi kegagalan yang tidak dapat dipulihkan. Anda menerima pemberitahuan pengosongan melalui instans Anda dan melalui email. Instans Anda mungkin terus berjalan. Jika Anda menghentikan atau menghentikan semua instans pada Host Khusus dengan status ini, host akan AWS pensiun. AWS tidak memulai ulang instance dalam keadaan ini. Instans tidak dapat diluncurkan ke Host Khusus dalam status ini.
`released-permanent-failure`	AWS secara permanen merilis Host Khusus yang gagal dan tidak lagi menjalankan instance di dalamnya. ID Host Khusus tidak lagi tersedia untuk digunakan.

Lacak perubahan konfigurasi Host Khusus Amazon EC2 menggunakan AWS Config

Anda dapat menggunakan AWS Config untuk merekam perubahan konfigurasi untuk Host Khusus, dan untuk instance yang diluncurkan, dihentikan, atau dihentikan pada mereka. Anda kemudian dapat menggunakan informasi yang ditangkap oleh AWS Config sebagai sumber data untuk pelaporan lisensi.

AWS Config mencatat informasi konfigurasi untuk Host Khusus dan instans satu per satu, dan memasangkan informasi ini melalui hubungan. Ada tiga kondisi pelaporan:

- AWS Config status perekaman —Saat Aktif, AWS Config merekam satu atau beberapa jenis AWS sumber daya, yang dapat mencakup Host Khusus dan Instans Khusus. Untuk menangkap informasi yang diperlukan untuk pelaporan lisensi, pastikan bahwa host dan instans sedang direkam dengan bidang berikut.
- Status pencatatan host—Saat Diaktifkan, informasi konfigurasi untuk Host Khusus dicatat.
- Status pencatatan instans—Saat Diaktifkan, informasi konfigurasi untuk Instans Khusus dicatat.

Jika salah satu dari ketiga kondisi ini dinonaktifkan, ikon di tombol Edit Config Recording akan berwarna merah. Untuk mendapatkan manfaat penuh dari alat ini, pastikan bahwa ketiga metode pencatatan diaktifkan. Jika ketiganya diaktifkan, ikon akan berwarna hijau. Untuk mengedit pengaturan, pilih Edit Pencatatan Konfigurasi. Anda diarahkan ke AWS Config halaman Siapkan di AWS Config konsol, tempat Anda dapat mengatur AWS Config dan mulai merekam untuk host, instans, dan jenis sumber daya lain yang didukung. Untuk informasi selengkapnya, lihat Menyiapkan AWS Config menggunakan Konsol di Panduan AWS Config Pengembang.

> **Note**
>
> AWS Config merekam sumber daya Anda setelah menemukannya, yang mungkin memakan waktu beberapa menit.

Setelah AWS Config mulai merekam perubahan konfigurasi ke host dan instance Anda, Anda bisa mendapatkan riwayat konfigurasi host mana pun yang telah Anda alokasikan atau rilis dan instance apa pun yang telah Anda luncurkan, hentikan, atau hentikan. Misalnya, di titik mana pun dalam riwayat konfigurasi Host Khusus, Anda dapat mencari berapa banyak instans yang diluncurkan pada host tersebut, bersama dengan jumlah soket dan inti pada host. Untuk salah satu instans tersebut, Anda juga dapat mencari ID dari Amazon Machine Image (AMI). Anda dapat menggunakan informasi ini untuk melaporkan tentang pelisensian untuk perangkat lunak terikat server Anda sendiri yang mendapat lisensi per soket atau per inti.

Anda dapat melihat riwayat konfigurasi dengan salah satu dari cara berikut ini:

- Dengan menggunakan AWS Config konsol. Untuk setiap sumber daya yang tercatat, Anda dapat melihat halaman kronologi, yang memberikan detail riwayat konfigurasi. Untuk melihat halaman ini, pilih ikon abu-abu di kolom Konfigurasi Kronologi pada halaman Host Khusus. Untuk informasi selengkapnya, lihat Melihat Detail Konfigurasi di AWS Config Konsol di Panduan AWS Config Pengembang.

- Dengan menjalankan AWS CLI perintah. Pertama, Anda dapat menggunakan list-discovered-resourcesperintah untuk mendapatkan daftar semua host dan instance. Kemudian, Anda dapat menggunakan get-resource-config-historyperintah untuk mendapatkan detail konfigurasi host atau instance untuk interval waktu tertentu.
- Dengan menggunakan AWS Config API dalam aplikasi Anda. Pertama, Anda dapat menggunakanListDiscoveredResources tindakan untuk mendapatkan daftar semua host dan instance. Kemudian, Anda dapat menggunakanGetResourceConfigHistory tindakan untuk mendapatkan detail konfigurasi host atau instance untuk interval waktu tertentu.

Misalnya, untuk mendapatkan daftar semua Host Khusus Anda AWS Config, jalankan perintah CLI seperti berikut ini.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Untuk mendapatkan riwayat konfigurasi Host Khusus dari AWS Config, jalankan perintah CLI seperti berikut ini.

```
aws configservice get-resource-config-history \
    --resource-type AWS::EC2::Instance \
    --resource-id i-1234567890abcdef0
```

Untuk mengelola AWS Config pengaturan menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di halaman Host Khusus, pilih Edit Pencatatan Konfigurasi.
3. Di AWS Config konsol, ikuti langkah-langkah yang disediakan untuk mengaktifkan perekaman. Untuk informasi selengkapnya, lihat Menyiapkan AWS Config menggunakan Konsol.

Untuk informasi selengkapnya, lihat Melihat Detail Konfigurasi di AWS Config Konsol.

Untuk mengaktifkan AWS Config menggunakan baris perintah atau API

- AWS CLI: Melihat Detail Konfigurasi (AWS CLI) di Panduan AWS Config Pengembang.
- API Amazon EC2:. GetResourceConfigHistory

Instans EC2 Khusus Amazon

Secara default, EC2 instance berjalan pada perangkat keras penyewaan bersama. Ini berarti bahwa beberapa AWS akun mungkin berbagi perangkat keras fisik yang sama.

Instans Khusus adalah EC2 instance yang berjalan pada perangkat keras yang didedikasikan untuk satu AWS akun. Ini berarti bahwa Instans Khusus secara fisik diisolasi pada tingkat perangkat keras host dari instans milik orang lain Akun AWS, bahkan jika akun tersebut ditautkan ke akun pembayar tunggal. Namun, Instans Khusus mungkin berbagi perangkat keras dengan instans lain dari instans yang sama Akun AWS yang bukan Instans Khusus.

Instans Khusus tidak memberikan visibilitas atau kontrol atas penempatan instans, dan instans tersebut tidak mendukung afinitas host. Jika Anda berhenti dan memulai Dedicated Instance, itu mungkin tidak berjalan pada host yang sama. Demikian pula, Anda tidak dapat menargetkan host tertentu untuk meluncurkan atau menjalankan instance. Selain itu, Instans Khusus memberikan dukungan terbatas untuk Bring Your Own License (BYOL).

Jika Anda memerlukan visibilitas dan kontrol atas penempatan instans dan dukungan BYOL yang lebih komprehensif, pertimbangkan untuk menggunakan Host Khusus. Instans Khusus dan Host Khusus keduanya dapat digunakan untuk meluncurkan EC2 instans Amazon ke server fisik khusus. Tidak ada perbedaan performa, keamanan, atau fisik di antara Instans Khusus dan instans pada Host Khusus. Namun, ada beberapa perbedaan utama di antara mereka. Tabel berikut menyoroti beberapa perbedaan utama antara Instans Khusus dan Host Khusus:

	Host Khusus	Instans Khusus
Server fisik khusus	Server fisik dengan kapasitas instans yang sepenuhnya didedikasikan untuk Anda gunakan.	Server fisik yang didedikasikan untuk satu akun pelanggan.
Pembagian kapasitas instans	Dapat berbagi kapasitas instans dengan akun lain.	Tidak didukung
Penagihan	Tagihan per host	Tagihan per instans
Visibilitas soket, inti, dan ID host	Memberikan visibilitas dalam jumlah soket dan inti fisik	Tidak ada visibilitas

	Host Khusus	Instans Khusus
Afinitas host dan instans	Memungkinkan Anda melakukan deployment instans Anda secara konsisten ke server fisik yang sama seiring waktu	Tidak didukung
Penempatan instans tertarget	Memberikan visibilitas dan kontrol tambahan atas cara penempatan instans di server fisik	Tidak didukung
Pemulihan instans otomatis	Didukung. Untuk informasi selengkapnya, lihat Pemulihan Host Khusus Amazon EC2.	Didukung
Bawa Lisensi Sendiri (BYOL)	Didukung	Dukungan parsial*
Reservasi Kapasitas	Tidak didukung	Didukung

* Microsoft SQL Server dengan License Mobility melalui Jaminan Perangkat Lunak, sedangkan lisensi Windows Virtual Desktop Access (VDA) dapat digunakan dengan Instans Khusus.

Untuk informasi selengkapnya, lihat Host Khusus Amazon EC.

Daftar Isi

- Dasar-dasar Instans Khusus
- Fitur yang didukung
- Batasan Instans Khusus
- Harga untuk Instans Khusus
- Luncurkan Instans Khusus ke dalam VPC dengan tenancy default
- Ubah penyewaan sebuah instance EC2
- Ubah penyewaan instance VPC

Dasar-dasar Instans Khusus

VPC dapat memiliki penghunian `default` atau `dedicated`. Secara default, Anda VPCs memiliki `default` penyewaan dan instance yang diluncurkan ke VPC `default` penyewaan memiliki penyewaan. `default` Untuk meluncurkan Instans Khusus, lakukan hal berikut:

- Buat VPC dengan penghunian `dedicated`, sehingga semua instans di VPC berjalan sebagai Instans Khusus. Untuk informasi selengkapnya, lihat Luncurkan Instans Khusus ke dalam VPC dengan tenancy default.
- Buat VPC dengan penghunian `default` dan tentukan secara manual penghunian `dedicated` untuk instans agar dijalankan sebagai Instans Khusus. Untuk informasi selengkapnya, lihat Luncurkan Instans Khusus ke dalam VPC dengan tenancy default.

Fitur yang didukung

Instans Khusus mendukung fitur dan integrasi AWS layanan berikut:

Fitur

- Instans Terpesan
- Penskalaan Otomatis
- Pemulihan otomatis
- Instans Spot Khusus
- Instance performa yang dapat melonjak

Instans Terpesan

Untuk memesan kapasitas Instans Khusus, Anda dapat membeli Instans Cadangan Khusus atau Reservasi Kapasitas. Untuk informasi selengkapnya, lihat Instans Cadangan untuk ikhtisar Amazon EC2 dan Cadangan kapasitas komputasi dengan Reservasi Kapasitas Sesuai Permintaan EC2.

Ketika Anda membeli Instans Cadangan Khusus, Anda membeli kapasitas untuk meluncurkan Instans Khusus dengan biaya penggunaan yang jauh lebih rendah; jeda harga dalam biaya penggunaan hanya berlaku jika Anda meluncurkan instans dengan penyewaan khusus. Saat Anda membeli Instans Terpesan dengan penghunian default, hal ini hanya berlaku untuk instans yang sedang berjalan dengan penghunian `default`, tetapi tidak berlaku untuk instans yang sedang berjalan dengan penghunian `dedicated`.

Anda tidak dapat menggunakan proses modifikasi untuk mengubah penghunian Instans Terpesan setelah Anda membelinya. Namun, Anda dapat menukar Instans Terpesan Konvertibel dengan Instans Terpesan Konvertibel baru dengan penghunian yang berbeda.

Penskalaan Otomatis

Anda dapat menggunakan Amazon EC2 Auto Scaling untuk meluncurkan Instans Khusus. Untuk informasi selengkapnya, lihat Membuat template peluncuran menggunakan setelan lanjutan di Panduan Pengguna Amazon EC2 Auto Scaling.

Pemulihan otomatis

Anda dapat mengonfigurasi pemulihan otomatis untuk Instans Khusus jika menjadi terganggu karena kegagalan perangkat keras yang mendasarinya atau masalah yang memerlukan AWS keterlibatan untuk memperbaiki. Untuk informasi selengkapnya, lihat Pemulihan instans otomatis.

Instans Spot Khusus

Anda dapat menjalankan Instans Spot Khusus dengan menentukan penghunian `dedicated` saat Anda membuat permintaan Instans Spot. Untuk informasi selengkapnya, lihat Peluncuran pada perangkat keras penyewa tunggal.

Instance performa yang dapat melonjak

Anda dapat memanfaatkan keuntungan menjalankan perangkat keras penghunian khusus dengan the section called “Instance performa yang dapat melonjak”. Instans Khusus T3 diluncurkan dalam mode tidak terbatas secara default, dan mereka memberikan tingkat acuan performa CPU dengan kemampuan untuk melonjak ke tingkat CPU yang lebih tinggi saat diperlukan oleh beban kerja Anda. Performa acuan T3 dan kemampuan melonjak diatur oleh kredit CPU. Karena sifat tipe instans T3 yang dapat melonjak, kami menyarankan Anda untuk memantau bagaimana instans T3 Anda menggunakan sumber daya CPU dari perangkat keras khusus untuk mendapatkan performa terbaik. Instans Khusus T3 ditujukan untuk pelanggan dengan beban kerja beragam yang menampilkan perilaku CPU acak, tetapi idealnya memiliki penggunaan CPU rata-rata pada atau di bawah penggunaan acuan. Untuk informasi selengkapnya, lihat the section called “Konsep utama”.

Amazon EC2 memiliki sistem untuk mengidentifikasi dan memperbaiki variabilitas dalam kinerja. Namun, masih mungkin untuk mengalami variabilitas jangka pendek jika Anda meluncurkan beberapa Instans Khusus T3 yang memiliki pola penggunaan CPU yang berkorelasi. Untuk beban kerja yang lebih menuntut atau berkorelasi ini, kami merekomendasikan penggunaan Instans Khusus M5 atau M5a daripada Instans Khusus T3.

Batasan Instans Khusus

Ingatlah hal-hal berikut ini saat menggunakan Instans Khusus:

- Beberapa AWS layanan atau fitur-fiturnya tidak didukung dengan VPC dengan penyewaan instance yang disetel ke. `dedicated` Lihat dokumentasi layanan masing-masing untuk mengonfirmasi jika ada batasan.
- Beberapa tipe instans tidak dapat diluncurkan ke VPC dengan penghunian instans yang diatur ke `dedicated`. Untuk informasi selengkapnya tentang jenis instans yang didukung, lihat Instans EC2 Khusus Amazon.
- Saat Anda meluncurkan Instans Khusus yang didukung Amazon EBS, volume EBS tidak berjalan pada perangkat keras penghunian tunggal.

Harga untuk Instans Khusus

Harga untuk Instans Khusus berbeda dari harga untuk Instans Sesuai Permintaan. Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.

Luncurkan Instans Khusus ke dalam VPC dengan tenancy default

Saat membuat VPC, Anda memiliki opsi untuk menentukan penghunian instansnya. Jika Anda meluncurkan instance ke dalam VPC yang memiliki penyewaan instance`dedicated`, instance tersebut berjalan sebagai Instans Khusus pada perangkat keras yang didedikasikan untuk Anda gunakan.

Untuk informasi selengkapnya tentang meluncurkan instans dengan penghunian `host`, lihat Luncurkan instans Amazon EC2 di Host Khusus Amazon EC2.

Untuk informasi selengkapnya tentang opsi penyewaan VPC, lihat Membuat VPC di Panduan Pengguna Amazon VPC.

Persyaratan

- Pilih jenis instans yang didukung. Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.

Console

Untuk meluncurkan Instans Khusus ke VPC tenancy default

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans, Luncurkan instans.
3. Di bagian Gambar Aplikasi dan OS, pilih AMI dari daftar.
4. Di bagian tipe instans, pilih tipe instans yang akan diluncurkan.
5. Di bagian Key pair, pilih key pair untuk diasosiasikan dengan instans.
6. Di bagian Detail lanjutan, untuk Penghunian, pilih Khusus.
7. Konfigurasikan opsi instans yang tersisa sesuai kebutuhan. Untuk informasi selengkapnya, lihat Referensi untuk parameter konfigurasi EC2 instans Amazon.
8. Pilih Luncurkan instans.

AWS CLI

Untuk mengatur opsi penyewaan untuk sebuah instance selama peluncuran

Gunakan perintah run-instance dan sertakan `Tenancy` dengan opsi. `--placement`

```
--placement Tenancy=dedicated
```

PowerShell

Untuk mengatur opsi penyewaan untuk sebuah instance selama peluncuran

Gunakan New-EC2Instancecmdlet dengan parameter. `-Placement_Tenancy`

```
-Placement_Tenancy dedicated
```

Ubah penyewaan sebuah instance EC2

Anda dapat mengubah penghunian instans yang dihentikan setelah peluncuran. Perubahan yang Anda buat berlaku saat berikutnya instans dimulai.

Atau, Anda dapat mengubah sewa virtual private cloud (VPC) Anda. Untuk informasi selengkapnya, lihat the section called “Mengubah penghunian VPC”.

Batasan

- Anda tidak dapat mengubah penyewaan instance menggunakan. Konsol Manajemen AWS
- Instans harus berada dalam status `stopped`.
- Detail sistem operasi instans Anda, dan apakah SQL Server diinstal, memengaruhi konversi apa yang didukung. Untuk informasi selengkapnya tentang jalur konversi penghunian yang tersedia untuk instans Anda, lihat Konversi penghunia di Panduan Pengguna Manajer Lisensi.
- Untuk instans T3, Anda harus meluncurkan instans pada Host Khusus untuk menggunakan penyewaan `host`. Anda tidak dapat mengubah penghunian dari `host` menjadi `dedicated` atau `default`. Percobaan mengubah salah satu penghunian yang tidak didukung ini dapat mengakibatkan kode kesalahan `InvalidRequest`.

AWS CLI

Untuk memodifikasi nilai sewa sebuah instance

Gunakan perintah modify-instance-placement.

```
aws ec2 modify-instance-placement \
    --instance-id i-1234567890abcdef0 \
    --tenancy dedicated
```

PowerShell

Untuk memodifikasi nilai sewa sebuah instance

Gunakan Edit-EC2InstancePlacementcmdlet.

```
Edit-EC2InstancePlacement `
    -InstanceId i-1234567890abcdef0 `
    -Tenancy Dedicated
```

Ubah penyewaan instance VPC

Anda dapat mengubah penyewaan instance virtual private cloud (VPC) `dedicated` dari `default` menjadi setelah Anda membuatnya. Memodifikasi penyewaan instance VPC tidak memengaruhi penyewaan instance yang ada di VPC. Lain kali Anda meluncurkan instance di VPC, itu memiliki penyewaan`default`, kecuali jika Anda menentukan sebaliknya selama peluncuran instance.

Atau, Anda dapat mengubah penyewaan instance tertentu. Untuk informasi selengkapnya, lihat the section called “Mengubah penghunian suatu instans”.

Batasan

- Anda tidak dapat mengubah penyewaan instance VPC `default` dari `dedicated` menjadi setelah dibuat.
- Anda tidak dapat memodifikasi penyewaan instance VPC menggunakan file. Konsol Manajemen AWS

AWS CLI

Untuk memodifikasi atribut penyewaan instance dari VPC

Gunakan perintah modify-vpc-tenancy. Satu-satunya nilai sewa yang didukung adalah`default`.

```
aws ec2 modify-vpc-tenancy \
    --vpc-id vpc-1234567890abcdef0 \
    --instance-tenancy default
```

PowerShell

Untuk memodifikasi atribut penyewaan instance dari VPC

Gunakan Edit-EC2VpcTenancycmdlet. Satu-satunya nilai sewa yang didukung adalah`Default`.

```
Edit-EC2VpcTenancy `
    -VpcId vpc-1234567890abcdef0 `
    -InstanceTenancy Default
```

Reservasi Kapasitas Sesuai Permintaan dan Blok Kapasitas untuk ML

Reservasi Kapasitas memungkinkan Anda untuk memesan kapasitas komputasi untuk EC2 instans Amazon di Availability Zone tertentu. Ada dua tipe Reservasi Kapasitas yang melayani kasus penggunaan yang berbeda.

Tipe Reservasi Kapasitas

- Reservasi Kapasitas Sesuai Permintaan

- Blok Kapasitas untuk ML

Berikut adalah beberapa kasus penggunaan umum untuk Reservasi Kapasitas Sesuai Permintaan:

- Acara penskalaan — Buat Reservasi Kapasitas Sesuai Permintaan sebelum acara penting bisnis Anda untuk memastikan bahwa Anda dapat menskalakan saat diperlukan.
- Persyaratan peraturan dan pemulihan bencana — Gunakan Reservasi Kapasitas Sesuai Permintaan untuk memenuhi persyaratan peraturan untuk ketersediaan tinggi, dan pesan kapasitas di Zona Ketersediaan atau Wilayah yang berbeda untuk pemulihan bencana.
- Berbagi kapasitas yang tidak terpakai — Gunakan Reservasi Kapasitas Interruptible untuk membuat kapasitas yang tidak terpakai tersedia untuk beban kerja lain dalam akun Anda sambil mempertahankan kontrol untuk merebut kembali ketika diperlukan.

Berikut ini adalah beberapa kasus penggunaan umum untuk Blok Kapasitas untuk ML:

- Pelatihan model machine learning (ML) dan fine-tuning — Dapatkan akses tanpa gangguan ke instans GPU yang Anda pesan untuk menyelesaikan pelatihan model dan fine-tuning.
- Eksperimen dan prototipe ML — Jalankan eksperimen dan bangun prototipe yang memerlukan instans GPU untuk jangka waktu pendek.

Kapan menggunakan Reservasi Kapasitas Sesuai Permintaan

Gunakan Reservasi Kapasitas Sesuai Permintaan jika Anda memiliki persyaratan kapasitas yang ketat, dan beban kerja penting bisnis Anda saat ini atau di masa depan memerlukan jaminan kapasitas. Dengan Pemesanan Kapasitas Sesuai Permintaan, Anda dapat memastikan bahwa Anda akan selalu memiliki akses ke EC2 kapasitas Amazon yang telah Anda pesan selama Anda membutuhkannya.

Kapan menggunakan Blok Kapasitas untuk ML

Gunakan Blok Kapasitas untuk ML saat Anda perlu memastikan bahwa Anda memiliki akses tanpa gangguan ke instans GPU untuk jangka waktu tertentu yang dimulai pada tanggal yang akan datang. Blok Kapasitas ideal untuk melatih dan menyempurnakan model ML, menjalankan eksperimen singkat, dan menangani lonjakan sementara dalam permintaan inferensi di masa mendatang. Dengan Blok Kapasitas, Anda dapat memastikan bahwa Anda akan memiliki akses ke sumber daya GPU pada tanggal tertentu untuk menjalankan beban kerja ML Anda.

Cadangan kapasitas komputasi dengan Reservasi Kapasitas Sesuai Permintaan EC2

Reservasi Kapasitas Amazon EC2 memungkinkan Anda memesan kapasitas komputasi untuk instans Amazon EC2 di Availability Zone tertentu untuk durasi berapa pun. Jika Anda memiliki persyaratan kapasitas yang ketat untuk beban kerja penting bisnis saat ini atau masa depan yang memerlukan tingkat jaminan kapasitas jangka panjang atau jangka pendek tertentu, kami sarankan Anda membuat Reservasi Kapasitas untuk membantu memastikan bahwa Anda selalu memiliki akses ke kapasitas Amazon EC2 saat Anda membutuhkannya, selama Anda membutuhkannya.

Anda dapat membuat Reservasi Kapasitas kapan saja, dan Anda dapat memilih kapan dimulai. Anda dapat meminta Reservasi Kapasitas untuk penggunaan segera atau Anda dapat meminta Reservasi Kapasitas untuk tanggal yang akan datang.

- Jika Anda meminta Reservasi Kapasitas untuk penggunaan segera, Reservasi Kapasitas akan segera tersedia untuk digunakan dan tidak ada komitmen jangka waktu. Anda dapat mengubah Reservasi Kapasitas kapan saja, dan Anda dapat membatalkannya kapan saja untuk melepaskan kapasitas yang dipesan dan untuk menghentikan biaya yang dikenakan.
- Jika Anda meminta Reservasi Kapasitas bertanggal di masa depan, Anda menentukan tanggal di masa depan di mana Anda memerlukan Reservasi Kapasitas agar tersedia untuk digunakan. Anda juga harus menentukan durasi komitmen di mana Anda berkomitmen untuk menjaga kapasitas yang diminta di akun Anda setelah tanggal yang ditentukan. Pada tanggal dan waktu yang diminta, Reservasi Kapasitas tersedia untuk digunakan dan durasi komitmen dimulai. Selama durasi komitmen, Anda tidak dapat mengurangi jumlah instans atau durasi komitmen di bawah komitmen awal Anda, atau membatalkan Reservasi Kapasitas. Setelah durasi komitmen berlalu, Anda dapat mengubah Reservasi Kapasitas dengan cara apa pun atau membatalkannya jika Anda tidak lagi membutuhkannya.

Reservasi Kapasitas hanya dapat digunakan oleh instans yang cocok dengan atributnya. Secara default, Reservasi Kapasitas secara otomatis mencocokkan instance baru dan instance berjalan yang memiliki atribut yang cocok (jenis instans, platform, Availability Zone, dan tenancy). Ini berarti bahwa setiap instans dengan atribut yang cocok secara otomatis berjalan di Reservasi Kapasitas. Namun, Anda juga dapat menargetkan Reservasi Kapasitas untuk beban kerja tertentu. Ini memungkinkan Anda untuk secara eksplisit mengontrol instance mana yang diizinkan untuk dijalankan dalam kapasitas cadangan tersebut. Anda juga dapat menentukan bahwa instance hanya akan berjalan di grup sumber daya Reservasi Kapasitas atau Reservasi Kapasitas.

> **Important**
>
> Reservasi Kapasitas masa depan adalah untuk membantu Anda meluncurkan dan mencakup instans tambahan, dan tidak mencakup instans yang sedang berjalan. Jika Anda perlu mencakup instans yang sedang berjalan, gunakan Reservasi Kapasitas yang segera dimulai.

Semua instans Amazon EC2 yang didukung dengan atribut yang cocok, yaitu jenis instans, platform, Availability Zone, dan tenancy, memenuhi syarat untuk dijalankan dalam Reservasi Kapasitas. Instans Amazon EC2 dapat diluncurkan oleh Anda (instans yang tidak dikelola) atau atas nama Anda oleh AWS layanan (instans terkelola). Hal ini terutama berlaku untuk Reservasi Kapasitas terbuka, yang secara otomatis cocok dengan instance yang berjalan yang memiliki atribut yang cocok. Misalnya, instans terkelola yang diluncurkan atas nama Anda oleh layanan berikut memenuhi syarat untuk dijalankan di Reservasi Kapasitas yang Anda buat dan kelola.

- Amazon EC2 Auto Scaling
- Amazon ECS
- Amazon EKS
- Amazon EMR
- Amazon SageMaker AI
- AWS Batch
- AWS Elastic Beanstalk
- AWS ParallelCluster
- AWS Parallel Computing Service (AWS PCS)

Daftar Isi

- Konsep untuk Pemesanan Kapasitas Amazon EC2
- Perbedaan antara Reservasi Kapasitas, Instans Terpesan, dan Savings Plans
- Platform yang didukung
- Kuota
- Batasan
- Harga dan penagihan Reservasi Kapasitas
- Membuat Reservasi Kapasitas

- Lihat status Reservasi Kapasitas
- Luncurkan instans ke dalam Reservasi Kapasitas yang ada
- Ubah Reservasi Kapasitas yang aktif
- Ubah pengaturan Reservasi Kapasitas instans Anda
- Pindahkan kapasitas antara Reservasi Kapasitas
- Memisahkan kapasitas dari Reservasi Kapasitas yang ada
- Membatalkan Reservasi Kapasitas
- Gunakan Reservasi Kapasitas dengan grup penempatan klaster
- Grup Reservasi Kapasitas
- Reservasi Kapasitas di Local Zones
- Reservasi Kapasitas di Wavelength Zones
- Reservasi Kapasitas di AWS Outposts
- Reservasi Kapasitas Bersama
- Armada Reservasi Kapasitas
- Memantau penggunaan Reservasi Kapasitas dengan metrik CloudWatch
- Monitor Reservasi Kapasitas yang kurang dimanfaatkan
- Pantau perubahan status untuk Reservasi Kapasitas yang bertanggal di masa mendatang
- Reservasi Kapasitas yang Dapat Diputus

Konsep untuk Pemesanan Kapasitas Amazon EC2

Konsep kunci berikut berlaku untuk Reservasi Kapasitas.

Topik

- Tanggal dan waktu mulai
- Tanggal dan waktu akhir
- Durasi komitmen
- Penilaian Reservasi Kapasitas Bertanggal di Masa Depan
- Atribut Reservasi Kapasitas
- Kriteria pencocokan instance

Tanggal dan waktu mulai

Tanggal dan waktu mulai menentukan kapan Reservasi Kapasitas tersedia untuk digunakan. Reservasi Kapasitas dapat segera dimulai, atau dapat dimulai di masa mendatang.

- Jika Anda memilih untuk segera memulai Reservasi Kapasitas, kapasitas cadangan akan tersedia untuk digunakan segera setelah Anda membuatnya, dan penagihan dimulai segera setelah Reservasi Kapasitas memasuki status aktif. Anda tidak perlu masuk ke dalam komitmen jangka apa pun. Anda dapat mengubah Reservasi Kapasitas sesuai kebutuhan kapan saja untuk memenuhi kebutuhan Anda, dan Anda dapat membatalkannya kapan saja untuk melepaskan kapasitas dan menghentikan biaya yang dikenakan.
- Jika Anda memilih untuk memulai Reservasi Kapasitas di masa mendatang, Anda menentukan tanggal dan waktu di masa mendatang di mana Anda akan memerlukan kapasitas cadangan, dan durasi komitmen, yang merupakan durasi minimum yang Anda komit untuk menyimpan Reservasi Kapasitas yang diminta di akun Anda setelah disediakan. Pada tanggal future yang ditentukan, Reservasi Kapasitas tersedia untuk digunakan dan penagihan dimulai pada saat itu, setelah Reservasi Kapasitas memasuki status aktif. Durasi komit dimulai segera setelah Reservasi Kapasitas disediakan di akun Anda. Selama waktu ini, Anda tidak dapat mengurangi jumlah instans di bawah jumlah instans yang dilakukan, memilih tanggal akhir sebelum durasi komitmen, atau membatalkan Reservasi Kapasitas. Namun, setelah durasi komitmen berakhir, Anda bebas untuk mengubah Reservasi Kapasitas dengan cara apa pun, atau membatalkannya untuk melepaskan kapasitas yang dipesan dan menghentikan biaya yang dikenakan.

Tanggal dan waktu akhir

Tanggal dan waktu berakhir menentukan kapan Reservasi Kapasitas berakhir dan kapasitas cadangan dilepaskan dari akun Anda. Anda dapat mengonfigurasi Reservasi Kapasitas untuk berakhir secara otomatis pada tanggal dan waktu tertentu, atau Anda dapat mengonfigurasinya agar tetap aktif tanpa batas hingga Anda membatalkannya secara manual.

Jika Anda mengonfigurasi Reservasi Kapasitas untuk berakhir secara otomatis, Reservasi Kapasitas akan kedaluwarsa dalam satu jam dari waktu yang ditentukan. Misalnya, jika Anda menentukan`5/31/2019, 13:30:55`, Reservasi Kapasitas dijamin berakhir antara `13:30:55` dan `14:30:55` seterusnya`5/31/2019`.

Setelah reservasi berakhir, kapasitas cadangan dilepaskan dari akun Anda dan Anda tidak dapat lagi menargetkan instans ke Reservasi Kapasitas. Instans yang berjalan dalam kapasitas terpesan terus berjalan tanpa interupsi. Jika instance yang menargetkan Reservasi Kapasitas dihentikan, Anda

tidak dapat memulai ulang hingga Anda menghapus preferensi penargetan Reservasi Kapasitas atau mengonfigurasinya untuk menargetkan Reservasi Kapasitas yang berbeda. Untuk informasi selengkapnya, lihat Ubah pengaturan Reservasi Kapasitas instans Anda.

Durasi komitmen

Durasi komitmen hanya berlaku untuk Reservasi Kapasitas bertanggal di masa depan.

Durasi komitmen adalah durasi minimum di mana Anda berkomitmen untuk memiliki Reservasi Kapasitas bertanggal di masa depan dalam status aktif di akun Anda setelah disediakan. Anda dapat menyimpan Reservasi Kapasitas masa depan lebih lama dari durasi komitmen, tetapi tidak lebih pendek. Berikut ini berlaku selama durasi komitmen:

- Anda tidak dapat membatalkan Reservasi Kapasitas selama durasi komitmen.
- Anda tidak dapat mengurangi jumlah instans di bawah jumlah instans yang dikomit, tetapi Anda dapat meningkatkannya.
- Anda tidak dapat mengonfigurasi Reservasi Kapasitas untuk secara otomatis berakhir pada tanggal atau waktu yang berada dalam durasi komitmen. Anda dapat memperpanjang tanggal dan waktu akhir selama periode komitmen.

Amazon EC2 menggunakan durasi komitmen yang Anda tentukan untuk menilai apakah permintaan dapat didukung. Durasi komitmen minimum adalah 14 hari. Saat menilai permintaan, Amazon EC2 mungkin menentukan bahwa itu dapat mendukung durasi komitmen yang lebih pendek. Dalam hal ini, Amazon EC2 akan menjadwalkan Reservasi Kapasitas bertanggal di masa depan dengan durasi komitmen yang lebih pendek. Ini berarti bahwa Anda berkomitmen untuk menyimpan Reservasi Kapasitas di akun Anda untuk jangka waktu yang lebih singkat dari yang Anda minta sebelumnya.

Penilaian Reservasi Kapasitas Bertanggal di Masa Depan

Saat Anda meminta Reservasi Kapasitas bertanggal mendatang, Amazon EC2 menilai permintaan tersebut untuk menentukan apakah permintaan tersebut dapat didukung berdasarkan ketersediaan kapasitas dan durasi komitmen yang Anda tentukan. Penilaian biasanya selesai dalam waktu 5 hari. Amazon EC2 mempertimbangkan beberapa faktor saat mengevaluasi permintaan, termasuk:

- Pasokan kapasitas yang diperkirakan
- Durasi komitmen
- Seberapa awal Anda meminta Reservasi Kapasitas relatif terhadap tanggal mulai Anda
- Ukuran permintaan Anda

Anda dapat meminta Reservasi Kapasitas bertanggal antara 5 dan 120 hari sebelumnya. Kami menyarankan Anda membuat permintaan setidaknya 56 hari (8 minggu) sebelumnya untuk meningkatkan kemampuan kami untuk mendukung permintaan Anda. Durasi komitmen minimum adalah 14 hari dan jumlah instans minimum adalah 32 vCPUs.

Reservasi Kapasitas tetap berada di `assessing` negara bagian saat permintaan sedang dinilai.

Jika permintaan dapat didukung, Reservasi Kapasitas memasuki `scheduled` negara bagian dan dijadwalkan untuk pengiriman pada tanggal dan waktu yang diminta. Jumlah instans total tetap 0 selama Reservasi Kapasitas berada di `scheduled` negara bagian. Reservasi Kapasitas yang dijadwalkan akan tersedia `active` dan tersedia untuk digunakan pada tanggal yang diminta.

Jika permintaan tidak dapat didukung, Reservasi Kapasitas akan memasuki `unsupported` status. Reservasi Kapasitas yang Tidak Didukung tidak dikirimkan.

Anda dapat membatalkan Reservasi Kapasitas bertanggal di masa depan saat berada di negara bagian. `assessing`

Untuk informasi selengkapnya, lihat Buat Reservasi Kapasitas masa depan.

Atribut Reservasi Kapasitas

Saat membuat Reservasi Kapasitas, Anda harus menentukan atribut berikut:

- Zona Ketersediaan
- Tipe instans
- Platform (tipe sistem operasi)
- Penyewaan (`defaultataudedicated`)

Hanya instance yang cocok dengan atribut ini yang dapat diluncurkan atau dijalankan di Reservasi Kapasitas.

Kriteria pencocokan instance

Kriteria pencocokan instans, atau kelayakan instans, menentukan instance mana yang diizinkan untuk diluncurkan dan dijalankan di Reservasi Kapasitas. Reservasi Kapasitas dapat memiliki salah satu kriteria pencocokan berikut:

- Buka — Reservasi Kapasitas secara otomatis cocok dengan semua instance yang memiliki atribut yang cocok (jenis instans, platform, dan Availability Zone). Instance baru dan yang sudah ada yang

memiliki atribut yang cocok secara otomatis berjalan di Reservasi Kapasitas tanpa konfigurasi tambahan apa pun.

- Targeted — Reservasi Kapasitas hanya menerima instans yang memiliki atribut yang cocok (tipe instans, platform, dan Availability Zone), dan yang secara eksplisit menargetkan Reservasi Kapasitas. Instans harus secara khusus menargetkan Reservasi Kapasitas untuk diluncurkan atau dijalankan dalam kapasitas yang dicadangkan. Hal ini memungkinkan Anda untuk secara eksplisit mengontrol instance mana yang diizinkan untuk berjalan dalam kapasitas cadangan dan membantu Anda menghindari penggunaan kapasitas cadangan yang tidak disengaja.

Saat Anda meminta Reservasi Kapasitas bertanggal mendatang, Anda hanya dapat menentukan kriteria pencocokan yang ditargetkan. Ini memastikan bahwa kapasitas yang dikirimkan oleh Reservasi Kapasitas bersifat tambahan, atau tambahan, untuk setiap instans yang sedang berjalan atau kapasitas cadangan yang Anda miliki pada saat pengiriman. Setelah Reservasi Kapasitas aktif di akun Anda, Anda dapat mengubah kriteria pencocokan instans untuk dibuka jika diperlukan. Namun, perlu diingat bahwa setiap instans yang cocok akan secara otomatis berjalan di Reservasi Kapasitas, yang dapat menyebabkan penggunaan kapasitas yang tidak disengaja dan mencegah Anda meluncurkan instans baru untuk jumlah instans yang diminta secara penuh.

Perbedaan antara Reservasi Kapasitas, Instans Terpesan, dan Savings Plans

Tabel berikut menyoroti perbedaan utama antara Reservasi Kapasitas, Instans Terpesan, dan Savings Plans:

	Reservasi Kapasitas	Instans Terpesan Zonal	Instans Terpesan Regional	Savings Plans
Jangka waktu	Tidak ada komitmen yang diperlukan untuk Reservasi Kapasitas yang segera digunakan . Mereka dapat dibuat, dimodifik asi, dan dibatalkan sesuai kebutuhan.	Memerlukan komitmen tetap satu tahun atau tiga tahun		

	Reservasi Kapasitas	Instans Terpesan Zonal	Instans Terpesan Regional	Savings Plans
	Dengan Reservasi Kapasitas masa depan, Anda menentukan durasi komitmen yang Anda berkomitmen untuk menjaga kapasitas di akun Anda. Setelah durasi komitmen berlalu, Anda dapat membatalkan Reservasi Kapasitas kapan saja.			
Keuntungan kapasitas	Kapasitas yang terpesan dalam Zona Ketersediaan tertentu.		Tidak ada kapasitas tersimpan.	
Diskon tagihan	Tidak ada diskon penagihan. †	Berikan diskon penagihan.		
Batas Instans	Batas Instans Sesuai Permintaan Anda per Wilayah berlaku.	Default adalah 20 per Zona Ketersediaan. Anda dapat meminta kenaikan batas.	Default adalah 20 per Wilayah. Anda dapat meminta kenaikan batas.	Tanpa batas.

† Anda dapat menggabungkan Reservasi Kapasitas dan Savings Plans atau Instans Terpesan regional dengan untuk mendapatkan diskon.

Untuk informasi selengkapnya, lihat berikut ini:

- Instans Cadangan untuk ikhtisar Amazon EC2

- Panduan Pengguna Savings Plans

Platform yang didukung

Anda harus membuat Reservasi Kapasitas dengan platform yang benar untuk memastikannya cocok dengan instans Anda. Reservasi Kapasitas mendukung nilai-nilai berikut untuk`platform`:

- Linux/UNIX
- Linux dengan SQL Server Standard
- Linux dengan SQL Server Web
- Linux dengan SQL Server Enterprise
- SUSE Linux
- Linux Red Hat Enterprise
- RHEL dengan SQL Server Standard
- RHEL dengan SQL Server Enterprise
- RHEL dengan SQL Server Web
- RHEL dengan HA
- RHEL dengan Standar HA dan SQL Server
- RHEL dengan HA dan SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows dengan SQL Server
- Windows dengan SQL Server Web
- Windows dengan SQL Server Standard
- Windows dengan SQL Server Enterprise

Untuk memastikan bahwa instans berjalan dalam Reservasi Kapasitas tertentu, platform Reservasi Kapasitas harus sesuai dengan platform AMI yang digunakan untuk meluncurkan instans. Untuk Linux AMIs, penting untuk memeriksa apakah platform AMI menggunakan nilai umum Linux/UNIX atau nilai yang lebih spesifik seperti SUSE Linux.

Console

Untuk memeriksa platform AMI

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih AMIs.
3. Pilih AMI.
4. Pada tab Detail, perhatikan nilai detail Platform.

AWS CLI

Untuk memeriksa platform AMI

Gunakan perintah deskripsi-gambar dan periksa nilai. `PlatformDetails`

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].PlatformDetails
```

Berikut ini adalah output contoh.

```
[
    "Linux/UNIX"
]
```

PowerShell

Untuk memeriksa platform AMI

Gunakan Get-EC2Imagecmdlet dan periksa nilai. `PlatformDetails`

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Select PlatformDetails
```

Berikut ini adalah output contoh.

```
PlatformDetails
```

```
---------------
Linux/UNIX
```

Kuota

Jumlah instans yang kapasitasnya dapat Anda pesan didasarkan pada kuota Instans Sesuai Permintaan akun Anda. Anda dapat memesan kapasitas untuk sebanyak mungkin instans sesuai kuota yang diizinkan, dikurangi jumlah instans yang sudah berjalan.

Reservasi Kapasitas di`assessing`,,`scheduled`, `pending`a`ctive`, dan `delayed` status dihitung terhadap kuota Instans Sesuai Permintaan Anda.

Batasan

Sebelum Anda membuat Reservasi Kapasitas, perhatikan batasan dan larangan berikut.

- Reservasi Kapasitas yang aktif dan tidak terpakai diperhitungkan dalam batas Instans Sesuai Permintaan Anda.
- Reservasi Kapasitas tidak dapat dipindahtangankan dari satu AWS akun ke akun lainnya. Namun, Anda dapat berbagi Reservasi Kapasitas dengan AWS akun lain. Untuk informasi selengkapnya, lihat Reservasi Kapasitas Bersama.
- Diskon penagihan Instans Terpesan zonal tidak berlaku untuk Reservasi Kapasitas.
- Reservasi Kapasitas dapat dibuat dalam grup penempatan klaster. Grup penempatan partisi dan tersebar tidak didukung.
- Reservasi Kapasitas tidak dapat digunakan dengan Host Khusus. Reservasi Kapasitas dapat digunakan dengan Instans Khusus.
- [Instans Windows] Reservasi Kapasitas tidak dapat digunakan dengan Bring Your Own License (BYOL).
- [Red Hat Instances] Reservasi Kapasitas dapat digunakan dengan Bring Your Own License (BYOL).
- Reservasi Kapasitas tidak memastikan bahwa instans yang dihibernasi dapat melanjutkan setelah Anda mencoba untuk memulainya.
- Anda dapat meminta Reservasi Kapasitas bertanggal di masa mendatang untuk jumlah instans dengan minimal 32 v. CPUs Misalnya, jika Anda meminta Reservasi Kapasitas bertanggal mendatang untuk `m5.xlarge` instans, Anda harus meminta setidaknya 8 instans (8 * m5.xlarge = 32 v). CPUs

- Anda dapat meminta Reservasi Kapasitas bertanggal mendatang untuk jenis instans hanya dalam seri berikut: C, G, I, M, R, dan T.

Harga dan penagihan Reservasi Kapasitas

Topik di bagian ini memberikan ikhtisar harga dan penagihan untuk Reservasi Kapasitas.

Topik

- Harga
- Penagihan
- Diskon tagihan
- Melihat tagihan Anda

Harga

Reservasi Kapasitas dibebankan dengan tarif Sesuai Permintaan yang setara baik Anda menjalankan instans dalam kapasitas cadangan atau tidak, termasuk biaya tambahan regional yang berlaku untuk Instans Khusus. Jika Anda tidak menggunakan reservasi, ini akan muncul sebagai reservasi yang tidak terpakai di tagihan Amazon EC2 Anda. Saat Anda menjalankan instans yang cocok dengan atribut reservasi, Anda cukup membayar untuk instans tersebut dan tidak membayar apa pun untuk reservasi. Tidak ada biaya di muka atau biaya tambahan.

Misalnya, jika Anda membuat Reservasi Kapasitas untuk 20 instans Linux `m4.large` dan menjalankan 15 instans Linux `m4.large` di Zona Ketersediaan yang sama, Anda akan dikenai biaya sebesar 15 instans aktif dan 5 instans yang tidak digunakan dalam reservasi.

Diskon tagihan untuk Savings Plans dan Instans Terpesan Regional berlaku untuk Reservasi Kapasitas. Untuk informasi selengkapnya, lihat Diskon tagihan.

Untuk informasi selengkapnya, lihat Penetapan Harga Amazon EC2.

Penagihan

Tagihan dimulai segera setelah Reservasi Kapasitas disediakan di akun Anda, dan tagihan berlanjut selama Reservasi Kapasitas tetap disediakan di akun Anda. Untuk Reservasi Kapasitas masa depan, ini berarti bahwa penagihan dimulai hanya setelah Reservasi Kapasitas disediakan di akun Anda pada tanggal future yang diminta.

Reservasi Kapasitas ditagih dengan perincian per detik. Ini berarti bahwa Anda akan dikenai biaya untuk sebagian jam. Misalnya, jika Reservasi Kapasitas tetap disediakan di akun Anda selama 24 jam dan 15 menit, Anda ditagih untuk 24.25 jam reservasi.

Contoh berikut menunjukkan bagaimana Reservasi Kapasitas ditagih. Reservasi Kapasitas dibuat untuk satu Instans Linux m4.large, yang memiliki tarif Sesuai Permintaan USD0,10 per jam penggunaan. Dalam contoh ini, Reservasi Kapasitas disediakan di akun selama lima jam. Reservasi Kapasitas tidak digunakan untuk satu jam pertama, jadi akan ditagih untuk satu jam yang tidak digunakan dengan tarif Sesuai Permintaan standar tipe instans m4.large. Dalam jam dua sampai lima, Reservasi Kapasitas ditempati oleh instans m4.large. Selama itu, Reservasi Kapasitas tidak mengakumulasi biaya, tetapi akun ditagih untuk instans m4.large yang menempatinya. Pada jam keenam, Reservasi Kapasitas dibatalkan dan instans m4.large berjalan normal di luar kapasitas terpesan. Untuk jam tersebut, biaya dikenakan pada tarif Sesuai Permintaan untuk tipe instans m4.large.

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Diskon tagihan

Diskon penagihan untuk Savings Plans dan Instans Cadangan Regional berlaku untuk Reservasi Kapasitas. AWS otomatis menerapkan diskon ini ke Reservasi Kapasitas yang memiliki atribut yang cocok. Saat Reservasi Kapasitas digunakan oleh sebuah instans, diskon diterapkan ke instans tersebut. Diskon secara istimewa diterapkan pada penggunaan instans sebelum mencakup Reservasi Kapasitas yang tidak digunakan.

Diskon tagihan Instans Terpesan zonal tidak berlaku untuk Reservasi Kapasitas.

Untuk informasi selengkapnya, lihat berikut ini:

- Instans Cadangan untuk ikhtisar Amazon EC2
- Panduan Pengguna Savings Plans
- Opsi tagihan dan pembelian

Melihat tagihan Anda

Anda dapat meninjau tagihan dan biaya untuk akun Anda di konsol AWS Manajemen Penagihan dan Biaya .

- Dasbor menampilkan ringkasan pengeluaran untuk akun Anda.
- Pada halaman Tagihan, pada Detail, perluas bagian Elastic Compute Cloud dan Wilayah untuk mendapatkan informasi tagihan terkait Kapasitas Terpesan Anda.

Anda dapat melihat tagihannya secara online, atau Anda dapat mengunduh file CSV. Untuk informasi selengkapnya, lihat item baris Reservasi Kapasitas.

Membuat Reservasi Kapasitas

Anda dapat membuat Reservasi Kapasitas kapan saja untuk memastikan bahwa Anda memiliki kapasitas komputasi yang tersedia di Availability Zone tertentu. Reservasi Kapasitas dapat segera dimulai, atau dapat dimulai di masa mendatang. Kapasitas menjadi tersedia untuk digunakan hanya setelah Reservasi Kapasitas memasuki `active` negara bagian.

> **Note**
>
> Jika Anda membuat Reservasi Kapasitas dengan kriteria pencocokan `open` instans, dan Anda telah menjalankan instance dengan atribut yang cocok pada saat Reservasi Kapasitas menjadi aktif, instans tersebut secara otomatis berjalan dalam kapasitas cadangan. Untuk menghindari hal ini, gunakan kriteria pencocokan `targeted` instance. Untuk informasi selengkapnya, lihat Kriteria pencocokan instance.

Permintaan Anda untuk membuat Reservasi Kapasitas bisa gagal jika salah satu dari yang berikut ini benar:

- Amazon EC2 tidak memiliki kapasitas yang cukup untuk memenuhi permintaan. Coba lagi nanti, coba Zona Ketersediaan yang berbeda, atau coba permintaan yang lebih kecil. Jika aplikasi Anda fleksibel di semua tipe dan ukuran instans, coba atribut instans yang berbeda.
- Kuantitas yang diminta melebihi batas Instans Sesuai Permintaan Anda untuk keluarga instans yang dipilih. Tingkatkan batas Instans Sesuai Permintaan Anda untuk keluarga instans dan coba lagi. Untuk informasi selengkapnya, lihat Kuota Instans Sesuai Permintaan.

Topik

- Buat Reservasi Kapasitas untuk penggunaan segera
- Buat Reservasi Kapasitas masa depan

Buat Reservasi Kapasitas untuk penggunaan segera

Anda membuat Reservasi Kapasitas untuk penggunaan segera.

Console

Untuk membuat Reservasi Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Reservasi Kapasitas, lalu pilih Buat Reservasi Kapasitas.
3. Konfigurasikan pengaturan berikut di bagian Detail instans.
   a. Tipe Instance — Jenis instans untuk kapasitas cadangan.
   b. Platform — Sistem operasi untuk instans Anda. Untuk informasi selengkapnya, lihat Platform yang didukung.
   c. Availability Zone — Availability Zone untuk memesan kapasitas.
   d. Sewa - Jenis sewa yang digunakan untuk kapasitas cadangan. Pilih Default untuk menyimpan kapasitas pada perangkat keras bersama, atau Didedikasikan untuk kapasitas cadangan pada perangkat keras yang didedikasikan untuk akun Anda.
   e. (Opsional) Grup penempatan ARN — ARN dari grup penempatan cluster untuk membuat Reservasi Kapasitas. Untuk informasi selengkapnya, lihat Gunakan Reservasi Kapasitas dengan grup penempatan klaster.
   f. Jumlah instans total — Jumlah instance untuk kapasitas cadangan. Jika Anda menentukan kuantitas yang melebihi sisa kuota Instans Sesuai Permintaan untuk jenis instans yang dipilih, permintaan akan gagal.
4. Konfigurasikan pengaturan berikut di bagian Detail reservasi:
   a. Reservasi Kapasitas dimulai — Pilih Segera.
   b. Reservasi Kapasitas berakhir — Pilih salah satu opsi berikut:
      - Secara manual — Pesan kapasitas sampai Anda membatalkannya secara eksplisit.

- Waktu tertentu — Batalkan reservasi kapasitas secara otomatis pada tanggal dan waktu yang ditentukan.

c. Kelayakan instans - Pilih salah satu opsi berikut:

- open — (Default) Reservasi Kapasitas cocok dengan setiap instance yang memiliki atribut yang cocok (tipe instans, platform, Availability Zone, dan tenancy). Jika Anda meluncurkan sebuah instans dengan atribut yang cocok, atribut ditempatkan ke dalam kapasitas terpesan secara otomatis.
- Target — Reservasi Kapasitas hanya menerima instans yang memiliki atribut yang cocok (jenis instans, platform, Availability Zone, dan tenancy), dan yang secara eksplisit menargetkan reservasi.

5. Pilih Buat.

AWS CLI

Untuk membuat Reservasi Kapasitas

Gunakan perintah create-capacity-reservation.

```
aws ec2 create-capacity-reservation \
    --availability-zone az_name \
    --instance-type instance_type \
    --instance-count number_of_instances \
    --instance-platform operating_system \
    --instance-match-criteria open|targeted
```

PowerShell

Untuk membuat Reservasi Kapasitas

Gunakan Add-EC2CapacityReservationcmdlet.

```
Add-EC2CapacityReservation `
    -AvailabilityZone az_name `
    -InstanceType instance_type `
    -InstanceCount number_of_instances `
    -InstancePlatform operating_system `
    -InstanceMatchCriterion open|targeted
```

Buat Reservasi Kapasitas masa depan

Minta Reservasi Kapasitas masa depan jika Anda memerlukan kapasitas yang dipesan agar tersedia pada tanggal dan waktu mendatang.

Setelah Anda meminta Reservasi Kapasitas bertanggal di masa mendatang, permintaan akan menjalani penilaian untuk menentukan apakah dapat didukung. Untuk informasi selengkapnya, lihat Penilaian Reservasi Kapasitas Bertanggal di Masa Depan.

Pertimbangan

- Anda dapat meminta Reservasi Kapasitas bertanggal di masa mendatang untuk jenis instans dalam seri berikut: C, G, I, M, R, dan T.
- Anda dapat meminta Reservasi Kapasitas bertanggal di masa mendatang untuk jumlah instans dengan minimal 32 v. CPUs Misalnya, jika Anda meminta Reservasi Kapasitas bertanggal mendatang untuk `m5.xlarge` instans, Anda harus meminta kapasitas untuk setidaknya 8 instans (8 * m5.xlarge = 32 v). CPUs
- Anda dapat meminta Reservasi Kapasitas bertanggal antara 5 dan 120 hari sebelumnya. Namun, kami menyarankan Anda memintanya setidaknya 56 hari (8 minggu) sebelumnya untuk meningkatkan dukungan.
- Durasi komitmen minimum adalah 14 hari.

Console

Untuk membuat Reservasi Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Reservasi Kapasitas, lalu pilih Buat Reservasi Kapasitas.
3. Konfigurasikan pengaturan berikut di bagian Detail instans.
   a. Tipe Instance — Jenis instans untuk kapasitas cadangan.
   b. Platform — Sistem operasi untuk instans Anda. Untuk informasi selengkapnya, lihat Platform yang didukung.
   c. Availability Zone — Availability Zone untuk memesan kapasitas.
   d. Sewa - Jenis sewa yang digunakan untuk kapasitas cadangan. Pilih Default untuk menyimpan kapasitas pada perangkat keras bersama, atau Didedikasikan untuk kapasitas cadangan pada perangkat keras yang didedikasikan untuk akun Anda.

e. Jumlah instans total — Jumlah instance untuk kapasitas cadangan. Jika Anda menentukan kuantitas yang melebihi sisa kuota Instans Sesuai Permintaan untuk jenis instans yang dipilih, permintaan akan gagal.

4. Konfigurasikan pengaturan berikut di bagian Detail reservasi:

   a. Reservasi Kapasitas dimulai — Pilih Pada waktu tertentu.

   b. Tanggal mulai — Tentukan tanggal dan waktu di mana Reservasi Kapasitas harus tersedia untuk digunakan. Untuk informasi selengkapnya, lihat Tanggal dan waktu mulai.

   c. Durasi komitmen — Tentukan durasi minimum yang Anda lakukan untuk menjaga Reservasi Kapasitas setelah dikirimkan. Untuk informasi selengkapnya, lihat Durasi komitmen.

   d. Reservasi Kapasitas berakhir — Pilih salah satu opsi berikut:

      - Ketika saya membatalkannya — Pesan kapasitas sampai Anda membatalkannya secara eksplisit.
      - Waktu tertentu — Batalkan reservasi kapasitas secara otomatis pada tanggal dan waktu yang ditentukan.

5. Pilih Buat.

AWS CLI

Untuk membuat Reservasi Kapasitas

Gunakan perintah create-capacity-reservation.

```
aws ec2 create-capacity-reservation \
    --availability-zone az_name \
    --instance-type instance_type \
    --instance-count number_of_instances \
    --instance-platform operating_system \
    --instance-match-criteria targeted \
    --delivery-preference incremental \
    --commitment-duration commitment_in_seconds \
    --start-date YYYY-MMDDThh:mm:ss.sssZ
```

PowerShell

Untuk membuat Reservasi Kapasitas

Gunakan Add-EC2CapacityReservationcmdlet.

```
Add-EC2CapacityReservation `
    -AvailabilityZone az_name `
    -InstanceType instance_type `
    -InstanceCount number_of_instances `
    -InstancePlatform operating_system `
    -InstanceMatchCriterion targeted `
    -DeliveryPreference incremental `
    -CommitmentDuration commitment_in_seconds `
    -StartDate  YYYY-MMDDThh:mm:ss.sssZ
```

Lihat status Reservasi Kapasitas

Amazon EC2 terus memantau status Reservasi Kapasitas Anda.

Karena model konsistensi akhirnya diikuti oleh Amazon EC2 API, setelah Anda membuat Reservasi Kapasitas, diperlukan waktu hingga 5 menit agar status Reservasi Kapasitas mencerminkan kondisi tersebut. `active` Selama waktu ini, Reservasi Kapasitas mungkin tetap di `pending` negara bagian. Namun, mungkin sudah tersedia untuk digunakan, dalam hal ini upaya untuk meluncurkan instance ke Reservasi Kapasitas akan berhasil.

Console

Untuk melihat Reservasi Kapasitas Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.
3. Pilih Reservasi Kapasitas.

AWS CLI

Untuk menggambarkan Reservasi Kapasitas Anda

Gunakan perintah describe-capacity-reservations.

Misalnya, perintah berikut menjelaskan semua Reservasi Kapasitas.

```
aws ec2 describe-capacity-reservations
```

Berikut ini adalah output contoh.


```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-
group/MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
}
```

PowerShell

Untuk menggambarkan Reservasi Kapasitas

Gunakan Get-EC2CapacityReservationcmdlet.

```
Get-EC2CapacityReservation `
    -CapacityReservationId cr-1234abcd56EXAMPLE
```

Status Reservasi Kapasitas

Reservasi Kapasitas memiliki kemungkinan status berikut.

Status	Deskripsi
`active`	Kapasitas tersedia untuk digunakan.
`expired`	Reservasi Kapasitas berakhir secara otomatis pada tanggal dan waktu yang ditentukan dalam permintaan reservasi Anda. Kapasitas terpesan tidak lagi tersedia untuk Anda gunakan.
`cancelled`	Reservasi Kapasitas dibatalkan. Kapasitas terpesan tidak lagi tersedia untuk Anda gunakan.
`pending`	Permintaan Reservasi Kapasitas berhasil tetapi penyediaan kapasitas masih tertunda.
`failed`	Permintaan Reservasi Kapasitas gagal. Permintaan dapat gagal karena parameter permintaan yang tidak valid, batasan kapasitas, atau batasan batas instans. Anda dapat melihat permintaan yang gagal selama 60 menit.
`scheduled`	(Hanya Reservasi Kapasitas Bertanggal Masa Depan) Permintaa n Reservasi Kapasitas masa depan telah disetujui dan Reservasi Kapasitas dijadwalkan untuk pengiriman pada tanggal mulai yang diminta.
`assessing`	(Hanya Reservasi Kapasitas Bertanggal di Masa Depan) Amazon EC2 sedang menilai permintaan Anda untuk Reservasi Kapasitas bertangga

Status	Deskripsi
	l mendatang. Untuk informasi selengkapnya, lihat Penilaian Reservasi Kapasitas Bertanggal di Masa Depan.
`delayed`	(Hanya Reservasi Kapasitas Bertanggal Masa Depan) Amazon EC2 mengalami penundaan dalam penyediaan Reservasi Kapasitas bertanggal mendatang yang diminta. Amazon EC2 tidak dapat mengirimkan kapasitas yang diminta berdasarkan tanggal dan waktu mulai yang diminta.
`unsupported`	(Hanya Reservasi Kapasitas Bertanggal di Masa Depan) Amazon EC2 tidak dapat mendukung permintaan Reservasi Kapasitas bertanggal mendatang karena kendala kapasitas. Anda dapat melihat permintaan yang tidak didukung selama 30 hari. Reservasi Kapasitas tidak akan dikirimkan.

Luncurkan instans ke dalam Reservasi Kapasitas yang ada

Anda hanya dapat meluncurkan instance ke Reservasi Kapasitas yang:

- Memiliki atribut yang cocok (tipe instance, platform, Availability Zone, dan tenancy)
- Memiliki kapasitas yang cukup
- Berada di `active` negara bagian

Saat Anda meluncurkan sebuah instans, Anda dapat menentukan apakah akan meluncurkan instans tersebut ke salah satu Reservasi Kapasitas `open`, ke dalam Reservasi Kapasitas tertentu, atau ke dalam kelompok Reservasi Kapasitas.

Atau, Anda dapat mengonfigurasi instans agar tidak berjalan di Reservasi Kapasitas, meskipun Anda memiliki Reservasi Kapasitas `open` yang cocok dengan atribut dan kapasitas yang tersedia.

Meluncurkan sebuah instans ke dalam Reservasi Kapasitas mengurangi kapasitasnya yang tersedia dengan jumlah instans yang diluncurkan. Misalnya, jika Anda meluncurkan tiga instans, kapasitas Reservasi Kapasitas yang tersedia dikurangi tiga.

Console

Untuk meluncurkan instance ke Reservasi Kapasitas yang ada

1. Ikuti prosedur untuk meluncurkan instance, tetapi jangan meluncurkan instance sampai Anda menyelesaikan langkah-langkah berikut untuk menentukan pengaturan untuk grup penempatan dan Reservasi Kapasitas.
2. Perluas Detail lanjutan dan lakukan hal berikut:

   a. Untuk grup Penempatan, pilih grup penempatan cluster untuk meluncurkan instance.

   b. Untuk Reservasi Kapasitas, pilih salah satu opsi berikut, tergantung pada konfigurasi Reservasi Kapasitas:

      - Tidak Ada — Mencegah instans diluncurkan ke Reservasi Kapasitas. Instans berjalan dalam kapasitas Sesuai Permintaan.
      - Buka — Meluncurkan instans ke Reservasi Kapasitas apa pun yang memiliki atribut yang cocok dan kapasitas yang cukup untuk jumlah instans yang Anda pilih. Jika tidak ada Reservasi Kapasitas yang sesuai dengan kapasitas yang memadai, instans akan menggunakan kapasitas Sesuai Permintaan.
      - Tentukan Reservasi Kapasitas — Meluncurkan instans ke Reservasi Kapasitas yang dipilih. Jika Reservasi Kapasitas yang dipilih tidak memiliki kapasitas yang cukup untuk jumlah instans yang Anda pilih, peluncuran instans akan gagal.
      - Tentukan grup sumber daya Reservasi Kapasitas — Meluncurkan instans ke Reservasi Kapasitas apa pun dengan atribut yang cocok dan kapasitas yang tersedia di grup Reservasi Kapasitas yang dipilih. Jika grup yang dipilih tidak memiliki Reservasi Kapasitas dengan atribut yang sesuai dan kapasitas yang tersedia, instans diluncurkan ke dalam kapasitas Sesuai Permintaan.
      - Tentukan Reservasi Kapasitas saja — Meluncurkan instans ke dalam Reservasi Kapasitas. Jika ID Reservasi Kapasitas tidak ditentukan, instans akan diluncurkan ke Reservasi Kapasitas terbuka. Jika kapasitas tidak tersedia, instance gagal diluncurkan.
      - Tentukan grup sumber daya Reservasi Kapasitas saja — Meluncurkan instans ke dalam Reservasi Kapasitas dalam grup sumber daya Reservasi Kapasitas. Jika grup sumber daya Reservasi Kapasitas ARN tidak ditentukan, instans akan diluncurkan ke Reservasi Kapasitas terbuka. Jika kapasitas tidak tersedia, instance gagal diluncurkan.
3. Di panel Ringkasan, tinjau konfigurasi instans Anda, lalu pilih Luncurkan instans.

AWS CLI

Untuk meluncurkan instance ke Reservasi Kapasitas yang ada

Gunakan perintah run-instance dan tentukan opsi. `--capacity-reservation-specification`

Contoh berikut meluncurkan instance ke Reservasi Kapasitas terbuka dengan atribut yang cocok dan kapasitas yang tersedia:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification CapacityReservationPreference=open
```

Contoh berikut meluncurkan instance ke Reservasi `targeted` Kapasitas:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationTarget={CapacityReservationId=cr-1234abcd56EXAMPLE}
```

Contoh berikut meluncurkan instance ke grup Reservasi Kapasitas yang ditentukan:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-2:123456789012:group/my-cr-group}
```

Contoh berikut meluncurkan instance ke Reservasi Kapasitas saja. Karena tidak menentukan ID Reservasi Kapasitas, instans akan diluncurkan di Reservasi Kapasitas terbuka apa pun dengan atribut yang cocok dan kapasitas yang tersedia:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-only
```

Contoh berikut meluncurkan instance ke Reservasi Kapasitas tertentu saja. Jika kapasitas tidak tersedia dalam Reservasi Kapasitas yang ditentukan, instans gagal diluncurkan.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-only \
        CapacityReservationTarget={CapacityReservationId=cr-1234abcd56EXAMPLE}
```

PowerShell

Untuk meluncurkan instance ke Reservasi Kapasitas yang ada

Gunakan New-EC2Instancecmdlet.

Contoh berikut meluncurkan instance ke Reservasi Kapasitas terbuka dengan atribut yang cocok dan kapasitas yang tersedia:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "open"
```

Contoh berikut meluncurkan instance ke Reservasi `targeted` Kapasitas:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationId cr-1234abcd56EXAMPLE
```

Contoh berikut meluncurkan instance ke grup Reservasi Kapasitas yang ditentukan:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationResourceGroupArn `
        "arn:aws:resource-groups:us-west-2:123456789012:group/my-cr-group"
```

Contoh berikut meluncurkan instance ke Reservasi Kapasitas saja. Karena tidak menentukan ID Reservasi Kapasitas, instans akan diluncurkan di Reservasi Kapasitas terbuka apa pun dengan atribut yang cocok dan kapasitas yang tersedia:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservations-only"
```

Contoh berikut meluncurkan instance ke Reservasi Kapasitas tertentu saja. Jika kapasitas tidak tersedia dalam Reservasi Kapasitas yang ditentukan, instans gagal diluncurkan.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservations-only" `
```

```
    -CapacityReservationTarget_CapacityReservationId cr-1234abcd56EXAMPLE
```

Ubah Reservasi Kapasitas yang aktif

Jika Anda memiliki Reservasi Kapasitas yang sudah ada yang tidak cocok untuk beban kerja yang membutuhkan kapasitas, Anda dapat mengubah kuantitas instans, kelayakan instans (`open`atau`targeted`), dan waktu akhir (`At specific time`atau). `Manually` Jika Anda menentukan kuantitas instans baru yang melebihi batas Instans Sesuai Permintaan yang tersisa untuk jenis instans yang dipilih, pembaruan akan gagal.

Modifikasi yang diizinkan tergantung pada status Reservasi Kapasitas:

- `assessing`atau `scheduled` negara - Anda hanya dapat memodifikasi tag.
- `pending`state - Anda tidak dapat mengubah Reservasi Kapasitas dengan cara apa pun.
- `active`status tetapi masih dalam durasi komitmen — Anda tidak dapat mengurangi jumlah instans di bawah jumlah instans yang dikomit, atau menetapkan tanggal akhir yang sebelum durasi komitmen. Semua modifikasi lainnya diperbolehkan.
- `active`negara tanpa durasi komitmen atau durasi komitmen yang telah berlalu — Semua modifikasi diperbolehkan.
- `expired`,`cancelled`,`unsupported`, atau `failed` negara - Anda tidak dapat mengubah Reservasi Kapasitas dengan cara apa pun.

Pertimbangan-pertimbangan

- Anda tidak dapat mengubah jenis instance, platform, Availability Zone, atau tenancy setelah pembuatan. Jika Anda perlu mengubah salah satu atribut ini, kami menyarankan Anda untuk membatalkan reservasi, dan kemudian membuat yang baru dengan atribut yang diperlukan.
- Jika Anda mengubah Reservasi Kapasitas yang ada dengan mengubah kelayakan instans dari `targeted` menjadi`open`, setiap instans yang berjalan yang cocok dengan atribut Reservasi Kapasitas, `CapacityReservationPreference` parameter disetel ke, dan belum berjalan dalam Reservasi Kapasitas`open`, akan secara otomatis menggunakan Reservasi Kapasitas yang dimodifikasi.
- Untuk mengubah kelayakan instans, Reservasi Kapasitas harus benar-benar tidak digunakan (penggunaan nol) karena Amazon EC2 tidak dapat mengubah kelayakan instans saat instans berjalan di dalam reservasi.

Console

Untuk mengubah Reservasi Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Reservasi Kapasitas, pilih Reservasi Kapasitas yang akan dimodifikasi, lalu pilih Edit.
3. Ubah opsi Total kapasitas, Reservasi Kapasitas, atau kelayakan Instans sesuai kebutuhan, dan pilih Simpan.

AWS CLI

Untuk mengubah Reservasi Kapasitas

Gunakan perintah modify-capacity-reservation. Contoh berikut memodifikasi Reservasi Kapasitas yang ditentukan untuk kapasitas cadangan untuk delapan instans.

```
aws ec2 modify-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --instance-count 8
```

PowerShell

Untuk mengubah Reservasi Kapasitas

Gunakan Edit-EC2CapacityReservationcmdlet. Contoh berikut memodifikasi Reservasi Kapasitas yang ditentukan untuk kapasitas cadangan untuk delapan instans.

```
Edit-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0 `
    -InstanceCount 8
```

Ubah pengaturan Reservasi Kapasitas instans Anda

Anda dapat memodifikasi pengaturan Reservasi Kapasitas berikut untuk instans yang berhenti kapan saja:

- Mulai di Reservasi Kapasitas apa pun yang memiliki atribut yang cocok (jenis instans, platform, Availability Zone, dan tenancy) dan kapasitas yang tersedia.

- Mulai instans di Reservasi Kapasitas tertentu.
- Mulailah di Reservasi Kapasitas apa pun yang memiliki kecocokan atribut dan ketersediaan kapasitas di grup Reservasi Kapasitas
- Mencegah instans dimulai dalam Reservasi Kapasitas.

Console

Untuk mengubah pengaturan Reservasi Kapasitas contoh

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Instans dan pilih instans yang akan dimodifikasi. Hentikan instans jika belum dihentikan.
3. Pilih Tindakan, Pengaturan instans, Ubah Pengaturan Reservasi Kapasitas.
4. Untuk Reservasi Kapasitas, pilih salah satu opsi berikut:
   - Buka — Meluncurkan instans ke Reservasi Kapasitas apa pun yang memiliki atribut yang cocok dan kapasitas yang cukup untuk jumlah instans yang Anda pilih. Jika tidak ada Reservasi Kapasitas yang sesuai dengan kapasitas yang memadai, instans akan menggunakan kapasitas Sesuai Permintaan.
   - Tidak Ada — Mencegah instans diluncurkan ke Reservasi Kapasitas. Instans berjalan dalam kapasitas Sesuai Permintaan.
   - Tentukan Reservasi Kapasitas — Meluncurkan instans ke Reservasi Kapasitas yang dipilih. Jika Reservasi Kapasitas yang dipilih tidak memiliki kapasitas yang cukup untuk jumlah instans yang Anda pilih, peluncuran instans akan gagal.
   - Tentukan grup Reservasi Kapasitas — Meluncurkan instans ke Reservasi Kapasitas apa pun dengan atribut yang cocok dan kapasitas yang tersedia di grup Reservasi Kapasitas yang dipilih. Jika grup yang dipilih tidak memiliki Reservasi Kapasitas dengan atribut yang sesuai dan kapasitas yang tersedia, instans diluncurkan ke dalam kapasitas Sesuai Permintaan.
   - Tentukan Reservasi Kapasitas saja — Meluncurkan instans ke dalam Reservasi Kapasitas. Jika ID Reservasi Kapasitas tidak ditentukan, instans akan diluncurkan ke Reservasi Kapasitas terbuka. Jika kapasitas tidak tersedia, instance gagal diluncurkan.
   - Tentukan grup sumber daya Reservasi Kapasitas saja — Meluncurkan instans ke dalam Reservasi Kapasitas dalam grup sumber daya Reservasi Kapasitas. Jika grup sumber daya Reservasi Kapasitas ARN tidak ditentukan, instans akan diluncurkan ke Reservasi Kapasitas terbuka. Jika kapasitas tidak tersedia, instance gagal diluncurkan.

AWS CLI

Untuk mengubah pengaturan Reservasi Kapasitas contoh

Gunakan perintah modify-instance-capacity-reservation-attributes.

Contoh berikut mengubah preferensi Reservasi Kapasitas menjadinone.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification CapacityReservationPreference=none
```

Contoh berikut target untuk Reservasi Kapasitas tertentu.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
    CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Contoh berikut mengubah target ke grup Reservasi Kapasitas tertentu.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-2:123456789012:group/my-cr-group}
```

Contoh berikut mengubah preferensi Reservasi Kapasitas menjadicapacity-reservation-only. Karena tidak menentukan Reservasi Kapasitas, instans diluncurkan ke Reservasi Kapasitas terbuka dengan atribut yang cocok dan kapasitas yang tersedia.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification CapacityReservationPreference=capacity-
reservation-only
```

Contoh berikut mengubah preferensi Reservasi Kapasitas capacity-reservation-only dan mengubah target ke Reservasi Kapasitas tertentu. Jika kapasitas tidak tersedia di Reservasi Kapasitas yang ditentukan, instans gagal diluncurkan.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservation-only \
        CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

PowerShell

Untuk mengubah pengaturan Reservasi Kapasitas contoh

Gunakan Edit-EC2InstanceCapacityReservationAttributecmdlet.

Contoh berikut mengubah preferensi Reservasi Kapasitas menjadinone.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "none"
```

Contoh berikut target untuk Reservasi Kapasitas tertentu.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationTarget_CapacityReservationId cr-1234567890abcdef0
```

Contoh berikut mengubah target ke grup Reservasi Kapasitas tertentu.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationTarget_CapacityReservationResourceGroupArn `
        "arn:aws:resource-groups:us-west-2:123456789012:group/my-cr-group"
```

Contoh berikut mengubah preferensi Reservasi Kapasitas menjadi`capacity-reservation-only`. Karena tidak menentukan Reservasi Kapasitas, instans diluncurkan ke Reservasi Kapasitas terbuka dengan atribut yang cocok dan kapasitas yang tersedia.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservation-only"
```

Contoh berikut mengubah preferensi Reservasi Kapasitas `capacity-reservation-only` dan mengubah target ke Reservasi Kapasitas tertentu. Jika kapasitas tidak tersedia di Reservasi Kapasitas yang ditentukan, instans gagal diluncurkan.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservation-only" `
    -CapacityReservationTarget_CapacityReservationId cr-1234567890abcdef0
```

Pindahkan kapasitas antara Reservasi Kapasitas

Anda dapat memindahkan kapasitas dari satu Reservasi Kapasitas ke Reservasi Kapasitas lainnya untuk mendistribusikan kembali sumber daya komputasi yang Anda pesan sesuai kebutuhan. Misalnya, jika Anda memerlukan kapasitas tambahan dalam reservasi dengan penggunaan yang terus meningkat, dan Anda memiliki kapasitas yang tersedia di reservasi lain, maka Anda dapat mengalokasikan kembali kapasitas tersebut di antara kedua reservasi tersebut.

Prasyarat untuk kapasitas bergerak

Sebagai prasyarat, kedua Reservasi Kapasitas harus memenuhi persyaratan berikut:

- Kedua reservasi harus dalam keadaan aktif.
- Kedua reservasi harus dimiliki oleh Anda Akun AWS. Anda tidak dapat memindahkan kapasitas antar reservasi yang dimiliki oleh yang berbeda Akun AWS.
- Kedua reservasi harus memiliki hal yang sama:
  - Tipe instans
  - Platform
  - Zona Ketersediaan
  - Penghunian
  - Grup penempatan
  - Waktu akhir

Kelayakan instans Reservasi Kapasitas tujuan (`openatautargeted`), dan tag, tidak harus cocok dengan reservasi sumber. Konfigurasi kedua reservasi tetap sama, kecuali bahwa reservasi sumber telah mengurangi kapasitas dan reservasi tujuan telah meningkatkan kapasitas.

Saat Anda menentukan jumlah instans yang akan dipindahkan, secara default, kapasitas apa pun yang tersedia dipindahkan terlebih dahulu, diikuti oleh instans berjalan yang memenuhi syarat (kapasitas yang digunakan dalam reservasi Anda). Misalnya, jika Anda memindahkan 4 instance dari reservasi dengan 5 instance yang digunakan dan 3 instance yang tersedia, maka 3 instance yang tersedia dan 1 instance yang digunakan akan dipindahkan.

> **Note**
>
> Ketika Anda memindahkan kapasitas yang digunakan dari reservasi Anda dengan menentukan Jumlah yang akan dipindahkan yang lebih besar dari kapasitas yang tersedia, hanya contoh yang diluncurkan dengan Spesifikasi Reservasi Kapasitas yang `open` akan dipindahkan.

Pertimbangan-pertimbangan

Pertimbangan berikut berlaku saat memindahkan kapasitas dari satu reservasi ke reservasi lainnya:

- Kapasitas yang digunakan hanya dapat dipindahkan antara Reservasi Kapasitas dengan kelayakan `open` instans yang dibagikan dengan kumpulan akun yang sama.
- Saat Anda memindahkan kapasitas yang digunakan, instance yang memenuhi syarat akan dipilih secara acak. Anda tidak dapat menentukan instance yang sedang berjalan dipindahkan. Jika jumlah yang cukup dari instance yang memenuhi syarat tidak ditemukan untuk memenuhi kuantitas pemindahan, operasi pemindahan akan gagal.
- Jika Anda memindahkan semua kapasitas dari reservasi sumber, Reservasi Kapasitas akan dibatalkan secara otomatis.
- Reservasi Kapasitas Bertanggal Masa Depan — Anda tidak dapat memindahkan kapasitas untuk Reservasi Kapasitas masa depan selama periode komitmen.

> **Note**
>
> Memindahkan kapasitas dari Blok Kapasitas tidak didukung.

Pindahkan kapasitas

Anda dapat memindahkan kapasitas dari Reservasi Kapasitas sumber ke Reservasi Kapasitas tujuan.

Console

Untuk memindahkan kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Reservasi Kapasitas.
3. Pilih ID Reservasi Kapasitas Sesuai Permintaan yang memiliki kapasitas untuk dipindahkan.
4. Di bawah Tindakan, Kelola kapasitas, pilih Pindahkan.
5. Pada halaman Pindahkan kapasitas, di bawah Reservasi Kapasitas Tujuan, pilih reservasi dari daftar.
6. Di bawah Kuantitas untuk memindahkan, gunakan penggeser atau ketik jumlah instans untuk berpindah dari Reservasi Kapasitas sumber ke Reservasi Kapasitas tujuan.
7. Tinjau ringkasan, dan saat Anda siap, pilih Pindahkan.

AWS CLI

Untuk memindahkan kapasitas

Gunakan perintah move-capacity-reservation-instances. Contoh berikut memindahkan 10 instance dari Reservasi Kapasitas sumber yang ditentukan ke Reservasi Kapasitas tujuan yang ditentukan.

```
aws ec2 move-capacity-reservation-instances \
    --source-capacity-reservation-id cr-1234567890abcdef0 \
    --destination-capacity-reservation-id cr-021345abcdef56789 \
    --instance-count 10
```

PowerShell

Untuk memindahkan kapasitas

Gunakan Move-EC2CapacityReservationInstancecmdlet. Contoh berikut memindahkan 10 instance dari Reservasi Kapasitas sumber yang ditentukan ke Reservasi Kapasitas tujuan yang ditentukan.

```
Move-EC2CapacityReservationInstance `
    -SourceCapacityReservationId cr-1234567890abcdef0 `
    -DestinationCapacityReservationId cr-021345abcdef56789 `
    -InstanceCount 10
```

Memisahkan kapasitas dari Reservasi Kapasitas yang ada

Anda dapat memisahkan kapasitas dari Reservasi Kapasitas yang ada untuk membuat reservasi baru. Dengan membagi kapasitas, Anda mengalokasikan sebagian dari reservasi awal ke beban kerja tertentu atau membagikannya dengan yang lain. Akun AWS Misalnya, untuk berbagi sebagian Reservasi Kapasitas dengan akun lain, Anda dapat memisahkan sebagian kapasitas untuk membuat Reservasi Kapasitas berukuran lebih kecil. Reservasi Kapasitas yang lebih kecil kemudian dapat dibagikan dengan akun lain menggunakan AWS Resource Access Manager.

Ketika Anda membagi kapasitas dari Reservasi Kapasitas yang ada, Reservasi Kapasitas baru akan dibuat secara otomatis. Reservasi yang ada tidak akan berubah, kecuali untuk pengurangan kapasitas total dari jumlah instans yang dipisahkan. Instans yang berjalan di Reservasi Kapasitas yang ada tidak terpengaruh. Anda dapat membagi reservasi yang ada menjadi hanya satu Reservasi Kapasitas baru.

Reservasi Kapasitas baru akan memiliki konfigurasi yang sama dengan Reservasi Kapasitas yang ada kecuali tag. Secara default, Reservasi Kapasitas baru tidak memiliki tag apa pun. Anda dapat menentukan tag baru selama operasi split. Reservasi Kapasitas baru juga dapat dimodifikasi setelah dibuat, jika perlu.

Bila Anda menentukan jumlah instans yang akan dibagi, secara default, kapasitas apa pun yang tersedia dibagi terlebih dahulu, diikuti oleh instans berjalan yang memenuhi syarat (kapasitas yang digunakan dalam reservasi Anda). Misalnya: jika Anda membagi 4 instance dari Reservasi Kapasitas dengan 5 instans yang digunakan dan 3 instans yang tersedia, maka 3 instans yang tersedia dan 1 instance yang digunakan akan dibagi menjadi reservasi baru.

Prasyarat untuk kapasitas pemisahan

Sebagai prasyarat, Reservasi Kapasitas Anda harus memenuhi persyaratan berikut:

- Reservasi sumber harus dalam keadaan aktif.
- Reservasi sumber harus dimiliki oleh Anda Akun AWS.

> **Note**
>
> Ketika Anda membagi kapasitas yang digunakan dari reservasi Anda dengan menentukan Kuantitas untuk membagi yang lebih besar dari kapasitas yang tersedia, hanya contoh yang diluncurkan dengan Spesifikasi Reservasi Kapasitas yang `open` akan dibagi.

Pertimbangan-pertimbangan

Pertimbangan berikut berlaku saat memisahkan kapasitas dari satu reservasi ke reservasi baru:

- Kapasitas yang digunakan hanya dapat dibagi untuk Reservasi Kapasitas dengan kelayakan instans “terbuka” yang tidak dibagikan dengan akun apa pun.
- Saat Anda membagi kapasitas yang digunakan, instance yang memenuhi syarat akan dipilih secara acak. Anda tidak dapat menentukan instance berjalan mana yang dibagi. Jika jumlah yang cukup dari instans yang memenuhi syarat tidak ditemukan untuk memenuhi kuantitas split, operasi split akan gagal.
- Jumlah maksimum instans untuk dipisahkan dari reservasi yang ada adalah ukuran reservasi dikurangi satu. Misalnya, jika total kapasitas reservasi Anda adalah 5 instans, Anda dapat membagi maksimal 4 instans menjadi reservasi baru.
- Reservasi Kapasitas Bertanggal Masa Depan — Anda tidak dapat membagi kapasitas untuk Reservasi Kapasitas masa depan selama periode komitmen.
- Grup sumber daya — Jika Reservasi Kapasitas yang ada milik grup sumber daya, Reservasi Kapasitas baru tidak akan ditambahkan secara otomatis ke grup sumber daya. Anda dapat menambahkan Reservasi Kapasitas baru ke grup sumber daya setelah dibuat, jika perlu.
- Berbagi — Jika Reservasi Kapasitas yang ada dibagikan dengan akun konsumen, Reservasi Kapasitas baru tidak akan dibagikan secara otomatis dengan akun konsumen. Anda dapat membagikan Reservasi Kapasitas baru setelah dibuat, jika perlu.
- Grup penempatan klaster — Jika Reservasi Kapasitas yang ada merupakan bagian dari grup penempatan klaster, Reservasi Kapasitas baru akan dibuat dalam grup penempatan klaster yang sama.

> **Note**
>
> Memisahkan kapasitas dari Blok Kapasitas tidak didukung.

Akses kontrol untuk membagi Reservasi Kapasitas menggunakan tag

Anda dapat menggunakan tag untuk mengontrol akses ke sumber daya Amazon EC2, termasuk memisahkan kapasitas dari Reservasi Kapasitas yang ada untuk membuat Reservasi Kapasitas baru. Untuk informasi selengkapnya, lihat Mengontrol akses ke AWS sumber daya menggunakan tag di Panduan Pengguna IAM.

Untuk mengontrol akses pemisahan Reservasi Kapasitas menggunakan tag, pastikan Anda menentukan tag sumber daya dan permintaan dalam pernyataan kebijakan karena kebijakan IAM dievaluasi terhadap Reservasi Kapasitas sumber dan Reservasi Kapasitas yang baru dibuat. Contoh kebijakan berikut mencakup kunci `ec2:ResourceTag` kondisi dengan tag `Owner=ExampleDepartment1` untuk Reservasi Kapasitas sumber dan kunci `ec2:RequestTag` kondisi dengan tag `stack=production` untuk Reservasi Kapasitas yang baru dibuat.

```
{
  "Statement": [
    {
      "Sid": "AllowSourceCapacityReservation",
      "Effect": "Allow",
      "Action": "ec2:CreateCapacityReservationBySplitting",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:capacity-reservation/
cr-1234567890abcdef0",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Owner": "ExampleDepartment1"
        }
      }
    },
    {
      "Sid": "AllowNewlyCreatedCapacityReservation",
      "Effect": "Allow",
      "Action": ["ec2:CreateCapacityReservationBySplitting", "ec2:CreateTags"],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:capacity-reservation/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/stack": "production"
        }
      }
    }
  ]
}
```

Memisahkan kapasitas

Anda dapat memisahkan kapasitas dari Reservasi Kapasitas yang ada untuk membuat Reservasi Kapasitas baru.

Console

Untuk memisahkan kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Reservasi Kapasitas.
3. Pilih ID Reservasi Kapasitas Sesuai Permintaan yang memiliki kapasitas untuk dibagi.
4. Di bawah Tindakan, Kelola kapasitas, pilih Split.
5. Pada halaman Split Capacity Reservation, di bawah Quantity to split, gunakan slider atau ketik jumlah instans untuk memisahkan dari reservasi saat ini.
6. (Opsional) Tambahkan tag untuk Reservasi Kapasitas baru.
7. Tinjau ringkasan, dan ketika Anda siap, pilih Split.

AWS CLI

Untuk memisahkan kapasitas

Gunakan perintah `create-capacity-reservation-by-splitting`. Contoh berikut membuat Reservasi Kapasitas baru dengan memisahkan 10 instance dari Reservasi Kapasitas yang ditentukan.

```
aws ec2 create-capacity-reservation-by-splitting \
    --source-capacity-reservation-id cr-1234567890abdef0 \
    --instance-count 10
```

PowerShell

Untuk memisahkan kapasitas

Gunakan New-EC2CapacityReservationBySplittingcmdlet. Contoh berikut membuat Reservasi Kapasitas baru dengan memisahkan 10 instance dari Reservasi Kapasitas yang ditentukan.

```
New-EC2CapacityReservationBySplitting `
    -SourceCapacityReservationId cr-1234567890abdef0 `
    -InstanceCount 10
```

Membatalkan Reservasi Kapasitas

Anda dapat membatalkan Reservasi Kapasitas yang berada di salah satu negara bagian berikut:

- `assessing`
- `active`dan tidak ada durasi komitmen atau durasi komitmen telah berlalu. Anda tidak dapat membatalkan Reservasi Kapasitas bertanggal di masa depan selama durasi komitmen.

> **Note**
>
> Anda tidak dapat mengubah atau membatalkan Blok Kapasitas. Untuk informasi selengkapnya, lihat Blok Kapasitas untuk ML.

Jika Reservasi Kapasitas bertanggal masa depan memasuki `delayed` negara bagian, durasi komitmen dibebaskan, dan Anda dapat membatalkannya segera setelah memasuki negara bagian. `active`

Saat Anda membatalkan Reservasi Kapasitas, kapasitas segera dilepaskan dan tidak lagi dipesan untuk Anda gunakan.

Anda dapat membatalkan Reservasi Kapasitas yang kosong dan Reservasi Kapasitas yang memiliki instans berjalan. Jika Anda membatalkan Reservasi Kapasitas yang menjalankan instans, instans tetap berjalan normal di luar reservasi kapasitas dengan tarif Instans Sesuai Permintaan standar atau dengan tarif diskon jika Anda memiliki Savings Plans atau Instans Cadangan Regional yang cocok.

Setelah Anda membatalkan Reservasi Kapasitas, instans yang menargetkannya tidak dapat diluncurkan lagi. Modifikasi instans ini sehingga mereka menargetkan Reservasi Kapasitas yang berbeda, meluncurkan Reservasi Kapasitas terbuka dengan atribut yang cocok dan kapasitas yang memadai, atau menghindari peluncuran ke Reservasi Kapasitas. Untuk informasi selengkapnya, lihat Ubah pengaturan Reservasi Kapasitas instans Anda.

Console

Untuk membatalkan Reservasi Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Reservasi Kapasitas dan pilih Rserrvasi Kapasitas untuk dibatalkan.

3. Pilih Batalkan reservasi, Batalkan reservasi.

AWS CLI

Untuk membatalkan Reservasi Kapasitas

Gunakan perintah cancel-capacity-reservation.

```
aws ec2 cancel-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0
```

PowerShell

Untuk membatalkan Reservasi Kapasitas

Gunakan Remove-EC2CapacityReservationcmdlet.

```
Remove-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0
```

Gunakan Reservasi Kapasitas dengan grup penempatan klaster

Anda dapat membuat Reservasi Kapasitas dalam grup penempatan klaster untuk memesan kapasitas komputasi Amazon EC2 untuk beban kerja Anda. Grup penempatan klaster menawarkan manfaat latensi jaringan yang rendah dan throughput jaringan yang tinggi.

Membuat Reservasi Kapasitas di grup penempatan klaster memastikan bahwa Anda memiliki akses ke kapasitas komputasi di grup penempatan klaster saat Anda membutuhkannya, selama Anda membutuhkannya. Ini sangat ideal untuk memesan kapasitas untuk beban kerja berkinerja tinggi (HPC) yang memerlukan penskalaan komputasi. Hal ini memungkinkan Anda untuk menurunkan skala klaster Anda sambil memastikan bahwa kapasitas tetap tersedia untuk Anda gunakan sehingga Anda dapat meningkatkan skala kembali saat diperlukan.

Setelah membuat Reservasi Kapasitas di grup penempatan klaster, Anda dapat membagikannya dengan AWS akun lain. Untuk informasi selengkapnya, lihat Berbagi Kapasitas Reservasi dalam kelompok penempatan klaster.

Topik

- Batasan
- Bekerja dengan Reservasi Kapasitas dalam grup penempatan klaster
- Berbagi Kapasitas Reservasi dalam kelompok penempatan klaster

Batasan

Ingatlah hal-hal berikut saat membuat Reservasi Kapasitas dalam grup penempatan klaster:

- Jika Reservasi Kapasitas yang ada tidak ada dalam grup penempatan, Anda tidak dapat mengubah Reservasi Kapasitas untuk memesan kapasitas dalam grup penempatan. Untuk reservasi kapasitas dalam grup penempatan, Anda harus membuat Reservasi Kapasitas di grup penempatan.
- Setelah membuat Reservasi Kapasitas di grup penempatan, Anda tidak dapat mengubahnya untuk memesan kapasitas di luar grup penempatan.
- Anda dapat meningkatkan kapasitas terpesan Anda dalam grup penempatan dengan memodifikasi Reservasi Kapasitas yang ada di grup penempatan, atau dengan membuat Reservasi Kapasitas tambahan di grup penempatan. Namun, Anda meningkatkan peluang Anda untuk mendapatkan kesalahan kapasitas yang tidak mencukupi.
- Anda dapat berbagi Reservasi Kapasitas hanya dari grup penempatan klaster yang Anda miliki. Anda tidak dapat membagikan Reservasi Kapasitas dari grup penempatan klaster yang tidak Anda miliki.
- Anda tidak dapat menghapus grup penempatan klaster yang memiliki Reservasi Kapasitas `active`. Anda harus membatalkan semua Reservasi Kapasitas di grup penempatan klaster sebelum Anda dapat menghapusnya.

Bekerja dengan Reservasi Kapasitas dalam grup penempatan klaster

Untuk mulai menggunakan Reservasi Kapasitas dengan grup penempatan klaster, lakukan langkah-langkah berikut.

> **Note**
>
> Jika Anda ingin membuat Reservasi Kapasitas di grup penempatan klaster yang ada, lewati Langkah 1. Kemudian, untuk Langkah 2 dan 3, tentukan ARN dari grup penempatan klaster yang ada.

Tugas

- Langkah 1: (Bersyarat) Buat grup penempatan klaster untuk digunakan dengan Reservasi Kapasitas
- Langkah 2: Buat Reservasi Kapasitas di grup penempatan klaster
- Langkah 3: Luncurkan instance ke Reservasi Kapasitas dalam grup penempatan klaster

Langkah 1: (Bersyarat) Buat grup penempatan klaster untuk digunakan dengan Reservasi Kapasitas

Lakukan langkah ini hanya jika Anda perlu membuat grup penempatan klaster baru. Untuk menggunakan grup penempatan klaster yang ada, lewati langkah ini dan untuk Langkah 2 serta 3, gunakan ARN dari grup penempatan klaster tersebut.

Console

Untuk membuat grup penempatan cluster

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Grup Penempatan, lalu pilih Buat grup penempatan.
3. Untuk Nama, tentukan nama deskriptif untuk grup penempatan.
4. Untuk Strategi penempatan, pilih Klaster.
5. Pilih Buat grup.
6. Dalam tabel Grup penempatan, di kolom ARN Grup, catat ARN grup penempatan klaster yang Anda buat. Anda akan membutuhkannya untuk langkah selanjutnya.

AWS CLI

Untuk membuat grup penempatan cluster

Gunakan perintah create-placement-group.

```
aws ec2 create-placement-group \
    --group-name MyPG \
    --strategy cluster
```

Catat grup penempatan ARN yang dikembalikan dalam output, karena Anda akan membutuhkannya untuk langkah berikutnya.

PowerShell

Untuk membuat grup penempatan cluster

Gunakan New-EC2PlacementGroupcmdlet.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy "cluster"
```

Catat grup penempatan ARN yang dikembalikan dalam output, karena Anda akan membutuhkannya untuk langkah berikutnya.

Langkah 2: Buat Reservasi Kapasitas di grup penempatan klaster

Anda membuat Reservasi Kapasitas dalam grup penempatan klaster dengan cara yang sama seperti Anda membuat Reservasi Kapasitas apa pun. Namun, Anda juga harus menentukan ARN grup penempatan klaster tempat membuat Reservasi Kapasitas.

Pertimbangan-pertimbangan

- Grup penempatan klaster yang ditentukan harus dalam status `available`. Jika grup penempatan klaster berada dalam status `pending`, `deleting`, atau `deleted`, permintaan akan gagal.
- Reservasi Kapasitas dan grup penempatan klaster harus berada di Zona Ketersediaan yang sama. Jika permintaan untuk membuat Reservasi Kapasitas menentukan Zona Ketersediaan yang berbeda dari grup penempatan klaster, permintaan gagal.
- Anda dapat membuat Reservasi Kapasitas hanya untuk tipe instans yang didukung oleh grup penempatan klaster. Jika Anda menentukan tipe instans yang tidak didukung, permintaan gagal.
- Jika Anda membuat Reservasi Kapasitas `open` dalam grup penempatan klaster dan ada instans berjalan yang memiliki atribut yang cocok (ARN grup penempatan, tipe instans, Zona Ketersediaan, platform, dan penghunian), instans tersebut secara otomatis berjalan di Reservasi Kapasitas.
- Permintaan Anda untuk membuat Reservasi Kapasitas bisa gagal jika salah satu dari yang berikut ini benar:
  - Amazon EC2 tidak memiliki kapasitas yang cukup untuk memenuhi permintaan. Coba lagi nanti, coba Zona Ketersediaan yang berbeda, atau coba kapasitas yang lebih kecil. Jika beban kerja Anda fleksibel di semua tipe dan ukuran instans, coba atribut instans yang berbeda.

- Kuantitas yang diminta melebihi batas Instans Sesuai Permintaan Anda untuk keluarga instans yang dipilih. Tingkatkan batas Instans Sesuai Permintaan Anda untuk keluarga instans dan coba lagi. Untuk informasi selengkapnya, lihat Kuota Instans Sesuai Permintaan.

Console

Untuk membuat Reservasi Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Reservasi Kapasitas, lalu pilih Buat Reservasi Kapasitas.
3. Pada halaman Buat Reservasi Kapasitas, tentukan jenis instans, platform, Availability Zone, Tenancy, quantity, dan tanggal akhir sesuai kebutuhan.
4. Untuk grup Penempatan, pilih ARN dari grup penempatan klaster untuk membuat Reservasi Kapasitas.
5. Pilih Buat.

Untuk informasi selengkapnya, lihat Membuat Reservasi Kapasitas.

AWS CLI

Untuk membuat Reservasi Kapasitas

Gunakan perintah create-capacity-reservation. Untuk `--placement-group-arn`, tentukan ARN grup penempatan klaster tempat membuat Reservasi Kapasitas.

```
aws ec2 create-capacity-reservation \
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone-id az_id \
    --instance-count quantity \
    --placement-group-arn "placement_group_arn"
```

PowerShell

Untuk membuat Reservasi Kapasitas

Gunakan Add-EC2CapacityReservationcmdlet. Untuk `-PlacementGroupArn`, tentukan ARN grup penempatan klaster tempat membuat Reservasi Kapasitas.

```
Add-EC2CapacityReservation `
    -InstanceType instance_type `
    -InstancePlatform platform `
    -AvailabilityZoneId az_id `
    -InstanceCount quantity `
    -PlacementGroupArn "placement_group_arn"
```

Langkah 3: Luncurkan instance ke Reservasi Kapasitas dalam grup penempatan klaster

Anda dapat meluncurkan instance ke Reservasi Kapasitas yang ada di grup penempatan klaster dengan salah satu opsi berikut:

- Menentukan ARN grup penempatan klaster yang akan digunakan untuk meluncurkan instance — Saat Anda menyediakan ARN grup penempatan klaster, Amazon EC2 meluncurkan instance ke grup penempatan klaster tersebut. Gunakan salah satu metode berikut:
  - Menentukan *open* — Anda tidak perlu menentukan Reservasi Kapasitas dalam permintaan peluncuran instans. Jika instans memiliki atribut (grup penempatan ARN, tipe instans, Zona Ketersediaan, platform, dan penghunian) yang cocok dengan Reservasi Kapasitas dalam grup penempatan yang ditentukan, instans secara otomatis berjalan di Reservasi Kapasitas.
  - Menentukan Reservasi Kapasitas — Jika Reservasi Kapasitas hanya menerima peluncuran instans yang ditargetkan, Anda harus menentukan Reservasi Kapasitas target selain grup penempatan klaster dalam permintaan.
  - Menentukan grup Reservasi Kapasitas — Untuk informasi selengkapnya, lihat Menggunakan Reservasi Kapasitas di grup penempatan klaster dengan grup Reservasi Kapasitas.
- Menentukan hanya grup Reservasi Kapasitas — Untuk informasi selengkapnya, lihat Menggunakan Reservasi Kapasitas di grup penempatan klaster dengan grup Reservasi Kapasitas.
- Menentukan hanya Reservasi Kapasitas — Anda dapat meluncurkan instance ke Reservasi Kapasitas dalam grup penempatan klaster.

> **Note**
>
> Saat Anda meluncurkan instance dengan hanya menentukan Reservasi Kapasitas atau hanya grup Reservasi Kapasitas, instans akan diluncurkan ke Reservasi Kapasitas yang dibuat di grup penempatan klaster, tetapi instance tidak langsung dilampirkan ke grup penempatan klaster.

Console

Untuk meluncurkan instance ke Reservasi Kapasitas yang ada

1. Ikuti prosedur untuk meluncurkan instance, tetapi jangan meluncurkan instance sampai Anda menyelesaikan langkah-langkah berikut untuk menentukan pengaturan untuk grup penempatan dan Reservasi Kapasitas.
2. Perluas Detail lanjutan dan lakukan hal berikut:
   a. Untuk grup Penempatan, pilih grup penempatan cluster untuk meluncurkan instance.
   b. Untuk Reservasi Kapasitas, pilih salah satu opsi berikut, tergantung pada konfigurasi Reservasi Kapasitas:
      - Buka — Untuk meluncurkan instans ke Reservasi open Kapasitas apa pun di grup penempatan klaster yang memiliki atribut yang cocok dan kapasitas yang memadai.
      - Target berdasarkan ID — Untuk meluncurkan instans ke Reservasi Kapasitas yang hanya menerima peluncuran instans yang ditargetkan.
      - Targetkan berdasarkan grup — Untuk meluncurkan instans ke Reservasi Kapasitas apa pun dengan atribut yang cocok dan kapasitas yang tersedia di grup Reservasi Kapasitas yang dipilih.
3. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

AWS CLI

Untuk meluncurkan instance ke Reservasi Kapasitas yang ada

Gunakan perintah run-instans. Jika Anda perlu menargetkan Reservasi Kapasitas atau grup Reservasi Kapasitas tertentu, tentukan parameter `--capacity-reservation-specification`. Untuk `--placement`, tentukan parameter `GroupName` lalu tentukan nama grup penempatan yang Anda buat di langkah sebelumnya.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
```

```
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=cluster_placement_group_name"
```

PowerShell

Untuk meluncurkan instance ke Reservasi Kapasitas yang ada

Gunakan New-EC2Instancecmdlet. Untuk `-Placement`, tentukan parameter `GroupName` lalu tentukan nama grup penempatan yang Anda buat di langkah sebelumnya.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType instance_type `
    -KeyName key_pair_name `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationId capacity_reservation_id `
    -Placement_GroupName cluster_placement_group_name
```

Berbagi Kapasitas Reservasi dalam kelompok penempatan klaster

Anda dapat berbagi Reservasi Kapasitas dalam grup penempatan klaster hanya dengan membagikan Reservasi Kapasitas, atau dengan membagikan Reservasi Kapasitas dan grup penempatan klaster tempat reservasi tersebut dibuat.

Dengan hanya membagikan Reservasi Kapasitas, Anda memberikan akses akun konsumen ke Reservasi Kapasitas tersebut saja. Akun konsumen tidak memiliki visibilitas atau akses ke grup penempatan klaster tempat Reservasi Kapasitas dibuat. Ini memberi Anda kontrol halus atas akses akun konsumen. Akun konsumen tidak dapat melihat informasi apa pun tentang grup penempatan klaster, termasuk ARN-nya.

Saat Anda berbagi grup penempatan klaster dan Reservasi Kapasitas, grup penempatan klaster akan terlihat dan dapat diakses oleh akun konsumen. Mereka dapat meluncurkan instance dan membuat Reservasi Kapasitas mereka sendiri di dalamnya.

Untuk informasi selengkapnya, lihat sumber daya berikut ini.

- Luncurkan instans ke Reservasi Kapasitas dalam grup penempatan klaster
- Reservasi Kapasitas Bersama

- Grup penempatan bersama

Grup Reservasi Kapasitas

Anda dapat menggunakan AWS Resource Groups untuk membuat koleksi logis dari Reservasi Kapasitas, yang disebut grup sumber daya. Kelompok sumber daya adalah pengelompokan AWS sumber daya yang logis yang semuanya berada di AWS Wilayah yang sama. Untuk informasi selenhkapnya tentang grup sumber daya, lihat Apa Itu Grup Sumber Daya? di Panduan Pengguna AWS Resource Groups .

Anda dapat menyertakan Reservasi Kapasitas yang Anda miliki di akun Anda, dan Reservasi Kapasitas yang dibagikan dengan Anda oleh AWS akun lain dalam satu grup sumber daya. Anda juga dapat menyertakan Reservasi Kapasitas yang memiliki atribut berbeda (jenis instans, platform, Availability Zone, dan tenancy) dalam satu grup sumber daya.

Saat Anda membuat grup sumber daya untuk Reservasi Kapasitas, Anda dapat menargetkan instans ke grup Reservasi Kapasitas alih-alih Reservasi Kapasitas individu. Instans yang menargetkan grup Reservasi Kapasitas cocok dengan Reservasi Kapasitas apa pun dalam grup yang memiliki atribut yang cocok (jenis instans, platform, Availability Zone, dan tenancy) dan kapasitas yang tersedia. Jika grup yang dipilih tidak memiliki Reservasi Kapasitas dengan atribut yang cocok dan kapasitas yang tersedia, instans berjalan menggunakan kapasitas Sesuai Permintaan. Jika Reservasi Kapasitas yang cocok ditambahkan ke grup yang ditargetkan di tahap selanjutnya, instans secara otomatis dicocokkan dengan dan dipindahkan ke kapasitas terpesan.

Untuk mencegah penggunaan Reservasi Kapasitas yang tidak disengaja dalam grup, konfigurasikan Reservasi Kapasitas dalam grup untuk menerima hanya instans yang secara eksplisit menargetkan reservasi kapasitas. Untuk melakukannya, setel kelayakan Instans ke Hanya instans yang menentukan reservasi ini saat membuat Reservasi Kapasitas menggunakan konsol Amazon EC2. Saat menggunakan AWS CLI, tentukan `--instance-match-criteria targeted` saat membuat reservasi kapasitas. Melakukan ini memastikan bahwa hanya instans yang secara eksplisit menargetkan grup, atau Reservasi Kapasitas dalam grup, yang dapat berjalan di grup.

Jika Reservasi Kapasitas dalam grup dibatalkan atau kedaluwarsa saat memiliki instans yang sedang berjalan, instans tersebut secara otomatis dipindahkan ke Reservasi Kapasitas lain dalam grup yang memiliki kecocokan atribut dan ketersediaan kapasitas. Jika tidak ada Reservasi Kapasitas yang tersisa di grup yang memiliki kecocokan atribut dan ketersediaan kapasitas, instans berjalan dalam kapasitas Sesuai Permintaan. Jika Reservasi Kapasitas yang cocok ditambahkan ke grup yang ditargetkan di tahap selanjutnya, instans secara otomatis dipindahkan ke kapasitas terpesan.

Tugas

- Membuat gru[Reservasi Kapasitas
- Tambahkan Reservasi Kapasitas ke grup
- Menghapus Reservasi Kapasitas dari grup
- Menghapus grup Reservasi Kapasitas
- Menggunakan Reservasi Kapasitas dalam grup penempatan klaster dengan grup Reservasi Kapasitas

Membuat gru[Reservasi Kapasitas

Anda dapat menggunakan contoh berikut untuk membuat grup sumber daya untuk Reservasi Kapasitas dengan parameter permintaan berikut.

- `AWS::EC2::CapacityReservationPool`— Memastikan bahwa kelompok sumber daya dapat ditargetkan misalnya peluncuran.
- `AWS::ResourceGroups::Generic`dengan `allowed-resource-types` disetel ke `AWS::EC2::CapacityReservation` - Memastikan bahwa grup sumber daya hanya menerima Reservasi Kapasitas.

Setelah membuat grup, Anda dapat menambahkan Reservasi Kapasitas ke grup.

AWS CLI

Untuk membuat grup untuk Reservasi Kapasitas

Gunakan perintah create-group AWS CLI .

```
aws resource-groups create-group \
    --name MyCRGroup \
    --configuration \
        '{"Type": "AWS::EC2::CapacityReservationPool"}' \
        '{"Type": "AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-
resource-types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

PowerShell

Untuk membuat grup untuk Reservasi Kapasitas

Gunakan New- RGGroup cmdlet.

```
New-RGGroup `
    -Name MyCRGroup `
    -Configuration `
        @{"Type"="AWS::EC2::CapacityReserationPool"} `
        @{"Type"="AWS::ResourceGroups::Generic"; "Parameters"=@{"allowed-resource-
types"=@{"Values"="AWS::EC2::CapacityReservations"}}}
```

Tambahkan Reservasi Kapasitas ke grup

Jika Anda menambahkan Reservasi Kapasitas yang dibagikan dengan Anda ke grup, dan Reservasi Kapasitas tersebut tidak dibagikan, tetapi akan dihapus secara otomatis dari grup.

AWS CLI

Untuk menambahkan Reservasi Kapasitas ke grup

Gunakan perintah group-resources.

Contoh berikut menambahkan dua Reservasi Kapasitas ke grup yang ditentukan.

```
aws resource-groups group-resources \
    --group MyCRGroup \
    --resource-arns \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1
 \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

PowerShell

Untuk menambahkan Reservasi Kapasitas ke grup

Gunakan RGResourceAdd-cmdlet.

Contoh berikut menambahkan dua Reservasi Kapasitas ke grup yang ditentukan.

```
Add-RGResource `
    -Group MyCRGroup `
    -ResourceArn `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-1234567890abcdef1", `
```

```
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-54321abcdef567890"
```

Menghapus Reservasi Kapasitas dari grup

Anda dapat menggunakan contoh berikut untuk menghapus Reservasi Kapasitas dari grup.

AWS CLI

Untuk menghapus Reservasi Kapasitas dari grup

Gunakan perintah ungroup-resources.

Contoh berikut menghapus dua Reservasi Kapasitas dari grup yang ditentukan.

```
aws resource-groups ungroup-resources \
    --group MyCRGroup \
    --resource-arns \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd
 \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

PowerShell

Untuk menghapus Reservasi Kapasitas dari grup

Gunakan Hapus- RGResource cmdlet.

Contoh berikut menghapus dua Reservasi Kapasitas dari grup yang ditentukan.

```
Remove-RGResource `
    -Group MyCRGroup `
    -ResourceArn `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-0e154d26a16094dd", `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-54321abcdef567890"
```

Menghapus grup Reservasi Kapasitas

Anda dapat menggunakan contoh berikut untuk menghapus grup Reservasi Kapasitas.

AWS CLI

Untuk menghapus grup

Gunakan perintah hapus-grup.

```
aws resource-groups delete-group --group MyCRGroup
```

PowerShell

Untuk menghapus grup

Gunakan Hapus- RGGroup cmdlet.

```
Remove-RGGroup -GroupName MyCRGroup
```

Menggunakan Reservasi Kapasitas dalam grup penempatan klaster dengan grup Reservasi Kapasitas

Amazon EC2 menyediakan metode peluncuran yang berbeda bagi Anda untuk menggunakan Reservasi Kapasitas dalam grup penempatan klaster dengan grup Reservasi Kapasitas. Anda dapat memilih salah satu metode berikut untuk menargetkan grup Reservasi Kapasitas berdasarkan persyaratan beban kerja Anda:

- Menentukan ARN grup penempatan klaster dan grup Reservasi Kapasitas — Ini akan menggunakan Reservasi Kapasitas yang tersedia dengan atribut yang cocok dan kapasitas yang tersedia dalam grup Reservasi Kapasitas yang dipilih. Jika grup yang dipilih tidak memiliki Reservasi Kapasitas dengan atribut yang sesuai dan kapasitas yang tersedia, instans diluncurkan ke dalam kapasitas Sesuai Permintaan.

  > **Note**
  >
  > Saat Anda meluncurkan instance menggunakan metode ini, instance ditempatkan di grup penempatan cluster yang ditentukan.

- Menentukan hanya grup Reservasi Kapasitas — Ini akan menggunakan semua kapasitas yang tersedia dalam grup Reservasi Kapasitas dengan hanya menentukan grup Reservasi Kapasitas. Saat meluncurkan instance, kapasitas digunakan dalam urutan sebagai berikut:
  - Reservasi Kapasitas tidak terkait dengan grup penempatan klaster mana pun.

- Reservasi Kapasitas di grup penempatan klaster mana pun dalam grup Reservasi Kapasitas.
- Jika grup tidak memiliki Reservasi Kapasitas dengan atribut yang cocok dan kapasitas yang tersedia, instans berjalan menggunakan kapasitas Sesuai Permintaan dan tidak ditempatkan di grup penempatan klaster mana pun.

> **Note**
>
> Saat Anda meluncurkan instance dengan hanya menentukan grup Reservasi Kapasitas, instance akan diluncurkan ke Reservasi Kapasitas yang dibuat di grup penempatan klaster, tetapi instance tidak langsung dilampirkan ke grup penempatan klaster.

Reservasi Kapasitas di Local Zones

Zona Lokal adalah perpanjangan dari AWS Wilayah yang secara geografis dekat dengan pengguna Anda. Sumber daya yang dibuat di Zona Lokal dapat melayani pengguna lokal dengan komunikasi latensi sangat rendah. Untuk informasi selengkapnya, lihat AWS Local Zones.

Anda dapat memperluas VPC dari AWS Wilayah induknya ke Zona Lokal dengan membuat subnet baru di Zona Lokal tersebut. Saat Anda membuat subnet di Zona Lokal, VPC Anda diperluas ke Zona Lokal itu. Subnet di Zona Lokal beroperasi sama dengan subnet lain di VPC Anda.

Dengan Local Zones, Anda dapat menempatkan Reservasi Kapasitas di banyak lokasi yang lebih dekat dengan pengguna Anda. Anda membuat dan menggunakan Reservasi Kapasitas di Local Zones dengan cara yang sama seperti Anda membuat dan menggunakan Reservasi Kapasitas di Zona Ketersediaan biasa. Fitur yang sama dan perilaku pencocokan contoh berlaku. Untuk informasi selengkapnya tentang model harga yang didukung di Local Zones, lihat AWS Local Zones FAQs.

Pertimbangan-pertimbangan

Anda tidak dapat menggunakan grup Reservasi Kapasitas dalam Zona Lokal.

Untuk menggunakan Reservasi Kapasitas di Zona Lokal

1. Aktifkan Zona Lokal untuk digunakan di AWS akun Anda. Untuk informasi selengkapnya, lihat Memulai AWS Local Zones di Panduan Pengguna AWS Local Zones.
2. Buat Reservasi Kapasitas di Zona Lokal. Untuk Zona Ketersediaan, pilih Zona Lokal. Zona Lokal ditunjukkan oleh kode Wilayah AWS dan diikuti oleh pengidentifikasi yang menunjukkan

lokasinya, misalnya `us-west-2-lax-1a`. Untuk informasi selengkapnya, lihat Membuat Reservasi Kapasitas.

3. Buat subnet di Zona Lokal. Untuk Zona Ketersediaan, pilih Zona Lokal. Untuk informasi selengkapnya, lihat Membuat subnet di VPC Anda dalam Panduan Pengguna Amazon VPC.
4. Luncurkan sebuah instans. Untuk Subnet, pilih subnet di Zona Lokal (misalnya `subnet-123abc | us-west-2-lax-1a`), dan untuk Reservasi Kapasitas, pilih spesifikasi (baik `open` atau targetkan menurut ID) yang diperlukan untuk Reservasi Kapasitas yang Anda buat di Zona Lokal. Untuk informasi selengkapnya, lihat Luncurkan instans ke dalam Reservasi Kapasitas yang ada.

Reservasi Kapasitas di Wavelength Zones

AWS Wavelength memungkinkan developer untuk membangun aplikasi yang menghasilkan latensi sangat rendah untuk perangkat seluler dan pengguna akhir. Wavelength melakukan deployment layanan komputasi dan penyimpanan AWS standar ke edge jaringan 5G operator telekomunikasi. Anda dapat memperluas Amazon Virtual Private Cloud (VPC) ke satu atau beberapa Wavelength Zones. Anda kemudian dapat menggunakan AWS sumber daya seperti instans Amazon EC2 untuk menjalankan aplikasi yang memerlukan latensi sangat rendah dan koneksi ke AWS layanan di Wilayah. Untuk informasi selengkapnya, lihat AWS Wavelength Zones.

Saat Anda membuat Reservasi Kapasitas Sesuai Permintaan, Anda dapat memilih Zona Wavelength dan Anda dapat meluncurkan instans ke dalam Reservasi Kapasitas dalam Zona Wavelength dengan menentukan subnet yang terkait dengan Zona Wavelength. Zona Wavelength diwakili oleh kode Wilayah diikuti oleh AWS pengidentifikasi yang menunjukkan lokasi, misalnya. `us-east-1-wl1-bos-wlz-1`

Wavelength Zones tidak tersedia di setiap Wilayah. Untuk informasi tentang Wilayah yang mendukung Wavelength Zones, lihat Wavelength Zones yang Tersedia di Panduan Developer AWS Wavelength .

Pertimbangan-pertimbangan

Anda tidak dapat menggunakan grup Reservasi Kapasitas dalam Zona Wavelength.

Untuk menggunakan Reservasi Kapasitas di Zona Wavelength

1. Aktifkan Wavelength Zone untuk digunakan di akun Anda. AWS Untuk informasi selengkapnya, lihat Memulai dengan AWS Wavelength di Panduan Developer AWS Wavelength .

2. Buat Reservasi Kapasitas di Zona Wavelength. Untuk Zona Ketersediaan, pilih Wavelength. Wavelength ditunjukkan oleh kode Wilayah AWS dan diikuti oleh pengidentifikasi yang menunjukkan lokasinya, misalnya `us-east-1-wl1-bos-wlz-1`. Untuk informasi selengkapnya, lihat Membuat Reservasi Kapasitas.
3. Buat subnet di Zona Wavelength. Untuk Zona Ketersediaan, pilih Zona Wavelength. Untuk informasi selengkapnya, lihat Membuat subnet di VPC Anda dalam Panduan Pengguna Amazon VPC.
4. Luncurkan sebuah instans. Untuk Subnet, pilih subnet di Wavelength Zone (misalnya `subnet-123abc | us-east-1-wl1-bos-wlz-1`), dan untuk Reservasi Kapasitas, pilih spesifikasi (baik `open` atau targetkan menurut ID) yang diperlukan untuk reservasi Kapasitas yang Anda buat di Wavelength. Untuk informasi selengkapnya, lihat Luncurkan instans ke dalam Reservasi Kapasitas yang ada.

Reservasi Kapasitas di AWS Outposts

AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, layanan APIs, dan alat ke tempat pelanggan. Dengan menyediakan akses lokal ke infrastruktur AWS terkelola, AWS Outposts memungkinkan pelanggan untuk membangun dan menjalankan aplikasi di tempat menggunakan antarmuka pemrograman yang sama seperti di AWS Wilayah, sambil menggunakan sumber daya komputasi dan penyimpanan lokal untuk latensi yang lebih rendah dan kebutuhan pemrosesan data lokal.

Outpost adalah kumpulan kapasitas AWS komputasi dan penyimpanan yang digunakan di situs pelanggan. AWS mengoperasikan, memantau, dan mengelola kapasitas ini sebagai bagian dari suatu AWS Wilayah.

Anda dapat membuat Reservasi Kapasitas pada Outposts yang telah Anda buat di akun Anda. Hal ini memungkinkan Anda untuk memesan kapasitas komputasi pada Outpost di situs Anda. Anda membuat dan menggunakan Reservasi Kapasitas di Outposts dengan cara yang sama seperti Anda membuat dan menggunakan Reservasi Kapasitas di Zona Ketersediaan biasa. Fitur yang sama dan perilaku pencocokan instans yang berlaku.

Anda juga dapat membagikan Reservasi Kapasitas di Outposts dengan akun AWS lain dalam organisasi Anda menggunakan. AWS Resource Access Manager Untuk informasi selengkapnya tentang berbagi Reservasi Kapasitas, lihat Reservasi Kapasitas Bersama.

Prasyarat

Anda harus menginstal Outpost di situs Anda. Untuk informasi selengkapnya, lihat Membuat Outpost dan memesan kapasitas Outpost di Panduan Pengguna AWS Outposts .

Pertimbangan-pertimbangan

- Anda tidak dapat menggunakan grup Reservasi Kapasitas di Outpost.

Untuk menggunakan Reservasi Kapasitas di Outpost

1. Buat subnet pada Outpost. Untuk informasi selengkapnya, lihat Membuat subnet di Panduan Pengguna AWS Outposts .
2. Buat Reservasi Kapasitas di Outpost.
   a. Buka AWS Outposts konsol di https://console.aws.amazon.com/outposts/.
   b. Di panel navigasi, pilih Outposts, lalu pilih Tindakan, Buat Reservasi Kapasitas.
   c. Konfigurasikan Reservasi Kapasitas sesuai kebutuhan kemudian pilih Buat. Untuk informasi selengkapnya, lihat Membuat Reservasi Kapasitas.

   > **Note**
   >
   > Daftar tarik-turun Tipe Instans hanya mencantumkan tipe instans yang didukung oleh Outpost yang dipilih, dan tarik-turun Zona Ketersediaan hanya mencantumkan Zona Ketersediaan yang terkait dengan Outpost yang dipilih.
3. Luncurkan sebuah instans ke dalam Reservasi Kapasitas. Untuk Subnet, pilih subnet yang Anda buat di Langkah 1, dan untuk Reservasi Kapasitas, pilih Reservasi Kapasitas yang Anda buat pada Langkah 2. Untuk informasi selengkapnya, lihat Meluncurkan instans pada Outpost di Panduan Pengguna AWS Outposts .

Reservasi Kapasitas Bersama

Pembagian Reservasi Kapasitas memungkinkan pemilik Reservasi Kapasitas untuk berbagi kapasitas cadangan mereka dengan AWS akun lain atau di dalam AWS organisasi. Hal ini memungkinkan Anda untuk membuat dan mengelola Reservasi Kapasitas secara terpusat, dan berbagi kapasitas cadangan di beberapa AWS akun atau dalam organisasi Anda AWS .

Dalam model ini, AWS akun yang memiliki Reservasi Kapasitas (pemilik) membagikannya dengan AWS akun lain (konsumen). Konsumen dapat meluncurkan instans ke Reservasi Kapasitas yang

dibagikan dengan mereka dengan cara yang sama seperti mereka meluncurkan instans ke Reservasi Kapasitas yang mereka miliki di akun mereka sendiri. Pemilik Reservasi Kapasitas bertanggung jawab untuk mengelola Reservasi Kapasitas dan instans yang diluncurkan ke dalamnya. Pemilik tidak dapat memodifikasi instans yang diluncurkan konsumen ke Reservasi Kapasitas yang telah mereka bagikan. Konsumen bertanggung jawab untuk mengelola instans yang mereka luncurkan ke Reservasi Kapasitas yang dibagikan dengan mereka. Konsumen tidak dapat menampilkan atau memodifikasi instans yang dimiliki oleh konsumen lain atau oleh pemilik Reservasi Kapasitas.

Pemilik Reservasi Kapasitas dapat berbagi Reservasi Kapasitas dengan:

- AWS Akun spesifik di dalam atau di luar AWS organisasinya
- Unit organisasi di dalam AWS organisasinya
- Seluruh AWS organisasinya

Prasyarat untuk berbagi Reservasi Kapasitas

- Untuk berbagi Reservasi Kapasitas, Anda harus memilikinya di AWS akun Anda. Anda tidak dapat membagikan Reservasi Kapasitas yang telah dibagikan dengan Anda.
- Anda hanya dapat berbagi Reservasi Kapasitas untuk instans penghunian bersama. Anda tidak dapat membagikan Reservasi Kapasitas untuk instans penghunian khusus.
- Kapasitas Berbagi reservasi tidak tersedia untuk AWS akun atau AWS akun baru yang memiliki riwayat penagihan terbatas.
- Untuk berbagi Reservasi Kapasitas dengan AWS organisasi Anda atau unit organisasi di AWS organisasi Anda, Anda harus mengaktifkan berbagi dengan AWS Organizations. Untuk informasi selengkapnya, lihat Aktifkan Berbagi dengan AWS Organizations dalam Panduan Pengguna AWS RAM .
- Anda dapat membagikan Reservasi Kapasitas di `active` atau `scheduled` negara bagian. Anda tidak dapat berbagi Reservasi Kapasitas di negara bagian lain, seperti `assessing` atau`unsupported`.

Layanan terkait

Pembagian Reservasi Kapasitas terintegrasi dengan AWS Resource Access Manager (AWS RAM). AWS RAM adalah layanan yang memungkinkan Anda untuk berbagi AWS sumber daya Anda dengan AWS akun apa pun atau melalui AWS Organizations. Dengan AWS RAM, Anda dapat berbagi sumber daya yang Anda miliki dengan membuat berbagi sumber daya. Pembagian

sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan dibagikan. Konsumen dapat berupa AWS akun individu, atau unit organisasi atau seluruh organisasi dari AWS Organizations.

Untuk informasi selengkapnya AWS RAM, lihat Panduan AWS RAM Pengguna.

Berbagi di seluruh Zona Ketersediaan

Untuk memastikan bahwa sumber daya didistribusikan di seluruh Zona Ketersediaan untuk suatu Wilayah, kami secara independen memetakan Zona Ketersediaan ke nama untuk setiap akun . Hal ini dapat menyebabkan perbedaan penamaan Zona Ketersediaan di seluruh akun. Misalnya, Availability Zone `us-east-1a` untuk AWS akun Anda mungkin tidak memiliki lokasi yang sama dengan AWS akun lain. `us-east-1a`

Untuk mengidentifikasi lokasi Reservasi Kapasitas Anda yang terkait dengan akun Anda, Anda harus menggunakan ID Zona Ketersediaan (AZ ID). ID AZ adalah pengidentifikasi unik dan konsisten untuk Availability Zone di semua AWS akun. Misalnya, `use1-az1` adalah ID AZ untuk `us-east-1` Wilayah dan itu adalah lokasi yang sama di setiap AWS akun.

Untuk melihat AZ IDs untuk Availability Zones di akun Anda

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/rumah.
2. AZ IDs untuk Wilayah saat ini ditampilkan di panel ID AZ Anda di sisi kanan layar.

Berbagi Reservasi Kapasitas

Ketika Anda berbagi Reservasi Kapasitas yang Anda miliki dengan orang lain Akun AWS, Anda memungkinkan mereka untuk meluncurkan instans ke dalam kapasitas cadangan Anda. Jika Anda berbagi Reservasi Kapasitas terbuka, perhatikan hal berikut karena dapat mengakibatkan penggunaan Reservasi Kapasitas yang tidak diinginkan:

- Jika konsumen memiliki instans berjalan yang cocok dengan atribut Reservasi Kapasitas, mengatur parameter `CapacityReservationPreference` ke `open`, tetapi belum berjalan dalam kapasitas terpesan, mereka secara otomatis menggunakan Reservasi Kapasitas bersama.
- Jika konsumen meluncurkan instance yang memiliki atribut yang cocok (jenis instans, platform, Availability Zone, dan tenancy) dan `CapacityReservationPreference` parameter disetel ke`open`, mereka secara otomatis meluncurkan ke Reservasi Kapasitas bersama.

Untuk membagikan Reservasi Kapasitas, Anda harus menambahkannya ke berbagi sumber daya. Berbagi sumber daya adalah AWS RAM sumber daya yang memungkinkan Anda berbagi sumber daya di seluruh AWS akun. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan berbagi dengan mereka. Saat Anda berbagi Reservasi Kapasitas menggunakan konsol Amazon EC2, Anda menambahkannya ke berbagi sumber daya yang ada. Untuk menambahkan Reservasi Kapasitas ke berbagi sumber daya baru, Anda harus membuat pembagian sumber daya menggunakan konsol AWS RAM.

Jika Anda adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, konsumen di organisasi Anda diberikan akses ke Reservasi Kapasitas bersama jika prasyarat untuk berbagi terpenuhi. Jika Reservasi Kapasitas dibagikan dengan akun eksternal, mereka menerima undangan untuk bergabung dengan berbagi sumber daya dan diberikan akses ke Reservasi Kapasitas bersama setelah menerima undangan.

> **Important**
>
> Sebelum meluncurkan instance ke Reservasi Kapasitas yang dibagikan dengan Anda, verifikasi bahwa Anda memiliki akses ke Reservasi Kapasitas bersama dengan melihatnya di konsol atau dengan menjelaskannya menggunakan perintah. describe-capacity-reservations AWS CLI Jika Anda dapat melihat Reservasi Kapasitas bersama di konsol atau menjelaskannya menggunakan AWS CLI, itu tersedia untuk Anda gunakan dan Anda dapat meluncurkan instance ke dalamnya. Jika Anda mencoba meluncurkan instans ke dalam Reservasi Kapasitas dan instans tidak dapat diakses karena kegagalan berbagi, instans akan diluncurkan ke kapasitas Sesuai Permintaan.

Console

Untuk membagikan Reservasi Kapasitas yang Anda miliki menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.
3. Pilih Reservasi Kapasitas untuk dibagikan dan pilih Tindakan, Bagikan reservasi.
4. Pilih bagian sumber daya yang ingin ditambahkan Reservasi Kapasitas dan pilih Bagikan Reservasi Kapasitas.

   Butuh beberapa menit bagi konsumen untuk mendapatkan akses ke Reservasi Kapasitas bersama.

Untuk berbagi Reservasi Kapasitas yang Anda miliki menggunakan AWS RAM konsol

Lihat Membuat berbagi sumber daya di Panduan AWS RAM Pengguna.

AWS CLI

Untuk berbagi Reservasi Kapasitas yang Anda miliki

Gunakan perintah create-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Untuk berbagi Reservasi Kapasitas yang Anda miliki

Gunakan cmdlet New- RAMResource Share.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

Berhenti membagikan Reservasi Kapasitas

Pemilik Reservasi Kapasitas dapat berhenti membagikan Reservasi Kapasitas kapan saja. Aturan-aturan berikut berlaku:

- Instans yang dimiliki oleh konsumen yang berjalan dalam kapasitas bersama pada saat pembagian berhenti terus berjalan secara normal di luar kapasitas terpesan, dan kapasitas dikembalikan ke Reservasi Kapasitas sesuai dengan ketersediaan kapasitas Amazon EC2.
- Konsumen dengan siapa Reservasi Kapasitas dibagikan tidak dapat lagi meluncurkan instans baru ke dalam kapasitas terpesan.

Untuk berhenti berbagi Reservasi Kapasitas yang Anda miliki, Anda harus menghapusnya dari berbagi sumber daya.

Console

Untuk membagikan Reservasi Kapasitas yang Anda miliki menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.
3. Pilih Reservasi Kapasitas dan pilih tab Berbagi.
4. Tab Berbagi menampilkan daftar sumber daya tempat Reservasi Kapasitas ditambahkan. Pilih bagian sumber daya tempat Reservasi Kapasitas dihapus dan pilih Hapus dari pembagian sumber daya.

Untuk berhenti membagikan Reservasi Kapasitas yang Anda miliki menggunakan AWS RAM konsol

Lihat Memperbarui Sumber Daya Bersama di Panduan Pengguna AWS RAM .

AWS CLI

Untuk berhenti berbagi Reservasi Kapasitas yang Anda miliki

Gunakan perintah disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
 --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Untuk berhenti berbagi Reservasi Kapasitas yang Anda miliki

Gunakan cmdlet Putus- RAMResource Bagikan.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE"
```

Penugasan penagihan untuk Reservasi Kapasitas Amazon EC2 bersama

Secara default, ketika Reservasi Kapasitas dibagikan, pemilik ditagih untuk instans yang mereka jalankan dalam Reservasi Kapasitas dan untuk kapasitas apa pun yang tersedia, juga disebut kapasitas yang tidak terpakai, dalam Reservasi Kapasitas; sementara konsumen hanya ditagih untuk instans yang mereka jalankan dalam Reservasi Kapasitas bersama.

Jika diperlukan, pemilik Reservasi Kapasitas dapat menetapkan tagihan kapasitas apa pun yang tersedia dalam Reservasi Kapasitas ke salah satu akun tempat Reservasi Kapasitas dibagikan. Setelah penagihan ditetapkan ke akun lain, akun tersebut menjadi pemilik tagihan dari kapasitas apa pun yang tersedia dalam Reservasi Kapasitas. Setiap biaya untuk kapasitas yang tersedia dalam Reservasi Kapasitas, mulai saat itu dan seterusnya, ditagih ke akun yang ditetapkan, bukan akun pemilik. Pemilik Reservasi Kapasitas dan akun yang digunakan bersama Reservasi Kapasitas terus ditagih untuk instans yang dijalankan dalam Reservasi Kapasitas.

> **Important**
>
> Pemilik Reservasi Kapasitas tetap menjadi pemilik sumber daya dan mereka tetap bertanggung jawab untuk mengelola Reservasi Kapasitas. Akun tempat penagihan diberikan tidak mendapatkan hak istimewa tambahan; akun tersebut tidak dapat membatalkan, memodifikasi, atau membagikan Reservasi Kapasitas dengan cara apa pun.

Topik

- Cara kerjanya
- Pertimbangan-pertimbangan
- Tetapkan tagihan Reservasi Kapasitas EC2 bersama ke akun lain
- Lihat permintaan penetapan tagihan untuk Reservasi Kapasitas EC2 bersama
- Menerima atau menolak penagihan Reservasi Kapasitas EC2 bersama
- Membatalkan atau mencabut permintaan penetapan tagihan untuk Reservasi Kapasitas EC2 bersama
- Memantau permintaan penetapan tagihan untuk Reservasi Kapasitas bersama

Cara kerjanya

Hanya pemilik Reservasi Kapasitas yang dapat menetapkan tagihan Reservasi Kapasitas bersama ke akun lain. Penagihan hanya dapat ditetapkan ke akun yang digunakan bersama Reservasi

Kapasitas dan yang dikonsolidasikan di bawah akun AWS Organizations pembayar yang sama dengan pemilik Reservasi Kapasitas.

Untuk menetapkan penagihan kapasitas yang tersedia dari Reservasi Kapasitas ke akun lain, pemilik Reservasi Kapasitas harus memulai permintaan ke akun yang diperlukan. Akun yang ditentukan menerima permintaan dan mereka harus menerima atau menolaknya dalam waktu 12 jam.

- Jika mereka menerima, mereka menjadi pemilik penagihan dari kapasitas apa pun yang tersedia, juga disebut kapasitas yang tidak terpakai, dalam Reservasi Kapasitas. Sejak saat itu dan seterusnya, biaya untuk kapasitas apa pun yang tersedia dalam Reservasi Kapasitas ditagih ke akun mereka, bukan akun pemilik. Setelah diterima, hanya pemilik Reservasi Kapasitas yang dapat mencabut tagihan dari akun yang ditetapkan.
- Jika menolak, pemilik Reservasi Kapasitas tetap menjadi pemilik tagihan atas kapasitas yang tersedia dalam Reservasi Kapasitas. Biaya untuk setiap kapasitas yang tersedia dalam Reservasi Kapasitas terus ditagih ke akun pemilik.
- Jika mereka tidak menerima atau menolak permintaan dalam waktu 12 jam, permintaan tersebut akan kedaluwarsa dan biaya untuk kapasitas yang tersedia dalam Reservasi Kapasitas terus ditagih ke akun pemilik.

Untuk periode penagihan ditetapkan ke akun lain, item `UnusedBox` baris `Reservation` dan muncul di Laporan Biaya dan Penggunaan (CUR) akun yang ditetapkan, bukan CUR pemilik.

Tabel berikut menunjukkan item baris mana yang muncul di CUR untuk pemilik Reservasi Kapasitas dan akun konsumen sebelum penagihan ditetapkan ke akun lain.

Akun	Item baris CUR sebelum penagihan ditetapkan
Pemilik Reservasi Kapasitas	• `Reservation` • `BoxUsage *` • `UnusedBox`
Akun konsumen dengan mana Reservasi Kapasitas dibagikan	•

Akun	Item baris CUR sebelum penagihan ditetapkan
	`BoxUsage` *

Tabel berikut menunjukkan item baris mana yang muncul di CUR untuk pemilik Reservasi Kapasitas dan akun konsumen setelah penagihan ditetapkan ke akun lain.

Akun	Item baris CUR setelah penagihan ditetapkan
Pemilik Reservasi Kapasitas	• `BoxUsage` *
Akun konsumen tempat penagihan ditetapkan	• `Reservation` • `BoxUsage` * • `UnusedBox`
Akun konsumen lain yang dengannya Reservasi Kapasitas dibagikan	• `BoxUsage` *

Note

- * Item `BoxUsage` baris muncul di CUR akun hanya jika mereka memiliki instance yang berjalan di Reservasi Kapasitas. Untuk informasi selengkapnya tentang item baris CUR, lihat Memantau Reservasi Kapasitas.
- Gunakan ARN Reservasi Kapasitas di CUR untuk menentukan siapa yang memiliki Reservasi Kapasitas. Jika ARN menyertakan ID AWS akun Anda, Anda adalah pemilik

Reservasi Kapasitas. Jika tidak, Reservasi Kapasitas dimiliki oleh akun yang berbeda tetapi penagihan diberikan kepada Anda.

- Tag alokasi biaya yang ditetapkan untuk Reservasi Kapasitas oleh pemilik tidak akan muncul di CUR akun konsumen. Tag alokasi biaya hanya muncul di CUR pemilik Reservasi Kapasitas.

Pertimbangan-pertimbangan

Ingatlah hal berikut saat menetapkan tagihan Reservasi Kapasitas bersama:

- Anda tidak dapat melakukan tugas penagihan sebagian atau terpisah. Penagihan semua kapasitas Reservasi Kapasitas yang tersedia dapat ditetapkan ke satu akun pada satu waktu.
- Kapasitas Reservasi Kapasitas yang tersedia dapat berubah seiring waktu. Ini akan memengaruhi penagihan untuk akun yang ditetapkan. Misalnya, kapasitas yang tersedia dapat meningkat jika pemilik Reservasi Kapasitas meningkatkan ukuran Reservasi Kapasitas, atau jika akun konsumen lain menghentikan atau menghentikan instans mereka yang berjalan di Reservasi Kapasitas.
- Penagihan hanya dapat ditetapkan ke akun konsumen yang dikonsolidasikan di bawah akun AWS Organizations pembayar yang sama. Penagihan secara otomatis dicabut dari akun konsumen jika mereka meninggalkan organisasi, atau jika Reservasi Kapasitas tidak lagi dibagikan dengan mereka.
- Hanya pemilik Reservasi Kapasitas yang dapat membatalkan permintaan penetapan tagihan yang tertunda dan mencabut tagihan dari akun yang ditetapkan setelah permintaan diterima.

Tetapkan tagihan Reservasi Kapasitas EC2 bersama ke akun lain

Untuk menetapkan tagihan kapasitas yang tersedia dari Reservasi Kapasitas bersama ke akun lain, pemilik Reservasi Kapasitas harus memulai permintaan ke akun yang diperlukan. Di konsol Amazon EC2, permintaan ini disebut permintaan transfer.

Pemilik Reservasi Kapasitas dapat menetapkan tagihan kapasitas Reservasi Kapasitas yang tersedia ke akun hanya jika:

- Reservasi Kapasitas sudah dibagikan dengan akun itu.
- Akun tersebut dikonsolidasikan di bawah akun AWS Organizations pembayar yang sama dengan pemilik Reservasi Kapasitas.

Penagihan ditetapkan ke akun yang ditentukan hanya setelah mereka menerima permintaan.

Saat pemilik Reservasi Kapasitas memulai permintaan, EventBridge acara Amazon akan dikirim ke akun yang diminta. Untuk informasi selengkapnya, lihat Memantau permintaan penetapan tagihan untuk Reservasi Kapasitas bersama.

Console

Untuk menetapkan tagihan Reservasi Kapasitas bersama

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas dan kemudian pilih Reservasi Kapasitas bersama.
3. Di bagian Penagihan kapasitas yang tersedia, pilih Tetapkan penagihan.
4. Di layar Tetapkan penagihan, pilih akun konsumen yang akan ditetapkan penagihan, lalu pilih Permintaan.

AWS CLI

Untuk menetapkan tagihan Reservasi Kapasitas bersama

Gunakan perintah associate-capacity-reservation-billing-owner. Untuk`--capacity-reservation-id`, tentukan ID Reservasi Kapasitas bersama. Untuk`--unused-reservation-billing-owner-id`, tentukan ID AWS akun yang akan ditetapkan penagihan.

```
aws ec2 associate-capacity-reservation-billing-owner \
    --capacity-reservation-id cr-01234567890abcdef \
    --unused-reservation-billing-owner-id 123456789012
```

PowerShell

Untuk menetapkan tagihan Reservasi Kapasitas bersama

Gunakan Register-EC2CapacityReservationBillingOwnercmdlet. Untuk`-CapacityReservationId`, tentukan ID Reservasi Kapasitas bersama. Untuk`-UnusedReservationBillingOwnerId`, tentukan ID AWS akun yang akan ditetapkan penagihan.

```
Register-EC2CapacityReservationBillingOwner `
    -CapacityReservationId cr-01234567890abcdef `
```

```
    -UnusedReservationBillingOwnerId 123456789012
```

Lihat permintaan penetapan tagihan untuk Reservasi Kapasitas EC2 bersama

Pemilik Reservasi Kapasitas hanya dapat melihat permintaan penetapan tagihan terbaru yang mereka mulai. Dan akun konsumen hanya dapat melihat permintaan penetapan tagihan terbaru yang dikirimkan kepada mereka.

Permintaan dapat dilihat selama 24 jam setelah mereka memasuki`cancelled`,`expired`, atau `revoked` negara bagian. Setelah 24 jam, mereka tidak dapat lagi dilihat.

Console

(Pemilik Reservasi Kapasitas) Untuk melihat permintaan yang Anda mulai

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas dan kemudian pilih Reservasi Kapasitas bersama untuk melihat permintaan.
3. Bagian Penagihan kapasitas yang tersedia menunjukkan permintaan terbaru dan statusnya saat ini.

(Akun konsumen) Untuk permintaan yang dikirimkan kepada Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.
3. Jika Anda memiliki permintaan yang tertunda, spanduk Permintaan penagihan penagihan tertunda muncul di bagian atas layar. Jika spanduk tidak muncul, Anda tidak memiliki permintaan yang tertunda.

   Untuk melihat permintaan, pilih Tinjau permintaan di spanduk.

AWS CLI

(Pemilik Reservasi Kapasitas) Untuk melihat permintaan yang Anda mulai

Gunakan perintah describe-capacity-reservation-billing-requests.

```
aws ec2 describe-capacity-reservation-billing-requests \
```

```
    --role odcr-owner
```

(Akun konsumen) Untuk melihat permintaan yang dikirimkan kepada Anda

Gunakan perintah describe-capacity-reservation-billing-requests.

```
aws ec2 describe-capacity-reservation-billing-requests \
    --role unused-reservation-billing-owner
```

PowerShell

(Pemilik Reservasi Kapasitas) Untuk melihat permintaan yang Anda mulai

Gunakan Get-EC2CapacityReservationBillingRequestcmdlet.

```
Get-EC2CapacityReservationBillingRequest `
    -Role odcr-owner
```

(Akun konsumen) Untuk melihat permintaan yang dikirimkan kepada Anda

Gunakan Get-EC2CapacityReservationBillingRequestcmdlet.

```
Get-EC2CapacityReservationBillingRequest `
    -Role unused-reservation-billing-owner
```

Permintaan dapat berada di salah satu negara bagian berikut.

Status	Deskripsi			
`pending`	Permintaan belum diterima atau ditolak, tetapi belum kedaluwarsa.			
`accepted`	Permintaan diterima oleh akun yang ditentukan. Penagihan kapasitas yang tersedia dari Reservasi Kapasitas ditetapkan ke akun konsumen.			

Status	Deskripsi
`rejected`	Permintaan tersebut ditolak oleh akun konsumen.
`cancelled`	Permintaan dibatalkan oleh pemilik Reservasi Kapasitas saat berada di `pending` negara bagian.
`revoked`	Tagihan dicabut dari akun konsumen karena salah satu alasan berikut: • Itu secara eksplisit dicabut oleh pemilik Reservasi Kapasitas. • Reservasi Kapasitas tidak lagi dibagikan dengan akun konsumen. • Akun konsumen tidak lagi menjadi bagian dari AWS organisasi.
`expired`	Permintaan kedaluwarsa karena akun konsumen tidak menerima atau menolaknya dalam waktu 12 jam.

Menerima atau menolak penagihan Reservasi Kapasitas EC2 bersama

Jika Anda menerima permintaan penetapan tagihan untuk Reservasi Kapasitas yang dibagikan dengan Anda, Anda dapat menerima atau menolaknya. Permintaan tetap di `pending` negara bagian sampai diterima atau ditolak.

Jika Anda menerima permintaan, permintaan masuk ke `accepted` negara bagian, dan penagihan kapasitas yang tersedia, atau tidak terpakai, dari Reservasi Kapasitas tersebut ditetapkan ke akun Anda sejak saat itu dan seterusnya. Setelah Anda menerima permintaan, hanya pemilik Reservasi Kapasitas yang dapat mencabut tagihan dari akun Anda.

Jika Anda menolak permintaan, permintaan masuk ke `rejected` negara bagian, dan penagihan kapasitas yang tersedia dari Reservasi Kapasitas tetap ditetapkan kepada pemilik Reservasi Kapasitas.

Permintaan kedaluwarsa jika tidak diterima atau ditolak dalam waktu 12 jam. Jika permintaan kedaluwarsa, penagihan kapasitas Reservasi Kapasitas yang tidak terpakai tetap diberikan kepada pemilik Reservasi Kapasitas.

Ketika permintaan diterima atau ditolak, EventBridge acara Amazon akan dikirim ke akun pemilik Reservasi Kapasitas. Ketika permintaan kedaluwarsa, EventBridge acara Amazon dikirim ke pemilik Reservasi Kapasitas dan akun konsumen. Untuk informasi selengkapnya, lihat Memantau permintaan penetapan tagihan untuk Reservasi Kapasitas bersama.

Console

Untuk menerima atau menolak permintaan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.
3. Jika Anda memiliki permintaan yang tertunda, spanduk Permintaan penagihan penagihan tertunda muncul di bagian atas layar. Jika spanduk tidak muncul, Anda tidak memiliki permintaan yang tertunda.

   Untuk melihat permintaan, pilih Tinjau permintaan di spanduk.
4. Pilih permintaan untuk menerima atau menolak, lalu pilih Terima atau Tolak.

AWS CLI

Untuk menerima permintaan

Gunakan perintah accept-capacity-reservation-billing-ownership. Untuk`--capacity-reservation-id`, tentukan ID Reservasi Kapasitas untuk menerima permintaan.

```
aws ec2 accept-capacity-reservation-billing-ownership \
```

```
    --capacity-reservation-id cr-01234567890abcdef
```

Untuk menolak permintaan

Gunakan perintah reject-capacity-reservation-billing-ownership. Untuk`--capacity-reservation-id`, tentukan ID Reservasi Kapasitas untuk menolak permintaan.

```
aws ec2 reject-capacity-reservation-billing-ownership \
    --capacity-reservation-id cr-01234567890abcdef
```

PowerShell

Untuk menerima permintaan

Gunakan Approve-EC2CapacityReservationBillingOwnershipcmdlet.

```
Approve-EC2CapacityReservationBillingOwnership `
    -CapacityReservationId cr-01234567890abcdef
```

Untuk menolak permintaan

Gunakan Deny-EC2CapacityReservationBillingOwnershipcmdlet.

```
Deny-EC2CapacityReservationBillingOwnership `
    -CapacityReservationId cr-01234567890abcdef
```

Membatalkan atau mencabut permintaan penetapan tagihan untuk Reservasi Kapasitas EC2 bersama

Hanya pemilik Reservasi Kapasitas yang dapat membatalkan permintaan penetapan `pending` tagihan. Jika permintaan yang tertunda dibatalkan, permintaan tersebut memasuki `cancelled` status dan penagihan kapasitas yang tersedia, atau tidak terpakai, dari Reservasi Kapasitas tetap ditetapkan untuk pemilik Reservasi Kapasitas.

Setelah permintaan`accepted`, hanya pemilik Reservasi Kapasitas yang dapat mencabut tagihan dari akun yang ditetapkan. Jika tagihan dicabut, permintaan masuk ke `revoked` negara bagian dan penagihan kapasitas yang tersedia dari Reservasi Kapasitas dipindahkan ke pemilik Reservasi Kapasitas.

Saat permintaan dibatalkan atau dicabut, EventBridge acara Amazon akan dikirim ke pemilik Reservasi Kapasitas dan akun konsumen yang ditentukan. Untuk informasi selengkapnya, lihat Memantau permintaan penetapan tagihan untuk Reservasi Kapasitas bersama.

Console

Untuk membatalkan atau mencabut permintaan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas dan kemudian pilih Reservasi Kapasitas untuk membatalkan atau mencabut permintaan.
3. Di bagian Penagihan kapasitas yang tersedia, pilih Batalkan transfer atau Cabut transfer, tergantung pada status permintaan saat ini.

AWS CLI

Untuk membatalkan atau mencabut permintaan

Gunakan perintah disassociate-capacity-reservation-billing-owner. Untuk `--unused-reservation-billing-owner-id`, tentukan ID AWS akun tempat permintaan dikirim.

```
aws ec2 disassociate-capacity-reservation-billing-owner \
    --capacity-reservation-id cr-01234567890abcdef \
    --unused-reservation-billing-owner-id 123456789012
```

PowerShell

Untuk membatalkan atau mencabut permintaan

Gunakan Unregister-EC2CapacityReservationBillingOwnercmdlet. Untuk `-UnusedReservationBillingOwnerId`, tentukan ID AWS akun tempat permintaan dikirim.

```
Unregister-EC2CapacityReservationBillingOwner `
    -CapacityReservationId cr-01234567890abcdef `
    -UnusedReservationBillingOwnerId 123456789012
```

Memantau permintaan penetapan tagihan untuk Reservasi Kapasitas bersama

Amazon EC2 mengirimkan EventBridge peristiwa Amazon saat status permintaan penetapan tagihan berubah.

- Acara dikirim ke pemilik Reservasi Kapasitas ketika permintaan memasuki status berikut: `accepted` | `rejected` | `expired` |`revoked`.
- Acara dikirim ke akun konsumen yang diminta ketika permintaan memasuki status berikut: `pending` | `expired` | `cancelled` |`revoked`.

Untuk informasi selengkapnya tentang Amazon EventBridge, lihat Panduan EventBridge Pengguna Amazon.

Berikut ini adalah pola EventBridge acara Amazon.

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"On-Demand Capacity Reservation Billing Ownership Request pending|
accepted|rejected|cancelled|revoked|expired",
   "source":"aws.ec2",
   "account":"account_id",
   "time":"state_change_timestamp",
   "region":"region",
   "resources":[
      "arn:aws:ec2:region:cr_owner_account_id:capacity-reservation/cr_id"
   ],
   "detail":{
      "capacity-reservation-id":"cr_id",
      "updateTime":timestamp,
      "ownerAccountId":"cr_owner_account_id",
      "unusedReservationChargesOwnerID":"consumer_account_id",
      "status":"pending|accepted|rejected|cancelled|revoked|expired",
      "statusMessage":"message
   }
}
```

Berikut ini adalah contoh peristiwa yang dikirim ke pemilik Reservasi Kapasitas (222222222222) ketika akun konsumen (111111111111) menerima permintaan penetapan tagihan untuk Reservasi Kapasitas bersama (). `cr-01234567890abcdef`

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"On-Demand Capacity Reservation Billing Ownership Request accepted",
   "source":"aws.ec2",
```

```
   "account":"222222222222",
   "time":"2024-09-01Thh:59:59Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:222222222222:capacity-reservation/cr-01234567890abcdef"
   ],
   "detail":{
      "capacity-reservation-id":"cr-01234567890abcdef",
      "updateTime":"2024-08-01Thh:59:59Z",
      "ownerAccountId":"222222222222",
      "unusedReservationChargesOwnerID":"111111111111",
      "status":"accepted",
      "statusMessage":"billing transfer status message"
   }
}
```

Izin Reservasi Kapasitas Bersama

Izin untuk pemilik

Pemilik bertanggung jawab untuk mengelola dan membatalkan Reservasi Kapasitas bersama mereka. Pemilik tidak dapat memodifikasi instans yang berjalan di Reservasi Kapasitas bersama yang dimiliki oleh akun lain. Pemilik tetap bertanggung jawab untuk mengelola instans yang mereka luncurkan ke dalam Reservasi Kapasitas bersama.

Izin untuk konsumen

Konsumen bertanggung jawab untuk mengelola instans mereka yang menjalankan Reservasi Kapasitas bersama. Konsumen tidak dapat memodifikasi Reservasi Kapasitas bersama dengan cara apa pun, dan mereka tidak dapat menampilkan atau memodifikasi instans yang dimiliki oleh konsumen lain atau pemilik Reservasi Kapasitas. Konsumen hanya dapat melihat total kapasitas dan kapasitas yang tersedia dalam reservasi bersama.

Tagihan dan pengukuran

Tidak ada biaya tambahan untuk berbagi Reservasi Kapasitas.

Secara default, pemilik Reservasi Kapasitas ditagih untuk instans yang dijalankan di dalam Reservasi Kapasitas dan untuk kapasitas cadangan yang tidak digunakan, sementara konsumen ditagih untuk kejadian yang mereka jalankan di dalam Reservasi Kapasitas bersama. Namun, Anda dapat menetapkan penagihan kapasitas yang tersedia dari Reservasi Kapasitas bersama ke akun

konsumen tertentu. Untuk informasi selengkapnya, lihat Penugasan penagihan untuk Reservasi Kapasitas Amazon EC2 bersama.

Jika pemilik Reservasi Kapasitas termasuk dalam rekening pembayar yang berbeda dan Reservasi Kapasitas tercakup oleh Instans Terpesan Regional atau Savings Plans, pemilik Reservasi Kapasitas akan terus ditagih untuk Instans Terpesan Regional atau Savings Plans. Dalam kasus ini, pemilik Reservasi Kapasitas membayar Instans Terpesan Regional atau Savings Plans, dan konsumen ditagih untuk instans yang dijalankan dalam Reservasi Kapasitas bersama.

Batas instans

Semua penggunaan Reservasi Kapasitas diperhitungkan dalam batas Instans Sesuai Permintaan pemilik Reservasi Kapasitas. Hal ini mencakup:

- Kapasitas terpesan yang tidak terpakai
- Penggunaan oleh instans yang dimiliki oleh pemilik Reservasi Kapasitas
- Penggunaan oleh instans yang dimiliki oleh konsumen

Instans yang diluncurkan ke dalam kapasitas bersama oleh konsumen diperhitungkan dalam batas Instans Sesuai Permintaan pemilik Reservasi Kapasitas. Batas instans Konsumen adalah jumlah dari batas Instans Sesuai Permintaan mereka sendiri dan kapasitas yang tersedia di Reservasi Kapasitas bersama yang aksesnya mereka miliki.

Armada Reservasi Kapasitas

Armada Reservasi Kapasitas Sesuai Permintaan adalah sekelompok Reservasi Kapasitas.

Permintaan Armada Reservasi Kapasitas berisi semua informasi konfigurasi yang diperlukan untuk meluncurkan Armada Reservasi Kapasitas. Menggunakan satu permintaan, Anda dapat memesan sejumlah besar kapasitas Amazon EC2 untuk beban kerja di banyak tipe instans, hingga kapasitas target yang Anda tentukan.

Setelah membuat Armada Reservasi Kapasitas, Anda dapat mengelola Reservasi Kapasitas dalam armada secara kolektif dengan memodifikasi atau membatalkan Armada Reservasi Kapasitas.

Topik

- Cara kerja Armada Reservasi Kapasitas
- Pertimbangan-pertimbangan

- Penetapan harga
- Konsep dan perencanaan Armada Reservasi Kapasitas
- Untuk mengubah Armada Reservasi Kapasitas
- Memodifikasi Armada Reservasi Kapasitas
- Membatalkan Armada Reservasi Kapasitas
- Contoh konfigurasi Armada Reservasi Kapasitas
- Menggunakan peran tertaut layanan untuk Armada Reservasi Kapasitas

Cara kerja Armada Reservasi Kapasitas

Saat Anda membuat Armada Reservasi Kapasitas, Armada mencoba membuat Reservasi Kapasitas individual untuk memenuhi total kapasitas target yang Anda tentukan dalam permintaan Armada.

Jumlah instans yang diandalkan kapasitas terpesan Armada bergantung pada total kapasitas target dan bobot tipe instans yang Anda tentukan. Tipe instans untuk reservasi kapasitas tergantung pada strategi alokasi dan prioritas tipe instans yang Anda gunakan.

Jika ada kapasitas yang tidak mencukupi pada saat Armada dibuat, dan tidak dapat segera memenuhi kapasitas target totalnya, Armada secara asinkron mencoba untuk membuat Reservasi Kapasitas sampai berhasil memesan sejumlah kapasitas yang diminta.

Ketika Armada mencapai kapasitas target totalnya, Armada berusaha mempertahankan kapasitas itu. Jika Reservasi Kapasitas di Armada dibatalkan, Armada secara otomatis membuat satu atau lebih Reservasi Kapasitas, tergantung pada konfigurasi Armada Anda, untuk mengganti kapasitas yang hilang dan mempertahankan total kapasitas targetnya.

Reservasi Kapasitas di Armada tidak dapat dikelola secara individual. Reservasi tersebut harus dikelola secara kolektif dengan memodifikasi Armada. Saat Anda memodifikasi Armada, Reservasi Kapasitas di Armada diperbarui secara otomatis untuk mencerminkan perubahan tersebut.

Saat ini, Armada Reservasi Kapasitas mendukung kriteria pencocokan instans `open`, dan semua Reservasi Kapasitas yang diluncurkan oleh Armada secara otomatis menggunakan kriteria pencocokan instans ini. Dengan kriteria ini, instance baru dan instans yang sudah ada yang memiliki atribut yang cocok (tipe instans, platform, Availability Zone, dan tenancy) secara otomatis berjalan di Reservasi Kapasitas yang dibuat oleh Armada. Armada Reservasi Kapasitas tidak mendukung kriteria pencocokan instans yang ditargetkan.

Pertimbangan-pertimbangan

Ingatlah hal-hal berikut ini saat bekerja dengan Armada Reservasi Kapasitas:

- Armada Reservasi Kapasitas dapat dibuat, dimodifikasi, dilihat, dan dibatalkan menggunakan AWS API AWS CLI dan.
- Reservasi Kapasitas dalam suatu Armada tidak dapat dikelola secara individual. Reservasi tersebut harus dikelola secara kolektif dengan memodifikasi atau membatalkan Armada.
- Armada Reservasi Kapasitas tidak dapat menjangkau seluruh Wilayah.
- Armada Reservasi Kapasitas tidak dapat menjangkau seluruh Zona Ketersediaan.
- Reservasi Kapasitas yang dibuat oleh Armada Reservasi Kapasitas secara otomatis ditandai dengan tanda yang dihasilkan AWS berikut:
  - Kunci — `aws:ec2-capacity-reservation-fleet`
  - Nilai — *`fleet_id`*

  Anda dapat menggunakan tanda ini untuk mengidentifikasi Reservasi Kapasitas yang dibuat oleh Armada Reservasi Kapasitas.

Penetapan harga

Tidak ada biaya tambahan untuk menggunakan Armada Reservasi Kapasitas. Anda ditagih untuk Reservasi Kapasitas individual yang dibuat oleh Armada Reservasi Kapasitas Anda. Untuk informasi selengkapnya tentang cara penagihan Reservasi Kapasitas, lihat Harga dan penagihan Reservasi Kapasitas.

Konsep dan perencanaan Armada Reservasi Kapasitas

Informasi berikut menjelaskan cara merencanakan Armada Reservasi Kapasitas dan menjelaskan konsep Armada Reservasi Kapasitas termasuk kapasitas target total, strategi alokasi, bobot jenis instans, dan prioritas tipe instans.

Topik

- Rencanakan Armada Reservasi Kapasitas
- Kapasitas target total
- Strategi alokasi
- Bobot tipe instans
- Prioritas tipe instans

Rencanakan Armada Reservasi Kapasitas

Saat merencanakan Armada Reservasi Kapasitas Anda, kami sarankan Anda melakukan hal berikut:

1. Tentukan jumlah kapasitas komputasi yang dibutuhkan oleh beban kerja Anda.
2. Tentukan tipe instans dan Zona Ketersediaan yang ingin Anda gunakan.
3. Tetapkan prioritas untuk setiap tipe instans berdasarkan kebutuhan dan preferensi Anda. Untuk informasi selengkapnya, lihat Prioritas tipe instans.
4. Buat sistem pembobotan kapasitas yang masuk akal untuk beban kerja Anda. Tetapkan bobot untuk setiap tipe instans dan tentukan total kapasitas target Anda. Untuk informasi selengkapnya, lihat Bobot tipe instans dan Kapasitas target total.
5. Tentukan apakah Anda memerlukan Reservasi Kapasitas tanpa batas waktu atau hanya untuk jangka waktu tertentu.

Kapasitas target total

Total kapasitas target menentukan jumlah total kapasitas komputasi yang dipesan oleh Armada Reservasi Kapasitas. Anda menentukan total kapasitas target saat Anda membuat Armada Reservasi Kapasitas. Setelah Armada dibuat, Amazon EC2 secara otomatis membuat Reservasi Kapasitas untuk memesan kapasitas hingga total kapasitas target.

Jumlah instans kapasitas yang dipesan Armada Reservasi Kapasitas ditentukan oleh total kapasitas target dan bobot tipe instans yang Anda tentukan untuk setiap tipe instans di Armada Reservasi Kapasitas (`total target capacity/instance type weight=number of instances`).

Anda dapat menetapkan total kapasitas target berdasarkan unit yang berarti bagi beban kerja Anda. Misalnya, jika beban kerja Anda memerlukan sejumlah vCPUs, Anda dapat menetapkan total kapasitas target berdasarkan jumlah v CPUs yang diperlukan. Jika beban kerja Anda memerlukan `2048` vCPUs, tentukan total kapasitas target, lalu tetapkan bobot tipe instans berdasarkan jumlah v yang CPUs disediakan oleh tipe instans di Armada. `2048` Sebagai contoh, lihat Bobot tipe instans.

Strategi alokasi

Strategi alokasi untuk Armada Reservasi Kapasitas Anda menentukan caranya memenuhi permintaan Anda untuk kapasitas terpesan dari spesifikasi tipe instans dalam konfigurasi Armada Capacity Reservation.

Saat ini, hanya strategi alokasi `prioritized` yang didukung. Dengan strategi ini, Armada Reservasi Kapasitas membuat Reservasi Kapasitas menggunakan prioritas yang telah Anda tetapkan untuk

setiap spesifikasi tipe instans dalam konfigurasi Armada Reservasi Kapasitas. Nilai prioritas yang lebih rendah menunjukkan prioritas penggunaan yang lebih tinggi. Misalnya, Anda membuat Armada Reservasi Kapasitas yang menggunakan tipe instans dan prioritas berikut:

- `m4.16xlarge` — prioritas = 1
- `m5.16xlarge` — prioritas = 3
- `m5.24xlarge` — prioritas = 2

Armada pertama kali mencoba untuk membuat Reservasi Kapasitas untuk `m4.16xlarge`. Jika Amazon EC2 memiliki kapasitas `m4.16xlarge` yang tidak mencukupi, Armada berupaya membuat Reservasi Kapasitas untuk `m5.24xlarge`. Jika Amazon EC2 memiliki kapasitas `m5.24xlarge` yang tidak mencukupi, Armada membuat Reservasi Kapasitas untuk `m5.16xlarge`.

Bobot tipe instans

Bobot tipe instans adalah bobot yang Anda tetapkan untuk setiap tipe instans di Armada Reservasi Kapasitas. Bobot menentukan berapa banyak unit kapasitas setiap instans dari tipe instans tertentu yang diperhitungkan dalam total kapasitas target Armada.

Anda dapat menetapkan bobot berdasarkan unit yang berarti bagi beban kerja Anda. Misalnya, jika beban kerja Anda memerlukan sejumlah vCPUs, Anda dapat menetapkan bobot berdasarkan jumlah v yang CPUs disediakan oleh setiap jenis instans di Armada Reservasi Kapasitas. Dalam hal ini, jika Anda membuat Armada Reservasi Kapasitas menggunakan `m4.16xlarge` dan `m5.24xlarge` instance, Anda akan menetapkan bobot yang sesuai dengan jumlah v CPUs untuk setiap instance sebagai berikut:

- `m4.16xlarge`- 64 vCPUs, berat = 64 satuan
- `m5.24xlarge`- 96 vCPUs, berat = 96 satuan

Bobot tipe instans menentukan jumlah instans yang kapasitasnya dipesan Armada Reservasi Kapasitas. Misalnya, jika Armada Reservasi Kapasitas dengan kapasitas target total 384 unit menggunakan tipe dan bobot instans dalam contoh sebelumnya, Armada dapat memesan kapasitas untuk instans 6 `m4.16xlarge` (384 kapasitas target total/64 bobot tipe instans=6 instans), atau 4 `m5.24xlarge` instans (384 / 96 = 4).

Jika Anda tidak menetapkan bobot tipe instans, atau jika Anda menetapkan bobot tipe instans 1, total kapasitas target hanya didasarkan pada jumlah instans. Misalnya, jika Armada Reservasi Kapasitas

dengan kapasitas target total `384` unit menggunakan tipe instans dalam contoh sebelumnya, tetapi menghilangkan bobot atau menentukan bobot `1` untuk kedua tipe instans, Armada dapat memesan kapasitas untuk `384` `m4.16xlarge` instans atau `384` `m5.24xlarge` instans.

Prioritas tipe instans

Prioritas tipe instans adalah nilai yang Anda tetapkan ke tipe instans di Armada. Prioritas digunakan untuk menentukan tipe instans mana yang ditentukan untuk Armada yang harus diprioritaskan untuk digunakan.

Nilai prioritas yang lebih rendah menunjukkan prioritas penggunaan yang lebih tinggi.

Untuk mengubah Armada Reservasi Kapasitas

Saat Anda membuat Armada Reservasi Kapasitas, Armada akan secara otomatis membuat Reservasi Kapasitas untuk tipe instans yang ditentukan dalam permintaan Armada, hingga total kapasitas target yang ditentukan. Jumlah instans kapasitas yang dipesan Armada Reservasi Kapasitas tergantung pada total kapasitas target dan bobot tipe instans yang Anda tentukan dalam permintaan. Untuk informasi selengkapnya, lihat Bobot tipe instans dan Kapasitas target total.

Saat membuat Armada, Anda harus menentukan tipe instans yang akan digunakan dan prioritas untuk masing-masing tipe instans tersebut. Untuk informasi selengkapnya, lihat Strategi alokasi dan Prioritas tipe instans.

> **Note**
>
> Peran AWSServiceRoleForEC2CapacityReservationFleetterkait layanan dibuat secara otomatis di akun Anda saat pertama kali membuat Armada Reservasi Kapasitas. Untuk informasi selengkapnya, lihat Menggunakan peran tertaut layanan untuk Armada Reservasi Kapasitas.

Saat ini, Armada Reservasi Kapasitas hanya mendukung kriteria pencocokan instans `open`.

AWS CLI

Untuk mengubah Armada Reservasi Kapasitas

Gunakan perintah create-capacity-reservation-fleet.

```
aws ec2 create-capacity-reservation-fleet \
    --total-target-capacity 24 \
    --allocation-strategy prioritized \
    --instance-match-criteria open \
    --tenancy default \
    --end-date 2021-12-31T23:59:59.000Z \
    --instance-type-specifications file://instanceTypeSpecification.json
```

Berikut ini adalah isi dari`instanceTypeSpecification.json`.

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

Berikut ini adalah output contoh.

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

PowerShell

Untuk mengubah Armada Reservasi Kapasitas

Gunakan New-EC2CapacityReservationFleetcmdlet.

```
New-EC2CapacityReservationFleet `
    -TotalTargetCapacity 24 `
    -AllocationStrategy "prioritized" `
    -InstanceMatchCriterion "open" `
    -Tenancy "default" `
```

```
    -EndDate 2021-12-31T23:59:59.000Z `
    -InstanceTypeSpecification $specification
```

Spesifikasi didefinisikan sebagai berikut.

```
$specification = New-Object Amazon.EC2.Model.ReservationFleetInstanceSpecification
$specification.InstanceType = "m5.xlarge"
$specification.InstancePlatform = "Linux/UNIX"
$specification.Weight = 3.0
$specification.AvailabilityZone = "us-east-1a"
$specification.EbsOptimized = $true
$specification.Priority = 1
```

Memodifikasi Armada Reservasi Kapasitas

Anda dapat memodifikasi total kapasitas target dan tanggal Armada Reservasi Kapasitas kapan saja. Saat Anda memodifikasi total kapasitas target Armada Reservasi Kapasitas, Armada secara otomatis membuat Reservasi Kapasitas baru, atau memodifikasi atau membatalkan Reservasi Kapasitas yang ada di Armada untuk memenuhi total kapasitas target yang baru. Ketika Anda memodifikasi tanggal akhir Armada, tanggal akhir untuk semua Reservasi Kapasitas individu akan diperbarui sesuai dengan modifikasi itu.

Pertimbangan-pertimbangan

- Setelah Anda memodifikasi Armada, statusnya beralih ke `modifying`. Anda tidak dapat mencoba modifikasi tambahan pada Armada saat berada dalam status `modifying`.
- Anda tidak dapat mengubah penghunian, Zona Ketersediaan, tipe instans, platform instans, prioritas, atau bobot yang digunakan oleh Armada Reservasi Kapasitas. Jika Anda perlu mengubah salah satu parameter ini, Anda mungkin perlu membatalkan Armada yang ada dan membuat armada baru dengan parameter yang diperlukan.
- Anda tidak dapat menentukan `--end-date` dan `--remove-end-date` dalam perintah yang sama.

AWS CLI

Untuk mengubah Armada Reservasi Kapasitas

Gunakan perintah modify-capacity-reservation-fleet.

Contoh 1: Ubah total kapasitas target

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --total-target-capacity 160
```

Contoh 2: Ubah tanggal akhir

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --end-date 2021-07-04T23:59:59.000Z
```

Contoh 3: Hapus tanggal akhir

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --remove-end-date
```

PowerShell

Untuk mengubah Armada Reservasi Kapasitas

Gunakan Edit-EC2CapacityReservationFleetcmdlet.

Contoh 1: Ubah total kapasitas target

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -TotalTargetCapacity 160
```

Contoh 2: Ubah tanggal akhir

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -EndDate 2021-07-04T23:59:59.000Z
```

Contoh 3: Hapus tanggal akhir

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
```

```
    -RemoveEndDate
```

Membatalkan Armada Reservasi Kapasitas

Bila Anda tidak lagi membutuhkan Armada Reservasi Kapasitas dan kapasitas dipesan, Anda dapat membatalkannya. Saat Anda membatalkan Armada, statusnya berubah menjadi `cancelled` dan Armada tidak dapat lagi membuat Reservasi Kapasitas baru. Selain itu, semua Reservasi Kapasitas individu di Armada dibatalkan. Instans yang sebelumnya berjalan dalam kapasitas cadangan terus berjalan normal dalam kapasitas bersama.

AWS CLI

Untuk membatalkan Armada Reservasi Kapasitas

Gunakan perintah cancel-capacity-reservation-fleets.

```
aws ec2 cancel-capacity-reservation-fleets \
    --capacity-reservation-fleet-ids crf-abcdef01234567890
```

Berikut ini adalah output contoh.

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

PowerShell

Untuk membatalkan Armada Reservasi Kapasitas

Gunakan Stop-EC2CapacityReservationFleetcmdlet.

```
Stop-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-abcdef01234567890
```

Contoh konfigurasi Armada Reservasi Kapasitas

Contoh berikut membuat Armada Reservasi Kapasitas yang menggunakan dua tipe instans: `m5.4xlarge` dan `m5.12xlarge`.

Ini menggunakan sistem pembobotan berdasarkan jumlah v yang CPUs disediakan oleh jenis instance yang ditentukan. Kapasitas target total adalah `480` vCPUs. `m5.4xlarge`Menyediakan 16 v CPUs dan mendapat bobot16, sedangkan `m5.12xlarge` menyediakan 48 v CPUs dan mendapat bobot48. Sistem pembobotan ini mengonfigurasi Armada Reservasi Kapasitas pada reservasi kapasitas untuk 30 instans `m5.4xlarge` (480/16=30), atau 10 instans `m5.12xlarge` (480/48=10).

Armada dikonfigurasi untuk memprioritaskan kapasitas `m5.12xlarge` dan mendapatkan prioritas 1, sementara `m5.4xlarge` mendapatkan prioritas 2 yang lebih rendah. Ini berarti bahwa armada akan mencoba untuk memesan kapasitas `m5.12xlarge` terlebih dahulu, dan hanya mencoba untuk memesan kapasitas `m5.4xlarge` jika kapasitas `m5.12xlarge` Amazon EC2 tidak mencukupi.

Armada memesan kapasitas untuk instans `Windows` dan reservasi secara otomatis berakhir pada `October 31, 2021` pukul `23:59:59` UTC.

```
aws ec2 create-capacity-reservation-fleet \
    --total-target-capacity 480 \
    --allocation-strategy prioritized \
    --instance-match-criteria open \
    --tenancy default \
    --end-date 2021-10-31T23:59:59.000Z \
    --instance-type-specifications file://instanceTypeSpecification.json
```

Berikut ini adalah isi dari `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
```

```
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
    }
]
```

Menggunakan peran tertaut layanan untuk Armada Reservasi Kapasitas

Armada Reservasi Kapasitas Sesuai Permintaan menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran tertaut layanan adalah tipe peran IAM unik yang tertaut langsung ke Armada Reservasi Kapasitas. Peran terkait layanan telah ditentukan sebelumnya oleh Armada Reservasi Kapasitas dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran tertaut layanan mempermudah pengaturan Armada Reservasi Kapasitas karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Armada Reservasi Kapasitas menentukan izin peran tertaut layanan, kecuali ditentukan lain, hanya Armada Reservasi Kapasitas yang dapat mengasumsikan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Hal ini melindungi sumber daya Armada Reservasi Kapasitas karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Izin peran tertaut layanan untuk Armada Reservasi Kapasitas

Armada Reservasi Kapasitas menggunakan peran terkait layanan yang diberi nama AWSServiceRoleForEC2CapacityReservationFleetuntuk membuat, mendeskripsikan, memodifikasi, dan membatalkan Reservasi Kapasitas dalam Armada Reservasi Kapasitas atas nama Anda.

Peran AWSService RoleFor EC2 CapacityReservationFleet terkait layanan mempercayai entitas berikut untuk mengambil peran:

- `capacity-reservation-fleet.amazonaws.com`

Peran tersebut menggunakan kebijakan `AWSEC2CapacityReservationFleetRolePolicy` AWS terkelola. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AWSEC2CapacityReservationFleetRolePolicy.

Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Menggunakan peran tertaut layanan untuk Armada Reservasi Kapasitas

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda membuat Armada Reservasi Kapasitas menggunakan `create-capacity-reservation-fleet` AWS CLI perintah atau `CreateCapacityReservationFleet` API, peran terkait layanan akan dibuat secara otomatis untuk Anda.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat Armada Reservasi Kapasitas, Armada Reservasi Kapasitas akan membuat peran terkait layanan untuk Anda lagi.

Mengedit peran tertaut layanan untuk Armada Reservasi Kapasitas

Armada Reservasi Kapasitas tidak mengizinkan Anda mengedit AWSService RoleFor EC2 CapacityReservationFleet peran terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit deskripsi peran terkait layanan di Panduan Pengguna IAM.

Menghapus peran tertaut layanan untuk Armada Reservasi Kapasitas

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Namun, Anda harus menghapus sumber daya untuk peran tertaut layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Armada Reservasi Kapasitas menggunakan peran tersebut saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran AWSService RoleFor EC2 CapacityReservationFleet terkait layanan

1. Gunakan `delete-capacity-reservation-fleet` AWS CLI perintah atau `DeleteCapacityReservationFleet` API untuk menghapus Armada Reservasi Kapasitas di akun Anda.
2. Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSService RoleFor EC2 CapacityReservationFleet terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran terkait layanan Armada Reservasi Kapasitas

Armada Reservasi Kapasitas mendukung penggunaan peran tertaut layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat Wilayah AWS dan Titik Akhir.

Memantau penggunaan Reservasi Kapasitas dengan metrik CloudWatch

Dengan CloudWatch metrik, Anda dapat memantau Reservasi Kapasitas secara efisien dan mengidentifikasi kapasitas yang tidak digunakan dengan menyetel CloudWatch alarm untuk memberi tahu Anda saat ambang batas penggunaan terpenuhi. Hal ini dapat membantu Anda mempertahankan volume Reservasi Kapasitas yang konstan dan mencapai tingkat pemanfaatan yang lebih tinggi.

Reservasi Kapasitas mengirim data metrik ke CloudWatch setiap lima menit. Metrik tidak didukung untuk Reservasi Kapasitas yang aktif kurang dari lima menit.

Untuk informasi selengkapnya tentang melihat metrik di CloudWatch konsol, lihat Menggunakan CloudWatch Metrik Amazon. Untuk informasi selengkapnya tentang membuat alarm, lihat Membuat CloudWatch Alarm Amazon.

Daftar Isi

- Metrik penggunaan Reservasi Kapasitas
- Dimensi metrik Reservasi Kapasitas
- Lihat CloudWatch metrik untuk Reservasi Kapasitas

Metrik penggunaan Reservasi Kapasitas

Namespace `AWS/EC2CapacityReservations` mencakup metrik penggunaan berikut yang dapat Anda gunakan untuk memantau dan mempertahankan kapasitas sesuai permintaan dalam ambang batas yang Anda tentukan untuk reservasi Anda.

Metrik	Deskripsi
`UsedInstanceCount`	Jumlah instans yang sedang digunakan. Unit: Jumlah
`AvailableInstanceCount`	Jumlah instans yang tersedia. Unit: Jumlah
`TotalInstanceCount`	Jumlah total instans yang telah Anda pesan. Unit: Jumlah
`InstanceUtilization`	Persentase instans kapasitas terpesan yang saat ini sedang digunakan. Satuan: Persen

Dimensi metrik Reservasi Kapasitas

Anda dapat menggunakan dimensi berikut untuk menyempurnakan metrik yang tercantum dalam tabel sebelumnya dalam Wilayah dan akun yang dipilih.

Dimensi	Deskripsi
(Tidak ada dimensi)	Dimensi ini menyaring metrik yang ditentukan untuk semua Reservasi Kapasitas.

Dimensi	Deskripsi
`CapacityReservationId`	Dimensi ini menyaring metrik yang ditentukan untuk Reservasi Kapasitas yang diidentifikasi.
`InstanceType`	Dimensi ini menyaring metrik yang ditentukan untuk jenis instance yang diidentifikasi.
`AvailabilityZone`	Dimensi ini menyaring metrik yang ditentukan untuk Availability Zone yang diidentifikasi.
`InstanceMatchCriteria`	Dimensi ini menyaring metrik yang ditentukan untuk kriteria kecocokan instance yang diidentifikasi (`openatautargeted`).
`InstancePlatform`	Dimensi ini menyaring data metrik yang ditentukan untuk platform yang diidentifikasi.
`Tenancy`	Dimensi ini menyaring metrik yang ditentukan untuk penyewaan yang diidentifikasi.

Lihat CloudWatch metrik untuk Reservasi Kapasitas

Metrik dikelompokkan berdasarkan namespace layanan, lalu dimensi yang didukung. Anda dapat menggunakan prosedur berikut untuk melihat metrik untuk Reservasi Kapasitas Anda.

Untuk melihat metrik Reservasi Kapasitas menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Jika perlu, ubah Wilayah. Dari bilah navigasi, pilih Wilayah tempat Anda Reservasi Kapasitas Anda berada. Untuk informasi selengkapnya, lihat Wilayah dan Titik Akhir.
3. Di panel navigasi, pilih Metrik.
4. Untuk Semua metrik, pilih Reservasi Kapasitas EC2.
5. Pilih dari dimensi metrik sebelumnya di Semua Reservasi Kapasitas, Berdasarkan Reservasi Kapasitas, Berdasarkan Jenis Instance, Berdasarkan Zona Ketersediaan, Berdasarkan Platform,

Berdasarkan Kriteria Pencocokan Instance atau Berdasarkan Penyewaan dan metrik akan dikelompokkan berdasarkan Tidak ada dimensi,,,,,, `CapacityReservationId` `InstanceType`, `AvailabilityZone` dan masing-masing. `Platform` `InstanceMatchCriteria` `Tenancy`

6. Untuk mengurutkan metrik, gunakan judul kolom. Untuk membuat grafik metrik, pilih kotak centang di sebelah metrik.

Untuk melihat metrik Reservasi Kapasitas menggunakan AWS CLI

Gunakan perintah list-metrics berikut:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Monitor Reservasi Kapasitas yang kurang dimanfaatkan

Anda dapat memantau kurangnya pemanfaatan Reservasi Kapasitas menggunakan yang berikut:

Topik

- EventBridge Acara Amazon
- Pemberitahuan Email dan AWS Health Dasbor

EventBridge Acara Amazon

AWS Health mengirimkan acara ke Amazon EventBridge ketika Reservasi Kapasitas di akun Anda kurang dari 20 persen penggunaan selama periode tertentu. Dengan EventBridge, Anda dapat menetapkan aturan yang memicu tindakan terprogram dalam menanggapi peristiwa tersebut. Misalnya, Anda dapat membuat aturan yang secara otomatis membatalkan Reservasi Kapasitas ketika pemanfaatannya turun di bawah 20 persen pemanfaatan selama periode 7 hari.

Peristiwa di EventBridge direpresentasikan sebagai objek JSON. Kolom-kolom yang unik untuk peristiwa tersebut terdapat di bagian "detail" dari objek JSON. Bidang "peristiwa" berisi nama peristiwa. Bidang "hasil" berisi status selesai dari tindakan yang memicu peristiwa. Untuk informasi selengkapnya, lihat pola EventBridge acara Amazon di Panduan EventBridge Pengguna Amazon.

Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Fitur ini tidak didukung di AWS GovCloud (US).

Peristiwa

AWS Health mengirimkan peristiwa berikut ketika penggunaan kapasitas untuk Reservasi Kapasitas di bawah 20 persen.

- `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`

  Berikut ini adalah contoh peristiwa yang dihasilkan ketika Reservasi Kapasitas yang baru dibuat di bawah 20 persen penggunaan kapasitas selama periode 24 jam.

```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
    ],
    "detail": {
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
        ]
    }
```

```
    }
```

- `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY`

  Berikut ini adalah contoh peristiwa yang dihasilkan ketika satu atau lebih Reservasi Kapasitas di bawah 20 persen penggunaan kapasitas selama periode 7 hari.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/
EC2/AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium |
 Linux/UNIX | 0.0%"
            },
            {
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium |
 Linux/UNIX | 0.0%"
```

```
            }
        ]
    }
}
```

Buat EventBridge aturan

Untuk menerima pemberitahuan email saat penggunaan Reservasi Kapasitas turun di bawah 20 persen, buat topik Amazon SNS, lalu buat aturan untuk EventBridge `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION` acara tersebut.

Untuk membuat topik Amazon SNS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Pada panel navigasi, silakan pilih Topik, lalu pilih Buat topik.
3. Untuk Tipe, pilih Standar.
4. Untuk Nama, masukkan nama untuk topik baru.
5. Pilih Buat topik.
6. Pilih Buat langganan.
7. Untuk Protokol, pilih Email, lalu untuk Titik akhir, masukkan alamat email yang menerima notifikasi.
8. Pilih Buat langganan.
9. Alamat email yang dimasukkan di atas akan menerima pesan email dengan baris subjek berikut: `AWS Notification - Subscription Confirmation`. Ikuti petunjuk untuk mengonfirmasi langganan Anda.

Untuk membuat EventBridge aturan

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, pilih Aturan, lalu pilih Buat aturan.
3. Untuk Nama, masukkan nama untuk aturan baru.
4. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
5. Pilih Selanjutnya.
6. Untuk Pola peristiwa, lakukan hal berikut:

a. Untuk Sumber peristiwa, pilih Layanan AWS .
b. Untuk Layanan AWS , pilih AWS Health.
c. Untuk Tipe peristiwa, pilih EC2 ODCR Underutilization Notification.

7. Pilih Selanjutnya.
8. Untuk Target 1, lakukan hal berikut:

a. Untuk Tipe Target, pilih Layanan AWS .
b. Untuk Pilih target, pilih Topik SNS.
c. Untuk Topic, pilih topik yang Anda buat sebelumnya.

9. Pilih Berikutnya lalu Berikutnya lagi.
10. Pilih Buat aturan.

Pemberitahuan Email dan AWS Health Dasbor

AWS Health mengirimkan email dan Dasbor Health pemberitahuan berikut ketika pemanfaatan kapasitas untuk Reservasi Kapasitas di akun Anda turun di bawah 20 persen.

- Notifikasi individual untuk setiap Reservasi Kapasitas yang baru dibuat dengan pemanfaatan di bawah 20 persen selama periode 24 jam terakhir.
- Ringkasan notifikasi untuk semua Reservasi Kapasitas dengan pemanfaatan di bawah 20 persen selama periode 7 hari terakhir.

Pemberitahuan dan Dasbor Health notifikasi email dikirim ke alamat email yang terkait dengan AWS akun yang memiliki Reservasi Kapasitas. Notifikasi mencakup informasi berikut:

- ID Reservasi Kapasitas.
- Zona Ketersediaan dari Reservasi Kapasitas.
- Tingkat pemanfaatan rata-rata untuk Reservasi Kapasitas.
- Tipe instans dan platform (sistem operasi) dari Reservasi Kapasitas.

Selain itu, ketika pemanfaatan kapasitas untuk Reservasi Kapasitas di akun Anda turun di bawah 20 persen selama periode 24 jam dan 7 hari, AWS Health kirimkan acara ke. EventBridge DenganEventBridge, Anda dapat membuat aturan yang mengaktifkan tindakan otomatis, seperti mengirim pemberitahuan email atau AWS Lambda fungsi pemicu, sebagai respons terhadap

peristiwa tersebut. Untuk informasi selengkapnya, lihat Monitor Reservasi Kapasitas yang kurang dimanfaatkan.

Pantau perubahan status untuk Reservasi Kapasitas yang bertanggal di masa mendatang

Amazon EC2 mengirimkan acara ke Amazon EventBridge ketika status Reservasi Kapasitas bertanggal mendatang berubah.

Berikut ini adalah contoh dari acara ini. Dalam contoh ini, Reservasi Kapasitas bertanggal masa depan memasuki negara bagian. `scheduled` Perhatikan status yang disorot di `detail-type` lapangan.

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"EC2 Capacity Reservation Scheduled",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"yyyy-mm-ddThh:mm:ssZ",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdefg"
   ],
   "detail":{
      "capacity-reservation-id":"cr-1234567890abcdefg",
      "state":"scheduled"
   }
}
```

Nilai yang mungkin untuk `detail-type` bidang tersebut adalah:

- `Scheduled`
- `Active`
- `Delayed`
- `Unsupported`
- `Failed`
- `Expired`

Untuk informasi selengkapnya tentang status ini, lihat Lihat status Reservasi Kapasitas.

Anda dapat membuat EventBridge peristiwa Amazon yang memantau peristiwa ini dan kemudian memicu tindakan tertentu saat terjadi. Untuk informasi selengkapnya, lihat Membuat aturan yang bereaksi terhadap peristiwa di Amazon EventBridge.

Untuk membuat aturan yang memantau semua peristiwa perubahan status, Anda dapat menggunakan pola peristiwa berikut.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation"
  }]
}
```

Untuk membuat aturan yang hanya memantau perubahan status tertentu, Anda dapat menggunakan pola peristiwa berikut.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation state"
  }]
}
```

Misalnya, pola peristiwa berikut memantau peristiwa yang dikirim saat Reservasi Kapasitas bertanggal masa depan memasuki status. `active`

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation Active"
  }]
}
```

Reservasi Kapasitas yang Dapat Diputus

Reservasi Kapasitas Interruptible membantu Anda membuat kapasitas yang tidak terpakai tersedia sementara untuk beban kerja lain dalam akun Anda. Ini memberi Anda kontrol untuk merebut kembali kapasitas saat dibutuhkan. Saat Anda merebut kembali kapasitas, setiap instance yang berjalan di dalam reservasi yang dapat diinterupsi akan dihentikan. Setelah membuat reservasi yang dapat

diinterupsi, Anda dapat membagikannya dengan AWS akun tambahan atau AWS organisasi Anda menggunakan AWS Resource Access Manager (RAM).

Gunakan Reservasi Kapasitas yang Dapat Diinterupsi jika Anda memiliki kapasitas cadangan yang tidak terpakai selama periode di luar puncak, di antara penerapan, atau saat beban kerja menurun. Jika Anda tahu tim lain yang dapat menggunakan kapasitas ini, Anda dapat membuatnya tersedia dengan membuat Reservasi Kapasitas yang dapat diinterupsi. Ketika beban kerja kritis Anda membutuhkan kapasitas kembali, Anda dapat merebutnya kembali.

Anda dapat menggunakan Reservasi Kapasitas yang dapat diinterupsi sebagai salah satu dari berikut ini:

- Pemilik Kapasitas — Anda memiliki Reservasi Kapasitas sumber dan membuat Reservasi Kapasitas yang dapat diinterupsi untuk berbagi kapasitas yang tidak terpakai dengan tim lain sambil mempertahankan kendali untuk merebut kembali bila diperlukan.
- Kapasitas konsumen — Anda meluncurkan instance ke reservasi interuptible bersama, memahami bahwa instans Anda dapat dihentikan ketika pemilik merebut kembali kapasitas.

Topik

- Cara kerjanya
- Penagihan
- Pertimbangan-pertimbangan
- Reservasi Kapasitas Interruptible untuk pemilik kapasitas
- Reservasi Kapasitas Interruptible untuk konsumen kapasitas
- Pantau Reservasi Kapasitas yang Dapat Diinterupsi dengan dan EventBridge CloudTrail

Cara kerjanya

Agar kapasitas yang tidak terpakai tersedia bagi tim lain, buat reservasi yang dapat diinterupsi dengan menentukan jumlah instans yang tidak terpakai yang ingin Anda bagikan dari reservasi sumber Anda. Saat Anda membuat reservasi yang dapat diinterupsi, kami mentransfer instans ini dari reservasi sumber Anda ke reservasi interuptible baru dalam akun Anda.

Kami mempertahankan hubungan antara reservasi sumber dan Reservasi Kapasitas yang dapat terputus. Akibatnya, ketika Anda merebut kembali kapasitas Anda, setiap instans konsumen yang sedang berjalan dihentikan, dan kapasitas dikembalikan ke reservasi sumber asli Anda.

Fitur kunci:

- Buat kapasitas yang tidak terpakai tersedia sementara sambil mempertahankan kontrol untuk merebutnya kembali
- Merebut kembali kapasitas kapan saja. Untuk informasi selengkapnya, lihat Proses reklamasi dan pelacakan
- Berbagi dengan akun tambahan atau AWS organisasi Anda menggunakan AWS Resource Access Manager (RAM)

Penagihan

Saat Anda membuat reservasi yang dapat diinterupsi, Anda ditagih sebagai reservasi baru yang independen. Ini membagi tagihan Anda:

- Reservasi sumber: Anda ditagih untuk total kapasitas dikurangi kapasitas yang dialokasikan
- Reservasi interruptible: Anda ditagih untuk kapasitas yang dialokasikan

Untuk informasi selengkapnya tentang penagihan Reservasi Kapasitas Sesuai Permintaan, lihat harga dan penagihan Reservasi Kapasitas.

Pertimbangan-pertimbangan

Sebelum menggunakan Reservasi Kapasitas yang Dapat Diinterupsi, tinjau batasan dan persyaratan berikut yang berlaku untuk pemilik kapasitas dan konsumen.

Pemilik kapasitas

- Anda tidak dapat secara langsung mengubah atau membatalkan Reservasi Kapasitas yang dapat diinterupsi. Untuk mengeditnya, perbarui kapasitas yang dialokasikan dari Reservasi Kapasitas sumber.
- Anda hanya dapat melihat, meluncurkan, menandai, berbagi, dan menetapkan tagihan untuk reservasi yang dapat terputus.
- Anda hanya dapat membuat satu alokasi interuptible per sumber Reservasi Kapasitas.

Kapasitas konsumen

- Reservasi Kapasitas Interruptible secara default adalah Reservasi Kapasitas yang ditargetkan, jadi Anda harus menargetkannya dalam peluncuran instans Anda.

- Anda tidak dapat menambahkan Reservasi Kapasitas yang dapat diinterupsi ke grup reservasi kapasitas.
- Kami menyarankan Anda hanya menggunakan Reservasi Kapasitas yang dapat terputus untuk aplikasi yang dapat terganggu.
- Instans Anda akan dihentikan ketika pemilik merebut kembali kapasitas - tidak ada fallback ke On-Demand atau Spot. Untuk informasi selengkapnya, lihat Pengalaman interupsi.

Reservasi Kapasitas Interruptible untuk pemilik kapasitas

Pemilik kapasitas adalah akun yang memiliki Reservasi Kapasitas sumber dan membuat Reservasi Kapasitas yang dapat diinterupsi untuk berbagi kapasitas yang tidak terpakai dengan tim lain sambil mempertahankan kendali untuk merebut kembali bila diperlukan.

Bagian ini mencakup bagaimana Anda (pemilik kapasitas) dapat membuat, memodifikasi, merebut kembali, dan melacak Reservasi Kapasitas yang dapat diinterupsi.

Topik

- Membuat Reservasi Kapasitas yang Dapat Diinterupsi
- Lihat Reservasi Kapasitas Anda yang Dapat Diinterupsi
- Memodifikasi Reservasi Kapasitas yang Dapat Diinterupsi
- Proses reklamasi dan pelacakan
- Berbagi reservasi yang dapat terputus

Membuat Reservasi Kapasitas yang Dapat Diinterupsi

Buat Reservasi Kapasitas yang dapat diinterupsi untuk membuat kapasitas yang tidak terpakai dari reservasi sumber Anda tersedia untuk beban kerja lain sambil mempertahankan kontrol untuk merebut kembali saat diperlukan.

Prasyarat

Sebelum membuat alokasi yang dapat diinterupsi, pastikan Reservasi Kapasitas Sesuai Permintaan sumber Anda memenuhi persyaratan ini:

- Reservasi Kapasitas Anda harus dalam keadaan aktif tanpa tanggal akhir yang ditetapkan. Anda tidak dapat membuat alokasi dari reservasi yang tertunda, kedaluwarsa, dibatalkan, atau memiliki tanggal akhir yang dijadwalkan.

- Reservasi Kapasitas Anda harus memiliki kapasitas yang tersedia untuk alokasi. Anda hanya dapat mengalokasikan instance yang tersedia (juga disebut kapasitas yang tidak digunakan).
- Anda hanya dapat membuat satu alokasi interuptible per sumber Reservasi Kapasitas. Jika alokasi sudah ada, Anda harus memodifikasi atau membatalkannya sebelum membuat yang baru.
- Anda dapat mengalokasikan maksimum 1000 instans sekaligus ke Reservasi Kapasitas yang dapat diinterupsi.

Penggunaan dapat menggunakan konsol atau AWS CLI untuk membuat Reservasi Kapasitas interuptible.

Console

Untuk membuat Reservasi Kapasitas yang Dapat Diinterupsi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Reservasi Kapasitas.
3. Pilih Reservasi Kapasitas Anda.
4. Pilih Tindakan, Buat alokasi yang dapat diinterupsi.
5. Agar Instans mengalokasikan, masukkan jumlah instans yang akan dialokasikan.
6. (Opsional) Tambahkan tanda.
7. Pilih Buat alokasi kapasitas yang dapat diinterupsi.

AWS CLI

Untuk membuat Reservasi Kapasitas yang Dapat Diinterupsi

Gunakan perintah create-interruptible-capacity-reservation-allocation:

```
aws ec2 create-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --instance-count 10
```

Lihat Reservasi Kapasitas Anda yang Dapat Diinterupsi

Setelah membuat Reservasi Kapasitas yang dapat diinterupsi, Anda dapat melihat reservasi yang dapat terputus di akun Anda atau dari sumber daya tertentu.

Lihat semua Reservasi Kapasitas yang dapat diinterupsi di akun Anda

Gunakan prosedur berikut untuk melihat Reservasi Kapasitas yang dapat terputus di akun Anda.

Console

Untuk melihat Reservasi Kapasitas yang dapat diinterupsi di akun Anda

1. Buka halaman Reservasi Kapasitas di konsol.
2. Cari reservasi dengan Interruptible di kolom type.
3. Pilih reservasi interruptible untuk melihat detailnya.

AWS CLI

Untuk melihat Reservasi Kapasitas yang dapat diinterupsi di akun Anda

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-id cr-interruptible-id \
    --filters Name=interruptible,Values=true
```

Lihat Reservasi Kapasitas yang Dapat Diinterupsi dari sumber tertentu

Gunakan prosedur berikut untuk melihat Reservasi Kapasitas yang dapat diinterupsi yang dibuat dari Reservasi Kapasitas sumber tertentu.

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-id cr-source-id
```

Dalam respons, Anda akan menemukan `interruptibleCapacityAllocations` objek yang berisi ID Reservasi Kapasitas yang dapat diinterupsi dan detail alokasi. Untuk informasi tentang struktur respons, lihat InterruptibleCapacityAllocationdi Referensi API Amazon EC2.

Memodifikasi Reservasi Kapasitas yang Dapat Diinterupsi

Gunakan prosedur berikut untuk mengedit atau membatalkan Reservasi Kapasitas Anda yang dapat terputus.

> **Note**
>
> - Saat Anda mengurangi alokasi, pertama-tama kami mengklaim kembali instance yang tersedia, lalu menjalankan instance, hingga kami memenuhi jumlah yang diminta. Jika kami dapat memenuhi hitungan sepenuhnya dengan instance yang tersedia, tidak ada penghentian yang terjadi. Semua modifikasi jumlah instans yang dialokasikan dilakukan melalui Reservasi Kapasitas sumber, tidak langsung pada Reservasi Kapasitas yang dapat diinterupsi.
> - Anda hanya dapat mengubah Reservasi Kapasitas yang dapat diinterupsi dengan maksimal 1000 instans sekaligus (naik atau turun).

Edit Reservasi Kapasitas Anda yang Dapat Diinterupsi

Gunakan prosedur berikut untuk mengedit Reservasi Kapasitas Anda yang dapat terputus.

Console

1. Dari halaman Detail Reservasi Kapasitas sumber, pilih Tindakan. Kemudian, Edit Reservasi Kapasitas yang Dapat Diinterupsi.
2. Untuk Instans untuk mengalokasikan, masukkan nomor baru:
   - Tambahkan lebih banyak kapasitas untuk berbagi
   - Dapatkan kembali kapasitas ke Reservasi Kapasitas sumber Anda
3. Pilih Perbarui.

AWS CLI

```
aws ec2 update-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --target-instance-count 80
```

Batalkan Reservasi Kapasitas yang Dapat Diinterupsi

Gunakan prosedur berikut untuk menghapus alokasi secara permanen dan mengembalikan semua kapasitas.

Console

1. Dari halaman Detail Reservasi Kapasitas sumber, buka detail alokasi kapasitas yang dapat diinterupsi.
2. Pilih Edit alokasi interuptible.
3. Untuk hitungan Instance, masukkan 0.
4. Pilih Perbarui.

AWS CLI

```
aws ec2 update-interruptible-capacity-reservation-allocation \
--capacity-reservation-id cr-1234567890abcdef0 \
--target-instance-count 0
```

Proses reklamasi dan pelacakan

Ketika Anda merebut kembali kapasitas:

- Instans yang sedang berjalan menerima peringatan interupsi 2 menit melalui acara. EventBridge
- Setelah periode pemberitahuan, instance yang berjalan dalam kapasitas reklamasi memasuki status shutting down dan dihentikan.
- Ketika dihentikan, instans reklamasi akan tersedia di Reservasi Kapasitas sumber Anda untuk penggunaan segera.
- Status alokasi Anda berubah dari pembaruan menjadi aktif saat selesai.

Reklamasi lengkap dapat memakan waktu beberapa menit tergantung pada jenis instans dan waktu shutdown. Untuk informasi selengkapnya tentang EventBridge notifikasi yang Anda terima saat proses selesai, lihatPenyelesaian reklamasi.

Lacak status reklamasi

Pantau kemajuan reklamasi dengan menjelaskan reservasi sumber Anda:

```
aws ec2 describe-capacity-reservations \
--capacity-reservation-id cr-1234567890abcdef0
```

Respons menunjukkan bidang-bidang ini di dalam `interruptibleCapacityAllocation` objek:

- `instance-count`: Instans yang dialokasikan saat ini
- `target-instance-count`: Kuantitas yang diminta setelah reklamasi
- `status`: memperbarui selama reklamasi dan aktif saat selesai

Berbagi reservasi yang dapat terputus

Anda dapat berbagi reservasi interuptible hanya dalam AWS organisasi Anda menggunakan AWS Resource Access Manager (RAM).

Pertimbangan:

- Jika akun konsumen meninggalkan organisasi Anda, reservasi yang dapat diinterupsi secara otomatis tidak dibagikan dari akun tersebut.
- Instance apa pun yang berjalan di reservasi yang tidak dibagikan pada akhirnya akan dihentikan.
- Semua fungsi berbagi lainnya berfungsi sama dengan Reservasi Kapasitas standar.

Untuk prosedur berbagi lengkap, lihat Reservasi Kapasitas Berbagi.

Reservasi Kapasitas Interruptible untuk konsumen kapasitas

Konsumen kapasitas adalah akun yang meluncurkan instance ke Reservasi Kapasitas interuptible bersama, memahami bahwa instans mereka dapat dihentikan ketika pemilik merebut kembali kapasitas.

Bagian ini mencakup bagaimana Anda (konsumen kapasitas) dapat meluncurkan instans ke dalam Reservasi Kapasitas yang dapat diinterupsi dan mempelajari tentang apa yang terjadi ketika kapasitas direklamasi oleh pemilik.

Topik

- Lihat Reservasi Kapasitas yang Dapat Diinterupsi
- Luncurkan instance ke reservasi yang dapat terputus
- Pengalaman interupsi

Lihat Reservasi Kapasitas yang Dapat Diinterupsi

Gunakan prosedur berikut untuk melihat Reservasi Kapasitas yang dapat diinterupsi.

Console

Untuk melihat Reservasi Kapasitas yang dapat terputus di akun Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Reservasi Kapasitas.
3. Di kolom Type, cari reservasi yang ditandai sebagai Interruptible.
4. Perhatikan reservasi IDs untuk digunakan dalam peluncuran instans Anda.

AWS CLI

Untuk menemukan semua Reservasi Kapasitas yang dapat terputus di akun Anda

Gunakan describe-capacity-reservationsperintah:

```
aws ec2 describe-capacity-reservations \
--filters Name=state,Values=active
```

Cari reservasi di mana `Interruptible` diatur `true` dalam tanggapan.

Untuk memfilter secara khusus untuk reservasi yang dapat terputus

Gunakan perintah berikut ini.

```
aws ec2 describe-capacity-reservations \
--capacity-reservation-ids cr-example123 \
--query 'CapacityReservations[?Interruptible==`true`]'
```

> **Note**
>
> Reservasi Kapasitas Interruptible secara default adalah Reservasi Kapasitas yang ditargetkan, jadi Anda perlu menargetkannya secara khusus dalam peluncuran instans Anda. Tidak seperti reservasi terbuka, reservasi interuptible tidak akan secara otomatis mencakup instans yang cocok. Anda harus secara eksplisit menentukan ID reservasi saat meluncurkan.

Luncurkan instance ke reservasi yang dapat terputus

Gunakan prosedur berikut untuk meluncurkan instans Amazon EC2 ke Reservasi Kapasitas yang dapat terputus dalam akun Anda.

> **Note**
>
> Kami menyarankan Anda hanya menggunakan Reservasi Kapasitas yang dapat terputus untuk aplikasi yang dapat terganggu.

Console

Untuk meluncurkan instans ke Reservasi Kapasitas yang dapat terputus

1. Buka konsol Amazon EC2 Amazon di. https://console.aws.amazon.com/ec2/
2. Dari dasbor Amazon EC2, pilih Luncurkan Instans.
3. Konfigurasikan pengaturan instans Anda.
4. Di Detail lanjutan untuk Reservasi Kapasitas, pilih Luncurkan instans yang dapat diinterupsi di reservasi aktif Anda.
5. Pilih ID reservasi interruptible dan opsi pembelian instans baru.
6. Pilih Luncurkan instans.

AWS CLI

```
aws ec2 run-instances \
--instance-type m5.large \
--count 2 \
--image-id ami-12345678 \
--instance-market-options '{
    "MarketType": "interruptible-capacity-reservation"
}' \
--capacity-reservation-specification '{
    "CapacityReservationTarget": {
        "CapacityReservationId": "cr-abcdef1234567890"
    }
}'
```

Luncurkan instans dengan Grup Auto Scaling

Anda juga dapat meluncurkan instance ke reservasi interuptible menggunakan Auto Scaling Groups dengan template peluncuran. Konfigurasikan template peluncuran dengan tipe pasar interruptible dan ID reservasi, lalu buat Grup Auto Scaling Anda menggunakan templat tersebut. Untuk informasi selengkapnya, lihat Reservasi Kapasitas yang Dapat Diinterupsi dengan EC2 Auto Scaling.

Pengalaman interupsi

Ketika kapasitas direklamasi oleh pemilik, Anda menerima pemberitahuan gangguan 2 menit sebelum penghentian instans. Peringatan ini datang melalui EventBridge acara, memberi Anda waktu untuk:

- Simpan pekerjaan Anda atau pos pemeriksaan aplikasi Anda
- Matikan proses
- Mempersiapkan untuk penghentian misalnya

EventBridge Acara ini mencakup rincian tentang contoh mana yang akan dihentikan dan waktu penghentian yang tepat. Untuk informasi selengkapnya, lihat Peringatan gangguan instance.

Pantau Reservasi Kapasitas yang Dapat Diinterupsi dengan dan EventBridge CloudTrail

Reservasi Kapasitas yang Dapat Diinterupsi mengirimkan EventBridge pemberitahuan dan CloudTrail acara untuk membantu Anda memantau dan menanggapi perubahan kapasitas.

Topik

- EventBridge pemberitahuan
- CloudTrail acara

EventBridge pemberitahuan

Anda menerima dua jenis EventBridge notifikasi. Untuk selengkapnya tentang cara mengatur EventBridge notifikasi, lihat Membuat EventBridge aturan Amazon.

Peringatan gangguan instance

Jika Anda menjalankan instance dalam reservasi yang dapat diinterupsi, Anda menerima pemberitahuan ini 2 menit sebelum instans Anda dihentikan:

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Capacity Reservation Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "[instance owner Account ID]",
    "time": "[Current time in yyyy-mm-ddThh:mm:ssZ]",
    "resources": "[instance arn]",
    "region": "[region]",
    "detail": {
        "instance-id": "[instance-id]",
        "instance-action": "terminate",
        "instance-termination-time": "yyyy-mm-ddThh:mm:ssZ",
        "azId": "[availability-zone-id]"
    }
}
```

Penyelesaian reklamasi

Jika Anda memiliki reservasi sumber, Anda menerima pemberitahuan ini ketika reklamasi kapasitas selesai:

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Interruptible Capacity Reservation Allocation Reclamation
 Completed",
    "source": "aws.ec2",
    "account": "[source Capacity Reservation Owner Account ID]",
    "time": "[Current time in yyyy-mm-ddThh:mm:ssZ]",
    "region": "us-east-1",
    "resources": ["source_cr_arn"],
    "detail": {
        "sourceCapacityReservationId": "string",
        "instanceType": "string",
        "availabilityZoneId": "string",
        "TotalInstanceCount": "current total count in the source",
        "ReclaimedInstanceCount": "count of instances added to the source",
        "targetInstanceCount": "number"
    }
}
```

CloudTrail acara

CloudTrail mencatat peristiwa ini untuk Reservasi Kapasitas yang dapat terputus:

- `InterruptibleCapacityReservationCreated`— Saat Anda membuat alokasi yang dapat diinterupsi
- `InterruptibleCapacityReservationAllocationUpdated`— Saat Anda memodifikasi alokasi
- `InterruptibleCapacityReservationCancelled`— Saat Anda membatalkan alokasi
- `CapacityReservationModified`— Saat kami memodifikasi reservasi sumber untuk alokasi
- `InterruptibleCapacityReservationInstancesTerminated`— Saat kami menghentikan instance selama reklamasi

Blok Kapasitas untuk ML

Blok Kapasitas untuk ML memungkinkan Anda untuk memesan instans komputasi akselerasi berbasis GPU di masa mendatang untuk mendukung beban kerja machine learning (ML) berdurasi pendek Anda. Instans yang berjalan di dalam Blok Kapasitas secara otomatis ditempatkan berdekatan di dalam Amazon UltraClusters EC2, untuk jaringan latensi rendah, skala petabit, dan non-pemblokiran.

Anda juga dapat menggunakan Blok Kapasitas untuk menyimpan kapasitas untuk Amazon EC2 UltraServers. UltraServers sambungkan beberapa instans Amazon EC2 dalam interkoneksi akselerator bandwidth tinggi latensi rendah. Anda dapat menggunakannya UltraServers untuk menangani AI/ML beban kerja komputasi dan memori yang paling intensif dalam pelatihan, fine-tuning, dan inferensi. Untuk informasi selengkapnya, lihat Amazon EC2 UltraServers.

Dengan Blok Kapasitas, Anda dapat melihat kapan kapasitas instans GPU tersedia di masa mendatang, dan Anda dapat menjadwalkan Blok Kapasitas untuk memulai pada waktu yang paling sesuai untuk Anda. Saat Anda memesan Blok Kapasitas, Anda mendapatkan jaminan kapasitas yang dapat diprediksi untuk instans GPU dengan membayar jumlah waktu yang Anda butuhkan saja. Kami merekomendasikan Blok Kapasitas saat Anda GPUs perlu mendukung beban kerja ML Anda selama berhari-hari atau berminggu-minggu dan tidak ingin membayar reservasi saat instans GPU Anda tidak digunakan.

Berikut ini adalah beberapa kasus penggunaan umum untuk Blok Kapasitas.

- Pelatihan model ML dan fine-tuning — Dapatkan akses tanpa gangguan ke instans GPU yang Anda pesan untuk menyelesaikan pelatihan model dan fine-tuning.
- Eksperimen dan prototipe ML — Jalankan eksperimen dan bangun prototipe yang memerlukan instans GPU untuk jangka waktu pendek.

Blok Kapasitas tersedia untuk jenis instans tertentu di beberapa AWS Wilayah. Untuk informasi selengkapnya, lihat Jenis dan Wilayah instans yang didukung.

Anda dapat memesan Blok Kapasitas dengan waktu mulai reservasi hingga delapan minggu ke depan. Setiap Blok Kapasitas dapat memiliki hingga 64 instans, dan Anda dapat memiliki hingga 256 instans di seluruh Blok Kapasitas.

Topik

- Jenis dan Wilayah instans yang didukung
- Platform yang didukung
- Pertimbangan-pertimbangan
- Sumber daya terkait
- Cara kerja Blok Kapasitas Amazon EC2
- Harga dan penagihan Blok Kapasitas
- Temukan dan beli Blok Kapasitas
- Luncurkan instance menggunakan Blok Kapasitas
- Melihat Blok Kapasitas
- Perluas Blok Kapasitas
- Bagikan Blok Kapasitas
- Buat grup sumber daya untuk Blok UltraServer Kapasitas
- Monitor Blok Kapasitas menggunakan EventBridge
- Kapasitas Pencatatan Memblokir panggilan API dengan AWS CloudTrail

Jenis dan Wilayah instans yang didukung

Instance dan UltraServer Capacity Blocks dapat digunakan dengan tipe dan AWS wilayah instance berikut.

> **Note**
>
> Ukuran Blok Kapasitas 64 instans tidak didukung untuk semua jenis instans secara keseluruhan Wilayah AWS.

Blok Kapasitas Instance

- **p6-b300.48xlarge**
  - AS Barat (Oregon) — us-west-2
- **p6-b200.48xlarge**
  - AS Timur (Virginia N.) - us-east-1
  - AS Timur (Ohio) — us-east-2
  - AS Barat (Oregon) — us-west-2
- **p5.4xlarge**
  - AS Timur (Virginia N.) - us-east-1
  - AS Timur (Ohio) — us-east-2
  - AS Barat (Oregon) — us-west-2
  - Eropa (London) — eu-west-2
  - Asia Pasifik (Mumbai) — ap-south-1
  - Asia Pasifik (Tokyo) — ap-northeast-1
  - Asia Pasifik (Sydney) — ap-southeast-2
  - Amerika Selatan (São Paulo) — sa-east-1
- **p5.48xlarge**
  - AS Timur (Virginia N.) - us-east-1
  - AS Timur (Ohio) — us-east-2
  - AS Barat (California N.) - us-west-1
  - AS Barat (Oregon) — us-west-2
  - Eropa (Stockholm) — eu-north-1
  - Eropa (London) — eu-west-2
  - Amerika Selatan (São Paulo) — sa-east-1
  - Asia Pasifik (Tokyo) — ap-northeast-1

  - Asia Pasifik (Mumbai) — `ap-south-1`
  - Asia Pasifik (Sydney) — `ap-southeast-2`
  - Asia Pasifik (Jakarta) — `ap-southeast-3`
  - Zona Lokal AS Timur (Atlanta) - `us-east-1-atl-2a`
- **`p5e.48xlarge`**
  - AS Timur (Virginia N.) - `us-east-1`
  - AS Timur (Ohio) — `us-east-2`
  - AS Barat (California N.) - `us-west-1`
  - AS Barat (Oregon) — `us-west-2`
  - Eropa (Stockholm) — `eu-north-1`
  - Eropa (London) — `eu-west-2`
  - Eropa (Spanyol) — `eu-south-2`
  - Amerika Selatan (São Paulo) — `sa-east-1`
  - Asia Pasifik (Tokyo) — `ap-northeast-1`
  - Asia Pasifik (Seoul) - `ap-northeast-2`
  - Asia Pasifik (Mumbai) — `ap-south-1`
  - Asia Pasifik (Jakarta) — `ap-southeast-3`
  - Zona Lokal AS Barat (Phoenix) - `us-west-2-phx-2a`
- **`p4d.24xlarge`**
  - AS Timur (Virginia N.) - `us-east-1`
  - AS Timur (Ohio) — `us-east-2`
  - AS Barat (Oregon) — `us-west-2`
- **`p4de.24xlarge`**
  - AS Timur (Virginia N.) - `us-east-1`
  - AS Barat (Oregon) — `us-west-2`
- **`trn1.32xlarge`**
  - AS Timur (Virginia N.) - `us-east-1`
  - AS Timur (Ohio) — `us-east-2`
  - AS Barat (California N.) - `us-west-1`
  - AS Barat (Oregon) — `us-west-2`

  - Eropa (Stockholm) — `eu-north-1`
  - Asia Pasifik (Mumbai) — `ap-south-1`
  - Asia Pasifik (Sydney) — `ap-southeast-2`
  - Asia Pasifik (Melbourne) — `ap-southeast-4`
- **`trn2.3xlarge`**
  - Asia Pasifik (Melbourne) — `ap-southeast-4`
  - Amerika Selatan (São Paulo) — `sa-east-1`
- **`trn2.48xlarge`**
  - AS Timur (Ohio) — `us-east-2`

UltraServer Blok Kapasitas

- **`Trn2`**
  - AS Timur (Ohio) — `us-east-2`
- **`P6e-GB200`**
  - Zona Lokal AS Timur (Dallas) - `us-east-1-dfw-2a`

Platform yang didukung

Blok Kapasitas untuk L saat ini mendukung instance dan hanya UltraServers dengan penyewaan default. Saat Anda menggunakan Konsol Manajemen AWS untuk membeli Blok Kapasitas, opsi platform default adalah Linux/UNIX. Saat Anda menggunakan AWS Command Line Interface (AWS CLI) atau AWS SDK untuk membeli Blok Kapasitas, opsi platform berikut tersedia:

- Linux/UNIX
- Linux Red Hat Enterprise
- RHEL dengan HA
- SUSE Linux
- Ubuntu Pro

Pertimbangan-pertimbangan

Sebelum Anda menggunakan Blok Kapasitas, pertimbangkan detail dan batasan berikut.

- Jika kami mendeteksi gangguan yang berdampak pada Blok UltraServer Kapasitas, kami akan memberi tahu Anda tetapi umumnya tidak akan mengambil tindakan untuk menghentikan instans Anda di Blok Kapasitas. Ini untuk meminimalkan gangguan yang tidak disengaja pada beban kerja Anda. Anda dapat terus menggunakan Blok UltraServer Kapasitas sebagaimana adanya setelah menerima pemberitahuan ini atau meminta perbaikan dengan menghentikan semua instance pada blok kapasitas dan mengirimkan kasus dukungan. AWS Setelah kami menerima kasus dukungan Anda, kami akan memberi tahu Anda ketika kami telah menyelesaikan remediasi dan Anda dapat meluncurkan kembali instans ke Blok Kapasitas Anda. UltraServer
- Untuk Blok `P6e-GB200` UltraServer Kapasitas, Anda harus menghentikan instans Anda setidaknya 60 menit sebelum waktu akhir Blok Kapasitas.
- Untuk membeli dan menggunakan Blok Kapasitas di Local Zones, Anda harus ikut serta dalam Zona Lokal.
- Setiap Blok Kapasitas dapat memiliki hingga 64 instans, dan Anda dapat memiliki hingga 256 instans di seluruh Blok Kapasitas.
- Anda dapat menjelaskan penawaran Blok Kapasitas yang dapat dimulai segera setelah 30 menit.
- Blok Kapasitas berakhir pada 11:30 Waktu Universal Terkoordinasi (UTC).
- Proses pengakhiran untuk instans yang berjalan di Blok Kapasitas dimulai pada pukul 11:00 Waktu Universal Terkoordinasi (UTC) pada hari terakhir reservasi.
- Blok Kapasitas dapat dipesan dengan waktu mulai hingga 8 minggu di masa mendatang.
- Pembatalan Blok Kapasitas tidak diizinkan.
- UltraServer Blok Kapasitas tidak dapat dibagikan di seluruh AWS akun atau di dalam AWS Organisasi Anda.
- Blok Kapasitas tidak dapat dipindahkan atau dipecah.
- Hanya Blok UltraServer Kapasitas yang dapat digunakan dengan grup sumber daya. Blok Kapasitas Instance tidak dapat digunakan dengan grup sumber daya. Untuk informasi selengkapnya, lihat Buat grup sumber daya untuk Blok UltraServer Kapasitas.
- Jumlah total instans yang dapat dicadangkan di Blok Kapasitas di semua akun di AWS Organisasi Anda tidak dapat melebihi 256 instans pada tanggal tertentu.
- Untuk menggunakan Blok Kapasitas, instans harus secara khusus menargetkan ID reservasi.
- Instans dalam Blok Kapasitas tidak diperhitungkan dalam batas Instans Sesuai Permintaan Anda.
- Untuk instans P5 yang menggunakan AMI kustom, pastikan Anda memiliki perangkat lunak dan konfigurasi yang diperlukan untuk EFA.

- Untuk grup node terkelola Amazon EKS, lihat Membuat grup node terkelola dengan Blok Kapasitas Amazon EC2 untuk ML. Untuk grup node yang dikelola sendiri Amazon EKS, lihat Menggunakan Blok Kapasitas untuk MLdengan node yang dikelola sendiri.

Sumber daya terkait

Setelah Anda membuat Blok Kapasitas, Anda dapat melakukan hal berikut dengan Blok Kapasitas:

- Luncurkan instance ke Blok Kapasitas. Untuk informasi selengkapnya, lihat Luncurkan instance menggunakan Blok Kapasitas.
- Buat grup Penskalaan Otomatis Amazon EC2. Untuk informasi selengkapnya, lihat Menggunakan Blok Kapasitas untuk beban kerja pembelajaran mesin di Panduan Pengguna Amazon EC2 Auto Scaling.

> **Note**
>
> Jika Anda menggunakan Amazon EC2 Auto Scaling atau Amazon EKS, Anda dapat menjadwalkan penskalaan untuk dijalankan di awal reservasi Blok Kapasitas. Dengan penskalaan terjadwal, AWS secara otomatis menangani percobaan ulang untuk Anda, jadi Anda tidak perlu khawatir menerapkan logika coba lagi untuk menangani kegagalan sementara.

- Tingkatkan alur kerja ML dengan Layanan Komputasi AWS Paralel. Untuk informasi selengkapnya, lihat Dukungan Blok Kapasitas untuk Layanan Komputasi AWS Paralel.
- Tingkatkan alur kerja ML dengan AWS ParallelCluster. Untuk informasi selengkapnya, lihat Meningkatkan alur kerja ML dengan AWS ParallelCluster dan Blok Kapasitas Amazon EC2 untuk ML.

Untuk informasi AWS selengkapnya tentang Layanan Komputasi Paralel, lihat Apa itu Layanan Komputasi AWS Paralel.

Untuk informasi lebih lanjut tentang AWS ParallelCluster, lihat Apa itu AWS ParallelCluster.

Cara kerja Blok Kapasitas Amazon EC2

Anda dapat memesan Blok Kapasitas dengan spesifikasi sebagai berikut:

- Pesan waktu mulai hingga 8 minggu sebelumnya

- Tetapkan durasi reservasi satu hingga 14 hari atau kelipatan 7 hari, hingga 182 hari (Contoh: 21 hari, 28 hari)
- Konfigurasikan hingga 64 instans per Blok Kapasitas
- Konfigurasikan hingga 256 instans di beberapa Blok Kapasitas

Untuk Amazon EC2 UltraServers, masing-masing UltraServer sesuai dengan satu Blok Kapasitas. Anda dapat meminta beberapa UltraServers melalui satu permintaan.

Anda dapat menggunakan Blok Kapasitas untuk memesan`p6-b200`,`p5`,`p5e`,`p5en`,`p4d`,`p4de`,`trn1`, dan `trn2` instance. Anda dapat membeli UltraServer jenis berikut melalui Blok Kapasitas: `P6e-GB200` dan `Trn2` (dalam pratinjau).

Untuk memesan Blok Kapasitas, Anda mulai dengan menentukan kebutuhan kapasitas Anda, termasuk jenis atau UltraServer jenis instans, jumlah instans atau UltraServers, jumlah waktu, tanggal mulai paling awal, dan tanggal akhir terbaru yang Anda butuhkan. Kemudian, Anda dapat melihat penawaran Blok Kapasitas yang tersedia yang memenuhi spesifikasi Anda. Penawaran Blok Kapasitas mencakup detail seperti waktu mulai, Zona Ketersediaan, dan harga reservasi. Harga penawaran Blok Kapasitas tergantung pada penawaran dan permintaan yang tersedia pada saat penawaran dikirimkan. Setelah Anda memesan Blok Kapasitas, harga tidak berubah. Untuk informasi selengkapnya, lihat Harga dan penagihan Blok Kapasitas.

Saat Anda membeli penawaran Blok Kapasitas, reservasi dibuat sesuai tanggal dan jumlah instans yang Anda pilih. Saat reservasi Blok Kapasitas dimulai, Anda dapat menargetkan peluncuran instans dengan menentukan ID reservasi dalam permintaan peluncuran.

Anda dapat menggunakan semua instans yang Anda pesan hingga 30 menit (misalnya jenis) atau 60 menit (untuk UltraServer jenis) sebelum waktu akhir Blok Kapasitas. Dengan 30 menit (misalnya jenis) atau 60 menit (untuk UltraServer tipe) tersisa di reservasi Blok Kapasitas Anda, kami mulai menghentikan semua instance yang berjalan di Blok Kapasitas. Kami menggunakan waktu ini untuk membersihkan instans Anda sebelum mengirimkan Blok Kapasitas ke pelanggan berikutnya. Kami memancarkan acara melalui EventBridge 10 menit sebelum proses penghentian dimulai. Untuk informasi selengkapnya, lihat Monitor Blok Kapasitas menggunakan EventBridge.

Harga dan penagihan Blok Kapasitas

Dengan Blok Kapasitas Amazon EC2 untuk M, Anda hanya membayar untuk apa yang Anda pesan. Harga Blok Kapasitas tergantung pada penawaran dan permintaan yang tersedia untuk Blok Kapasitas pada saat pembelian. Anda dapat melihat harga penawaran Blok Kapasitas sebelum Anda

memesannya. Harga Blok Kapasitas dibebankan di muka pada saat reservasi dilakukan. Saat Anda mencari Blok Kapasitas di suatu rentang tanggal, kami mengembalikan penawaran Blok Kapasitas dengan harga terendah yang tersedia. Setelah Anda memesan Blok Kapasitas, harga tidak berubah.

Ketika Anda menggunakan Blok Kapasitas, Anda membayar untuk sistem operasi yang Anda gunakan saat instans Anda berjalan. Untuk informasi selengkapnya tentang harga sistem operasi, lihat Blok Kapasitas Amazon EC2 untuk Harga ML.

Penagihan

Harga penawaran Blok Kapasitas dibebankan di muka. Pembayaran ditagih ke AWS akun Anda dalam waktu 5 menit hingga 12 jam setelah Anda membeli Blok Kapasitas. Saat pembayaran Anda diproses, sumber daya reservasi Blok Kapasitas Anda tetap dalam status `payment-pending`. Jika pembayaran Anda tidak dapat diproses setidaknya 5 menit sebelum waktu mulai pemblokiran, atau dalam 12 jam (mana yang lebih dulu), Blok Kapasitas Anda dilepaskan dan status reservasi berubah menjadi. `payment-failed`

Setelah pembayaran Anda berhasil diproses, status sumber daya Blok Kapasitas berubah dari `payment-pending` menjadi `scheduled`. Anda menerima faktur yang menunjukkan pembayaran satu kali di muka. Dalam faktur, Anda dapat mengaitkan jumlah yang dibayarkan dengan ID reservasi Blok Kapasitas.

Ketika reservasi Blok Kapasitas dimulai, Anda ditagih hanya berdasarkan sistem operasi yang Anda gunakan saat instans Anda berjalan di reservasi. Anda dapat melihat penggunaan dan biaya terkait dalam tagihan setahun Anda untuk bulan penggunaan di AWS Cost and Usage Report Anda.

> **Note**
>
> Diskon Savings Plans dan Reserved instans tidak berlaku untuk Blok Kapasitas.

Melihat tagihan Anda

Anda dapat melihat tagihan Anda di AWS Manajemen Penagihan dan Biaya konsol. Pembayaran di muka untuk Blok Kapasitas Anda muncul di bulan pembelian reservasi.

Setelah reservasi dimulai, tagihan Anda menunjukkan reservasi blok yang digunakan dan waktu yang tidak digunakan dalam baris yang terpisah. Anda dapat menggunakan item baris ini untuk melihat berapa banyak waktu yang digunakan dalam reservasi Anda. Anda hanya akan melihat biaya penggunaan di baris untuk waktu yang digunakan jika Anda menggunakan sistem operasi premium.

Untuk informasi selengkapnya, lihat Harga dan penagihan Blok Kapasitas. Tidak ada biaya tambahan untuk waktu yang tidak digunakan.

Untuk informasi selengkapnya, lihat Melihat tagihan Anda dalam Panduan Pengguna AWS Manajemen Penagihan dan Biaya .

Jika Blok Kapasitas dimulai pada bulan yang berbeda dari bulan pembelian reservasi, harga di muka dan penggunaan reservasi muncul di bawah bulan tagihan yang terpisah. Dalam ID reservasi Blok Kapasitas Anda AWS Cost and Usage Report tercantum dalam item baris Reservasi/ReservationARN dari biaya dimuka Anda dan LineItem/ResourceID di tagihan ulang tahun Anda sehingga Anda dapat mengaitkan penggunaan dengan harga di muka yang sesuai.

Temukan dan beli Blok Kapasitas

Untuk memesan Blok Kapasitas, pertama-tama Anda harus menemukan blok waktu ketika kapasitas tersedia yang sesuai dengan kebutuhan Anda. Untuk menemukan Blok Kapasitas yang tersedia untuk cadangan, Anda tentukan yang berikut.

- Jumlah instans yang Anda butuhkan
- Durasi waktu Anda membutuhkan instans
- Rentang tanggal yang Anda perlukan untuk reservasi

Untuk mencari penawaran Blok Kapasitas yang tersedia, tentukan durasi reservasi dan jumlah instans. Anda harus menentukan durasi reservasi dalam kenaikan 1 hari hingga 14 hari, dan dalam kenaikan 7 hari hingga 182 hari. Setiap Blok Kapasitas dapat memiliki hingga 64 instans, dan Anda dapat memiliki hingga 256 instans di seluruh Blok Kapasitas.

Saat Anda meminta Blok Kapasitas yang sesuai dengan spesifikasi Anda, kami memberikan detail hingga 6 blok yang tersedia. Semua Blok Kapasitas berakhir pada 11:30 UTC, sehingga blok yang dimulai pada hari yang sama akan memiliki durasi yang paling cocok dengan durasi yang Anda inginkan. Satu blok akan memiliki durasi yang sedikit kurang dari durasi yang Anda inginkan, sementara yang lain akan memiliki durasi sedikit lebih besar dari durasi yang Anda inginkan.

Detail penawaran termasuk waktu mulai reservasi, Zona Ketersediaan untuk reservasi, dan harga reservasi. Untuk informasi selengkapnya, lihat Harga dan penagihan Blok Kapasitas.

Anda dapat membeli penawaran Blok Kapasitas yang ditampilkan, atau Anda dapat memodifikasi kriteria pencarian untuk melihat opsi lain yang tersedia. Tidak ada waktu kedaluwarsa yang telah ditentukan untuk penawaran, tetapi penawaran hanya tersedia berdasarkan siapa cepat, dia dapat.

Ketika Anda membeli penawaran Blok Kapasitas, Anda mendapatkan tanggapan langsung yang mengonfirmasi bahwa Blok Kapasitas Anda telah terpesan. Setelah konfirmasi, Anda akan melihat Reservasi Kapasitas baru di akun Anda dengan tipe reservasi `capacity-block` dan `start-date` diatur ke waktu mulai penawaran yang Anda beli. Reservasi Blok Kapasitas Anda dibuat dengan status `payment-pending`. Setelah pembayaran di muka berhasil diproses, status reservasi berubah menjadi `scheduled`. Untuk informasi selengkapnya, lihat Penagihan.

> **Note**
>
> Untuk membeli dan menggunakan Blok Kapasitas di Local Zones, Anda harus ikut serta dalam Zona Lokal.

Console

Untuk menemukan dan membeli Blok Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di bilah navigasi di bagian atas layar, pilih file AWS Region. Pilihan ini penting karena ukuran Blok Kapasitas 64 instans tidak didukung untuk semua jenis instans di semua Wilayah.
3. Di panel navigasi, pilih Reservasi Kapasitas, Buat Blok Kapasitas.
4. Di bawah tipe Blok Kapasitas, pilih Instans atau UltraServers.
5. Di bawah Atribut kapasitas, Anda dapat menentukan parameter pencarian Blok Kapasitas. Secara default, platformnya adalah Linux. Jika Anda ingin memilih sistem operasi yang berbeda, gunakan AWS CLI. Untuk informasi selengkapnya, lihat Platform yang didukung.
6. Di bawah Total kapasitas (untuk Instans) atau UltraServer hitung (untuk UltraServers), tentukan jumlah instance atau yang ingin UltraServers Anda pesan.
7. Di bawah Durasi, masukkan jumlah hari atau minggu yang Anda butuhkan untuk reservasi.
8. Di bawah Rentang tanggal untuk mencari Blok Kapasitas, masukkan tanggal paling awal yang Anda inginkan untuk memulai reservasi.
9. Pilih Temukan Blok Kapasitas.
10. Jika Blok Kapasitas tersedia yang memenuhi spesifikasi Anda, Anda akan melihat penawaran di bawah Blok Kapasitas yang Disarankan. Jika ada beberapa penawaran yang memenuhi spesifikasi Anda, penawaran Blok Kapasitas paling awal yang tersedia ditampilkan. Untuk melihat penawaran Blok Kapasitas lainnya, sesuaikan input pencarian Anda dan pilih Temukan Blok Kapasitas lagi.

11. Ketika Anda menemukan penawaran Blok Kapasitas yang ingin Anda beli, pilih Berikutnya.
12. (Opsional) Pada halaman Tambahkan tanda, pilih Tambahkan tanda baru.
13. Halaman Tinjauan dan pembelian menampilkan daftar tanggal mulai dan berakhir, durasi, jumlah total instans, dan harga.

> **Note**
>
> Blok Kapasitas tidak dapat dibatalkan setelah Anda memesannya.

14. Di jendela popup Beli Blok Kapasitas, ketik konfirmasi, lalu pilih Beli.

AWS CLI

Untuk menemukan contoh Blok Kapasitas

Gunakan perintah describe-capacity-block-offerings.

Contoh berikut menemukan contoh Capacity Blocks.

```
aws ec2 describe-capacity-block-offerings \
--instance-type p5.48xlarge \
--instance-count 16 \
--start-date-range 2023-08-14T00:00:00Z \
--end-date-range 2023-10-22-T00:00:00Z \
--capacity-duration-hours 48 \
--all-availability-zones
```

Contoh berikut menemukan Blok UltraServer Kapasitas.

```
aws ec2 describe-capacity-block-offerings \
--ultraserver-type u-p6e-gb200x72 \
--ultraserver-count 1 \
--start-date-range 2023-08-14T00:00:00Z \
--end-date-range 2023-10-22-T00:00:00Z \
--capacity-duration-hours 48
```

Untuk membeli Blok Kapasitas

Gunakan purchase-capacity-blockperintah dengan ID penawaran Blok Kapasitas dari output dari contoh sebelumnya.

```
aws ec2 purchase-capacity-block \
--capacity-block-offering-id cb-0123456789abcdefg \
--instance-platform Linux/UNIX
```

PowerShell

Untuk menemukan Blok Kapasitas

Gunakan Get-EC2CapacityBlockOfferingcmdlet.

Contoh berikut menemukan contoh Capacity Blocks.

```
Get-EC2CapacityBlockOffering `
-InstanceType p5.48xlarge `
-InstanceCount 16 `
-CapacityDurationHour 48 `
-StartDateRange 2023-08-14T00:00:00Z `
-EndDateRange 2023-10-22-T00:00:00Z `
-AllAvailabilityZones $true
```

Contoh berikut menemukan Blok UltraServer Kapasitas.

```
Get-EC2CapacityBlockOffering `
-UltraserverType u-p6e-gb200x72 `
-UltraserverCount  1 `
-CapacityDurationHour 48 `
-StartDateRange 2023-08-14T00:00:00Z `
-EndDateRange 2023-10-22-T00:00:00Z
```

Untuk membeli Blok Kapasitas

Gunakan New- EC2 EC2 CapacityBlock cmdlet dengan ID penawaran Blok Kapasitas dari output contoh sebelumnya.

```
New-EC2EC2CapacityBlock `
-CapacityBlockOfferingId cb-0123456789abcdefg `
-InstancePlatform Linux/UNIX
```

Luncurkan instance menggunakan Blok Kapasitas

Untuk menggunakan Blok Kapasitas, Anda harus menentukan ID reservasi Blok Kapasitas saat meluncurkan instans. Meluncurkan sebuah instans ke dalam Blok Kapasitas mengurangi kapasitasnya yang tersedia dengan jumlah instans yang diluncurkan. Misalnya, jika kapasitas instans yang Anda beli adalah delapan instans dan Anda meluncurkan empat instans, kapasitas yang tersedia dikurangi empat instans.

Jika Anda mengakhiri instans yang berjalan di Blok Kapasitas sebelum reservasi berakhir, Anda dapat meluncurkan instans baru sebagai gantinya. Saat Anda mengakhiri atau menghentikan instans di Blok Kapasitas, dibutuhkan waktu beberapa menit untuk membersihkan instans sebelum Anda dapat meluncurkan instans lain untuk menggantinya. Selama waktu ini, instans Anda akan dalam status berhenti atau `shutting-down`. Setelah proses ini selesai, status instans Anda akan berubah menjadi `stopped` atau `terminated`. Kemudian, kapasitas yang tersedia di Blok Kapasitas Anda akan diperbarui untuk menampilkan instans lain yang tersedia untuk digunakan.

Persyaratan

- Instans Anda tidak dapat diluncurkan di subnet di Zona Ketersediaan yang berbeda dari Zona Ketersediaan tempat Blok Kapasitas Anda berada.
- Instans Anda tidak dapat diluncurkan menggunakan AMI dengan platform yang berbeda dari platform untuk Blok Kapasitas Anda.
- Untuk menggunakan Blok Kapasitas di Local Zones, Anda harus memilih masuk ke Zona Lokal.

Console

Untuk meluncurkan instance ke Blok Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah untuk reservasi Blok Kapasitas Anda.
3. Dari dasbor konsol Amazon EC2, pilih Luncurkan instans.
4. Ikuti prosedur untuk meluncurkan instans.
5. Perluas Detail lanjutan, dan untuk opsi Pembelian, pilih Blok Kapasitas. Kemudian lakukan salah satu hal berikut:
   - Untuk meluncurkan instans ke Blok Kapasitas tertentu, untuk Reservasi Kapasitas pilih Tentukan Reservasi Kapasitas, lalu pilih Blok Kapasitas.

- (UltraServers hanya) Untuk meluncurkan instance ke grup sumber daya Blok UltraServer Kapasitas, untuk Reservasi Kapasitas pilih Tentukan grup sumber daya Reservasi Kapasitas, lalu pilih grup sumber daya.

6. Pilih Luncurkan instans.

AWS CLI

Untuk meluncurkan instance menggunakan ke dalam Blok Kapasitas

Gunakan perintah run-instance dengan opsi. `instance-market-options MarketType`

Contoh berikut meluncurkan sebuah instance ke dalam Blok Kapasitas tertentu.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--count 1 \
--instance-type p5.48xlarge \
--key-name my-key-pair \
--subnet-id subnet-0abcdef1234567890 \
--instance-market-options MarketType='capacity-block' \
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_block_id}
```

Contoh berikut meluncurkan instance ke grup sumber daya Blok UltraServer Kapasitas.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--count 1 \
--instance-type p6e-gb200.36xlarge \
--key-name my-key-pair \
--subnet-id subnet-0abcdef1234567890 \
--instance-market-options MarketType='capacity-block' \
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=resource_group_arn}
```

PowerShell

Untuk meluncurkan instance ke Blok Kapasitas

Gunakan New-EC2Instancecmdlet dengan `-InstanceMarketOption` opsi yang didefinisikan sebagai berikut.

```
$marketoption = New-Object Amazon.EC2.Model.InstanceMarketOptionsRequest
$marketoption.MarketType = "capacity-block"
```

Contoh berikut meluncurkan sebuah instance ke dalam Blok Kapasitas tertentu.

```
New-EC2Instance `
-ImageId ami-0abcdef1234567890 `
-InstanceType p5.48xlarge `
-KeyName "my-key-pair" `
-SubnetId subnet-0abcdef1234567890 `
-InstanceMarketOptions $marketoption `
-CapacityReservationTarget_CapacityReservationId capacity_block_id
```

Contoh berikut meluncurkan instance ke grup sumber daya Blok UltraServer Kapasitas.

```
New-EC2Instance `
-ImageId ami-0abcdef1234567890 `
-InstanceType p6e-gb200.36xlarge `
-KeyName "my-key-pair" `
-SubnetId subnet-0abcdef1234567890 `
-InstanceMarketOptions $marketoption `
-CapacityReservationTarget_CapacityReservationResourceGroupArn "resource_group_arn"
```

Sumber daya terkait

- Untuk membuat template peluncuran yang menargetkan Blok Kapasitas, lihatthe section called “Templat peluncuran”.
- Untuk meluncurkan instans ke Blok Kapasitas menggunakan Armada EC2, lihat. Tutorial: Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Blok Kapasitas
- Untuk menyiapkan grup node terkelola EKS dengan Blok Kapasitas, lihat Membuat grup node terkelola dengan Blok Kapasitas untuk ML di Panduan Pengguna Amazon EKS.
- Untuk mengatur AWS ParallelCluster menggunakan Blok Kapasitas, lihat ML aktif AWS ParallelCluster.

Melihat Blok Kapasitas

Setelah Anda memesan Blok Kapasitas, Anda dapat melihat reservasi Blok Kapasitas di akun AWS Anda. Anda dapat menampilkan `start-date` dan `end-date` untuk melihat

kapan reservasi Anda akan dimulai dan berakhir. Sebelum reservasi Blok Kapasitas dimulai, kapasitas yang tersedia muncul adalah nol. Anda dapat melihat berapa banyak instans yang akan tersedia di Blok Kapasitas Anda dengan nilai tanda untuk kunci tanda `aws:ec2capacityreservation:incrementalRequestedQuantity`.

Saat reservasi Blok Kapasitas dimulai, status reservasi berubah dari `scheduled` menjadi `active`. Kami mengeluarkan acara melalui Amazon EventBridge untuk memberi tahu Anda bahwa Blok Kapasitas tersedia untuk digunakan. Untuk informasi selengkapnya, lihat Monitor Blok Kapasitas menggunakan EventBridge.

Blok Kapasitas memiliki status sebagai berikut:

- `payment-pending` – Pembayaran dimuka belum diproses.
- `payment-failed`—Pembayaran tidak dapat diproses dalam jangka waktu 12 jam. Blok Kapasitas Anda telah dirilis.
- `scheduled` – Pembayaran telah diproses dan reservasi Blok Kapasitas belum dimulai.
- `active` – Kapasitas terpesan tersedia untuk Anda gunakan.
- `expired` – Reservasi Blok Kapasitas kedaluwarsa secara otomatis pada tanggal dan waktu yang ditentukan dalam permintaan reservasi Anda. Kapasitas terpesan tidak lagi tersedia untuk Anda gunakan.

Console

Untuk melihat Blok Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.
3. Pada halaman ikhtisar Reservasi Kapasitas, Anda melihat tabel sumber daya dengan detail tentang semua sumber daya Reservasi Kapasitas Anda. Untuk menemukan reservasi Blok Kapasitas, pilih Blok Kapasitas dari daftar tarik-turun di atas ID Reservasi Kapasitas. Dalam tabel, Anda dapat melihat informasi tentang Blok Kapasitas seperti tanggal mulai dan berakhir, durasi, dan status.
4. Untuk detail selengkapnya tentang Blok Kapasitas, pilih ID reservasi untuk Blok Kapasitas yang ingin Anda lihat. Halaman detail Reservasi Kapasitas menampilkan semua properti reservasi dan jumlah instans yang digunakan serta tersedia di Blok Kapasitas.

> **Note**
>
> Sebelum reservasi Blok Kapasitas dimulai, kapasitas yang tersedia muncul adalah nol. Anda dapat melihat berapa banyak instans yang akan tersedia saat reservasi Blok Kapasitas dimulai dengan menggunakan nilai tanda berikut untuk kunci tanda: `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Untuk melihat Blok Kapasitas

Secara default, saat Anda menggunakan describe-capacity-reservationsperintah, reservasi Kapasitas Sesuai Permintaan dan Blok Kapasitas terdaftar. Untuk hanya melihat reservasi Blok Kapasitas Anda, filter untuk jenis pemesanan. `capacity-block`

```
aws ec2 describe-capacity-reservations \
    --filters Name=reservation-type,Values=capacity-block
```

PowerShell

Untuk melihat Blok Kapasitas

Gunakan Get-EC2CapacityReservationcmdlet. Secara default, Reservasi Kapasitas Sesuai Permintaan dan reservasi Blok Kapasitas terdaftar. Untuk hanya melihat reservasi Blok Kapasitas Anda, filter untuk jenis pemesanan. `capacity-block`

```
Get-EC2CapacityReservation `
    -Filter @{Name="reservation-type"; Values="capacity-block"}
```

Perluas Blok Kapasitas

Dengan Blok Kapasitas, Anda mencadangkan kapasitas komputasi untuk beban kerja Anda, memastikan ketersediaan dan konsistensi. Untuk mengakomodasi perubahan kebutuhan Anda, Anda dapat memperpanjang durasi Blok Kapasitas yang ada sesuai kebutuhan.

Untuk memperluas Blok Kapasitas, ia harus memiliki status `active` atau`scheduled`, dan tidak memiliki ekstensi yang ada`payment-pending`. Anda dapat meminta untuk memperpanjang durasi

Blok Kapasitas hingga minimal 1 jam atau maksimal 56 hari sebelum habis masa berlakunya. Anda dapat memperpanjang Blok Kapasitas Anda dengan kenaikan 1 hari hingga 14 hari, dan kenaikan 7 hari hingga total 182 hari (26 minggu). Saat Anda memperpanjang Blok Kapasitas, tanggal berakhirnya akan diperbarui sehingga instans Anda dapat terus berjalan tanpa gangguan.

- Tidak ada batasan jumlah ekstensi yang dapat Anda terapkan ke Blok Kapasitas
- ID Reservasi Kapasitas Anda akan tetap sama setelah memperpanjang blok
- Blok Kapasitas hanya dapat diperpanjang jika ada kapasitas yang cukup tersedia untuk mendukungnya, yang tidak dijamin.

Penagihan

Harga penawaran Blok Kapasitas dibebankan di muka. Perpanjangan akan tetap ada `payment-pending` sampai tagihan dibayarkan. Jika pembayaran Anda tidak dapat diproses dalam waktu 12 jam, atau hingga 35 menit sebelum Blok Kapasitas dijadwalkan berakhir (mana yang lebih dulu), ekstensi Anda tidak berhasil dan status berubah menjadi. `payment-failed` Reservasi Blok Kapasitas Anda akan tetap `active` dan akan dihentikan pada tanggal akhir asli.

Setelah pembayaran Anda berhasil diproses, status ekstensi Blok Kapasitas berubah menjadi `payment-succeeded` dan tanggal akhir reservasi Blok Kapasitas akan diperbarui ke tanggal akhir yang baru. Detail ekstensi Anda dapat dilihat di bagian detail Ekstensi Blok Kapasitas konsol, atau dengan menggunakan perintah describe-capacity-block-extension-history.

Perluas Blok Kapasitas Anda

Console

Untuk memperluas Blok Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.
3. Pada halaman ikhtisar Reservasi Kapasitas, Anda melihat tabel sumber daya dengan detail tentang semua sumber daya Reservasi Kapasitas Anda. Pilih ID reservasi untuk Blok Kapasitas yang ingin Anda perpanjang.
4. Dari menu tarik-turun Tindakan, pilih Perluas Blok Kapasitas.
5. Di bawah Durasi, masukkan jumlah hari atau minggu yang Anda perlukan untuk memperpanjang reservasi.

6. Pilih Temukan Blok Kapasitas.
7. Jika Blok Kapasitas tersedia yang memenuhi spesifikasi Anda, penawaran akan muncul di bawah Blok Kapasitas yang Disarankan. Untuk melihat penawaran Blok Kapasitas lainnya, sesuaikan input pencarian Anda dan pilih Temukan Blok Kapasitas lagi.
8. Ketika Anda menemukan penawaran Blok Kapasitas yang ingin Anda beli, pilih Perpanjang.
9. Di jendela pop-up Perpanjang Blok Kapasitas, masukkan konfirmasi, lalu pilih Perpanjang.

AWS CLI

Untuk menemukan ekstensi Blok Kapasitas

Gunakan perintah describe-capacity-block-extension-offerings. Contoh berikut mencari ekstensi Blok Kapasitas 48 jam untuk Reservasi yang ditentukan.

```
aws ec2 describe-capacity-block-extension-offerings \
    --capacity-reservation-id cr-1234567890abcdefg \
    --capacity-block-extension-duration-hours 48
```

Untuk memperluas Blok Kapasitas

Gunakan perintah purchase-capacity-block-extension. Tentukan ID penawaran ekstensi dari output dari contoh sebelumnya.

```
aws ec2 purchase-capacity-block-extension \
    --capacity-block-extension-offering-id cbe-0123456789abcdefg \
    --capacity-reservation-id cr-1234567890abcdefg
```

PowerShell

Untuk menemukan ekstensi Blok Kapasitas

Gunakan Get-EC2CapacityBlockExtensionOfferingcmdlet. Contoh berikut mencari ekstensi Blok Kapasitas 48 jam untuk Reservasi yang ditentukan.

```
Get-EC2CapacityBlockExtensionOffering `
    -CapacityReservationId cr-1234567890abcdefg `
    -CapacityBlockExtensionDurationHour 48
```

Untuk memperluas Blok Kapasitas

Gunakan Invoke-EC2CapacityBlockExtensioncmdlet. Tentukan ID penawaran ekstensi dari output dari contoh sebelumnya.

```
Invoke-EC2CapacityBlockExtension `
    -CapacityBlockExtensionOfferingId cbe-0123456789abcdefg `
    -CapacityReservationId cr-1234567890abcdefg
```

Bagikan Blok Kapasitas

Berbagi Blok Kapasitas memungkinkan pemilik Blok Kapasitas berbagi Blok Kapasitas Amazon EC2 dengan AWS akun lain dalam Organisasi. AWS Ini memungkinkan Anda memaksimalkan pemanfaatan kapasitas GPU cadangan di berbagai tim dan proyek untuk menggunakan Blok Kapasitas secara efisien.

AWS Akun yang memiliki Blok Kapasitas (pemilik) dapat membagikannya dengan AWS akun lain (konsumen). Pemilik dapat berbagi Blok Kapasitas dengan AWS akun tertentu di dalam AWS Organisasi mereka, unit organisasi di dalam AWS Organisasi mereka, atau seluruh AWS Organisasi. Konsumen dapat meluncurkan instans ke Blok Kapasitas yang dibagikan dengan mereka dengan cara yang sama seperti mereka meluncurkan instans ke Blok Kapasitas yang mereka miliki.

Prasyarat untuk berbagi Blok Kapasitas

Sebelum Anda dapat berbagi Blok Kapasitas, kondisi berikut harus dipenuhi:

- Anda harus memiliki Blok Kapasitas - Anda tidak dapat berbagi Blok Kapasitas yang telah dibagikan dengan Anda.
- Status Blok Kapasitas harus aktif atau terjadwal - Blok Kapasitas yang berada di negara bagian lain, seperti `expired` atau `payment-pending` tidak dapat dibagikan.
- Berbagi hanya dalam AWS Organisasi Anda - Pemilik dapat berbagi Blok Kapasitas dengan AWS akun tertentu di dalam AWS Organisasi mereka, unit organisasi di dalam AWS Organisasi mereka, atau seluruh AWS Organisasi.
- UltraServer Blok Kapasitas tidak didukung - Anda tidak dapat berbagi Blok Kapasitas untuk Amazon EC2 UltraServers.
- Kelayakan akun - Berbagi Blok Kapasitas tidak tersedia untuk AWS akun atau AWS akun baru yang memiliki riwayat penagihan terbatas.

Layanan terkait

Berbagi Blok Kapasitas terintegrasi dengan AWS Resource Access Manager (AWS RAM). AWS RAM adalah layanan yang memungkinkan Anda untuk berbagi AWS sumber daya Anda dengan AWS akun apa pun atau melalui AWS Organizations. Dengan AWS RAM, Anda dapat berbagi sumber daya yang Anda miliki dengan membuat berbagi sumber daya. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan dibagikan. Konsumen dapat berupa AWS akun individu, atau unit organisasi atau seluruh organisasi dari AWS Organizations.

Untuk informasi selengkapnya AWS RAM, lihat Panduan AWS RAM Pengguna.

Izin Blok Kapasitas Bersama

Izin untuk pemilik

Pemilik Blok Kapasitas tetap bertanggung jawab untuk mengelola Blok Kapasitas (misalnya memperluas, berbagi), dan instance yang mereka luncurkan ke dalamnya. Pemilik tidak dapat memodifikasi instance yang diluncurkan konsumen ke Blok Kapasitas yang telah mereka bagikan.

Izin untuk konsumen

Konsumen dapat meluncurkan instance ke dalam kapasitas bersama dan bertanggung jawab untuk mengelola instans tersebut. Konsumen tidak dapat melihat atau memodifikasi instans yang dimiliki oleh konsumen lain atau oleh pemilik Blok Kapasitas. Konsumen juga hanya dapat melihat total kapasitas dan kapasitas yang tersedia di Blok Kapasitas bersama.

Bagikan Blok Kapasitas

Untuk berbagi Blok Kapasitas, Anda harus menambahkannya ke pembagian sumber daya. Berbagi sumber daya adalah AWS RAM sumber daya yang memungkinkan Anda berbagi sumber daya Akun AWS.

Jika Anda menambahkan Blok Kapasitas ke pembagian sumber daya yang dibagikan dengan seluruh AWS Organisasi, konsumen di organisasi Anda akan diberikan akses ke Blok Kapasitas bersama.

Console

Untuk berbagi Blok Kapasitas yang Anda miliki menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.

3. Pilih Blok Kapasitas untuk dibagikan dan pilih Tindakan, Bagikan reservasi.
4. Pilih pembagian sumber daya untuk menambahkan Blok Kapasitas dan pilih Bagikan Reservasi Kapasitas.

   Butuh beberapa menit bagi konsumen untuk mendapatkan akses ke Blok Kapasitas bersama.

Untuk menambahkan Blok Kapasitas ke pembagian sumber daya baru

Anda harus terlebih dahulu membuat pembagian sumber daya menggunakan AWS RAM konsol. Untuk informasi selengkapnya, lihat Membuat pembagian sumber daya di Panduan AWS RAM Pengguna.

AWS CLI

Untuk berbagi Blok Kapasitas yang Anda miliki

Gunakan create-resource-sharedan associate-resource-shareperintah.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

```
aws ram associate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-
b505-7e2a-420d-6f5d3EXAMPLE \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Untuk berbagi Blok Kapasitas yang Anda miliki

Gunakan cmdlet New- RAMResource Share dan Connect- RAMResource Share.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

```
Connect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-
b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

Blok Kapasitas beroperasi berdasarkan siapa datang pertama, dilayani pertama untuk semua akun, terlepas dari status kepemilikan. Saat Anda membagikan Blok Kapasitas, jika konsumen meluncurkan instans sebelum pemilik, instans tersebut menempati kapasitas hingga konsumen menghentikan instans atau hingga 30 menit sebelum Blok Kapasitas kedaluwarsa.

Berhenti berbagi Blok Kapasitas

Anda dapat berhenti berbagi Blok Kapasitas kapan saja hingga 30 menit sebelum tanggal kedaluwarsa blok.

Apa yang terjadi ketika Anda berhenti berbagi:

- Konsumen tidak dapat lagi meluncurkan instans baru ke dalam Blok Kapasitas yang tidak dibagikan.
- Setiap instans yang berjalan terus berjalan hingga 30 menit sebelum tanggal kedaluwarsa Blok Kapasitas, kecuali dihentikan oleh konsumen.

Console

Untuk berhenti berbagi Blok Kapasitas yang Anda miliki menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Reservasi Kapasitas.
3. Pilih Blok Kapasitas dan pilih tab Berbagi.
4. Tab Berbagi mencantumkan pembagian sumber daya yang telah ditambahkan Blok Kapasitas. Pilih bagian sumber daya untuk menghapus Blok Kapasitas.
5. Pilih Hapus dari berbagi sumber daya.

AWS CLI

Untuk berhenti berbagi Blok Kapasitas yang Anda miliki

Gunakan perintah disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Untuk berhenti berbagi Blok Kapasitas yang Anda miliki

Gunakan cmdlet Putus- RAMResource Bagikan.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE"
```

Pantau penggunaan Blok Kapasitas bersama

Pemilik Blok Kapasitas dapat memantau akun mana yang menggunakan Blok Kapasitas bersama mereka dan melacak penggunaan instans per akun.

AWS CLI

Untuk memantau penggunaan Blok Kapasitas

Gunakan perintah get-capacity-reservation-usage.

```
aws ec2 get-capacity-reservation-usage \
    --capacity-reservation-id cr-1234abcd56EXAMPLE
```

API ini memungkinkan pemilik untuk:

- Lihat akun mana yang saat ini menggunakan Blok Kapasitas.
- Lihat jumlah instance yang dijalankan setiap akun.

Pemberitahuan penghentian instans

Akun pemilik dan konsumen yang memiliki instans yang berjalan di Blok Kapasitas akan menerima EventBridge peristiwa 40 menit sebelum reservasi Blok Kapasitas berakhir, yang menunjukkan bahwa setiap instans yang berjalan dalam reservasi akan mulai berakhir dalam 10 menit. Untuk informasi selengkapnya, lihat Monitor Blok Kapasitas menggunakan EventBridge.

Ekstensi Blok Kapasitas

Blok Kapasitas dapat diperpanjang saat dibagikan. Hanya akun pemilik yang dapat memperpanjang Blok Kapasitas bersama.

Ketika Blok Kapasitas diperpanjang, instans yang dijalankan yang diluncurkan oleh pemilik atau konsumen secara otomatis mewarisi tanggal kedaluwarsa yang baru, dan konsumen dapat terus menggunakan kapasitas bersama hingga tanggal kedaluwarsa baru tanpa gangguan instans apa pun.

Harga dan penagihan

Pemilik ditagih untuk Blok Kapasitas yang mereka bagikan dan membayar di muka untuk Blok Kapasitas saat mereka membelinya. Pemilik juga membayar biaya sistem operasi untuk instance yang mereka jalankan di Blok Kapasitas.

Konsumen hanya ditagih untuk biaya sistem operasi untuk instance yang mereka jalankan di Blok Kapasitas bersama. Konsumen tidak dikenakan biaya untuk reservasi Blok Kapasitas itu sendiri.

Buat grup sumber daya untuk Blok UltraServer Kapasitas

Anda dapat menggunakan AWS Resource Groups untuk membuat koleksi logis Blok UltraServer Kapasitas. Setelah Anda membuat grup sumber daya, Anda dapat menambahkan Blok UltraServer Kapasitas yang Anda miliki di akun Anda. Setelah menambahkan Blok UltraServer Kapasitas, Anda dapat menargetkan peluncuran instance ke grup sumber daya, bukan Blok Kapasitas individual. Instance yang menargetkan grup sumber daya cocok dengan Blok UltraServer Kapasitas apa pun dalam grup yang memiliki atribut yang cocok dan kapasitas yang tersedia. Jika grup sumber daya tidak memiliki Blok UltraServer Kapasitas dengan atribut yang cocok dan kapasitas yang tersedia, peluncuran instance gagal.

Jika Blok UltraServer Kapasitas dihapus dari grup sumber daya saat menjalankan instance, instance tersebut akan terus berjalan di Blok Kapasitas. Jika Blok UltraServer Kapasitas dalam grup berakhir saat menjalankan instance, instance akan dihentikan.

Anda tidak dapat menambahkan Blok Kapasitas instance ke grup sumber daya.

Untuk membuat grup sumber daya untuk Blok UltraServer Kapasitas, gunakan salah satu metode berikut.

AWS CLI

Untuk membuat grup sumber daya untuk Blok UltraServer Kapasitas

Gunakan AWS CLI perintah create-group, dan untuk `--configuration`, tentukan yang berikut ini:

```
{
  "Configuration": [
    {
      "Type": "AWS::EC2::CapacityReservationPool",
      "Parameters": [
        {
          "Name": "instance-type",
          "Values": [
            "instance_type"
          ]
        },
        {
          "Name": "reservation-type",
          "Values": [
            "capacity-block"
          ]
        }
      ]
    },
    {
      "Type": "AWS::ResourceGroups::Generic",
      "Parameters": [
        {
          "Name": "allowed-resource-types",
          "Values": [
            "AWS::EC2::CapacityReservation"
          ]
        }
      ]
    }
  ]
```

```
}
```

PowerShell

Untuk membuat grup sumber daya untuk Blok UltraServer Kapasitas

Gunakan New- RGGroup cmdlet. Untuk`-Configuration`, tentukan yang berikut ini:

```
{
  "Configuration": [
    {
      "Type": "AWS::EC2::CapacityReservationPool",
      "Parameters": [
        {
          "Name": "instance-type",
          "Values": [
            "instance_type"
          ]
        },
        {
          "Name": "reservation-type",
          "Values": [
            "capacity-block"
          ]
        }
      ]
    },
    {
      "Type": "AWS::ResourceGroups::Generic",
      "Parameters": [
        {
          "Name": "allowed-resource-types",
          "Values": [
            "AWS::EC2::CapacityReservation"
          ]
        }
      ]
    }
  ]
}
```

Setelah Anda membuat grup sumber daya untuk Blok UltraServer Kapasitas, gunakan salah satu metode berikut untuk menambahkan Blok UltraServer Kapasitas yang ada ke dalamnya.

AWS CLI

Untuk menambahkan Blok UltraServer Kapasitas ke grup sumber daya

Gunakan perintah group-resources. Untuk `--group` tentukan nama grup sumber daya yang Anda buat. Untuk`--resource-arns`, tentukan Blok ARNs UltraServer Kapasitas yang akan ditambahkan.

```
aws resource-groups group-resources \
--group MyCRGroup \
--resource-arns CapacityReservationArn
```

PowerShell

Untuk menambahkan Blok UltraServer Kapasitas ke grup sumber daya

Gunakan RGResourceAdd-cmdlet. Untuk `-Group` tentukan nama grup sumber daya yang Anda buat. Untuk`-ResourceArn` , tentukan Blok ARNs UltraServer Kapasitas yang akan ditambahkan.

Contoh berikut menambahkan dua Reservasi Kapasitas ke grup yang ditentukan.

```
Add-RGResource `
-Group MyCRGroup `
-ResourceArn CapacityReservationArn
```

Monitor Blok Kapasitas menggunakan EventBridge

Saat reservasi Blok Kapasitas Anda dimulai, Amazon EC2 akan memancarkan peristiwa EventBridge yang menunjukkan kapasitas Anda siap digunakan. Empat puluh menit sebelum reservasi Blok Kapasitas berakhir, Anda menerima EventBridge acara lain yang memberi tahu Anda bahwa setiap kejadian yang berjalan dalam reservasi akan mulai berakhir dalam 10 menit. Untuk informasi selengkapnya tentang EventBridge acara, lihat EventBridge Acara Amazon.

Peristiwa berikut menyusun peristiwa yang dipancarkan untuk Blok Kapasitas:

Blok Kapasitas Dikirimkan

Contoh berikut menunjukkan peristiwa untuk Blok Kapasitas Terkirim.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Peringatan Kedaluwarsa Blok Kapasitas

Contoh berikut menunjukkan peristiwa untuk Peringatan Kedaluwars Blok Kapasitas.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Peringatan Gangguan Instans Reservasi Kapasitas

Contoh berikut menunjukkan peristiwa untuk Peringatan Gangguan Instans Reservasi Kapasitas EC2.

```
{
```

```
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail_type": "EC2 Capacity Reservation Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "[Customer Account ID]",
    "time": "[Current time]",
    "region": "[Region]",
    "resources": [
        "[Instance ARN]"
    ],
    "detail": {
        "instance-id": "[Instance ID]",
        "instance-action": "terminate",
        "instance-termination-time": "[Current time]",
        "availability-zone-id": "[Availability Zone ID]",
        "instance-lifecycle": "capacity-block"
    }
}
```

Kapasitas Pencatatan Memblokir panggilan API dengan AWS CloudTrail

Blok Kapasitas terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Blok Kapasitas. CloudTrail menangkap panggilan API untuk Blok Kapasitas sebagai peristiwa. Panggilan yang ditangkap tersebut mencakup panggilan dari konsol Blok Kapasitas dan panggilan kode ke operasi Blok Kapasitas. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Blok Kapasitas. Jika Anda tidak membuat konfigurasi jejak, Anda masih dapat melihat kejadian terbaru dalam konsol CloudTrail di Riwayat peristiwa. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Blok Kapasitas, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Blok Kapasitas di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Blok Kapasitas, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Blok Kapasitas, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua tindakan Blok Kapasitas dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API Amazon EC2. Misalnya, panggilan ke`CapacityBlockScheduled`, dan `CapacityBlockActive` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log Blok Kapasitas

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Sebuah kejadian mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. Berkas log CloudTrail bukan merupakan jejak tumpukan terurut dari panggilan API publik, sehingga tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log untuk:

- TerminateCapacityBlocksInstances
- CapacityBlockPaymentFailed
- CapacityBlockScheduled
- CapacityBlockActive
- CapacityBlockFailed
- CapacityBlockExpired

> **Note**
>
> Beberapa bidang telah disensor dari contoh untuk privasi data.

TerminateCapacityBlocksInstances


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
```

```
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-0598c7d356eba48d7"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```

CapacityBlockPaymentFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```

CapacityBlockScheduled


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```


CapacityBlockActive


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
```

```
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```

CapacityBlockFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
```

```
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
      }
 }
```

CapacityBlockExpired

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
```

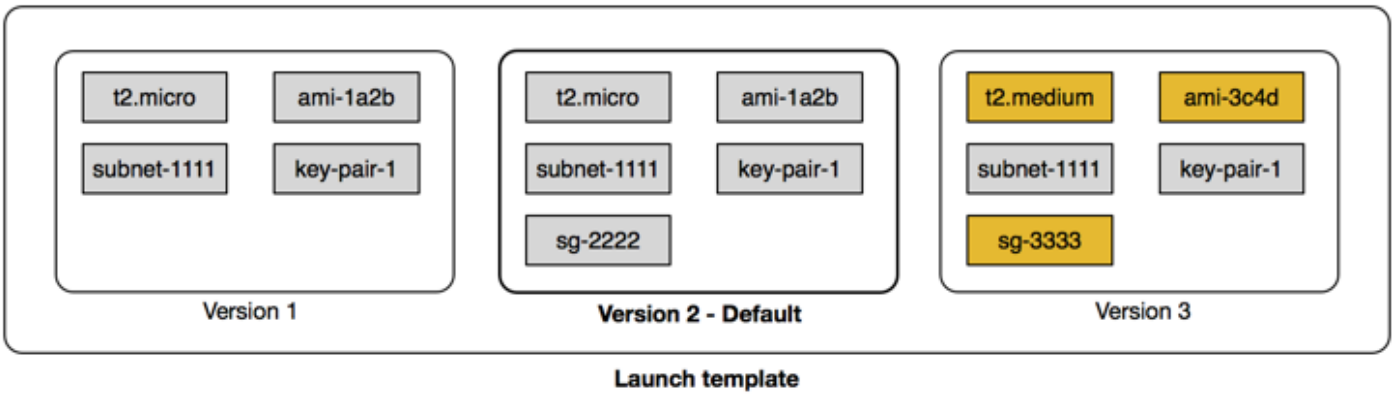
```
        }
}
```

Simpan parameter peluncuran instans di templat peluncuran Amazon EC2

Anda dapat menggunakan template peluncuran Amazon EC2 untuk menyimpan parameter peluncuran instans sehingga Anda tidak perlu menentukannya setiap kali meluncurkan instans Amazon EC2. Misalnya, Anda dapat membuat template peluncuran yang menyimpan ID AMI, jenis instans, dan setelan jaringan yang biasanya Anda gunakan untuk meluncurkan instance. Saat meluncurkan instance menggunakan konsol Amazon EC2, AWS SDK, atau alat baris perintah, Anda dapat menentukan templat peluncuran alih-alih memasukkan parameter lagi.

Untuk setiap templat peluncuran, Anda dapat membuat satu atau beberapa versi templat peluncuran bernomor. Setiap versi dapat memiliki parameter peluncuran yang berbeda. Saat Anda meluncurkan sebuah instans dari templat peluncuran, Anda dapat menggunakan templat peluncuran versi apa pun. Jika Anda tidak menentukan versi, versi default akan digunakan. Anda dapat mengatur templat peluncuran versi apa pun sebagai versi default—secara default, ini adalah templat peluncuran versi pertama.

Diagram berikut memperlihatkan templat peluncuran dengan tiga versi. Versi pertama menentukan tipe instans, ID AMI, subnet, dan pasangan kunci yang akan digunakan untuk meluncurkan instans. Versi kedua didasarkan pada versi pertama dan juga menentukan grup keamanan untuk instans tersebut. Versi ketiga menggunakan nilai yang berbeda untuk beberapa parameter. Versi 2 ditetapkan sebagai versi default. Jika Anda meluncurkan sebuah instans dari templat peluncuran ini, parameter peluncuran dari versi 2 akan digunakan jika tidak ada versi lain yang ditentukan.



Daftar Isi

- Pembatasan untuk templat peluncuran Amazon EC2
- Izin IAM diperlukan untuk templat peluncuran Amazon EC2
- Gunakan templat peluncuran Amazon EC2 untuk mengontrol peluncuran instans Amazon EC2
- Buat template peluncuran Amazon EC2
- Modifikasi templat peluncuran (mengelola versi templat peluncuran)
- Menghapus template peluncuran atau versi template peluncuran

Pembatasan untuk templat peluncuran Amazon EC2

Pembatasan berikut berlaku untuk meluncurkan template dan meluncurkan versi template:

- Kuota - Untuk melihat kuota untuk template peluncuran dan meluncurkan versi template, buka konsol Service Quotas atau gunakan perintah. list-service-quotas AWS CLI Setiap AWS akun dapat memiliki hingga maksimum 5.000 templat peluncuran per Wilayah dan hingga 10.000 versi per templat peluncuran. Akun Anda mungkin memiliki kuota yang berbeda berdasarkan usia dan riwayat penggunaannya.
- Parameter bersifat opsional - Parameter templat peluncuran bersifat opsional. Namun, Anda harus memastikan bahwa permintaan peluncuran instans Anda mencakup semua parameter yang diperlukan. Misalnya, jika template peluncuran Anda tidak menyertakan ID AMI, Anda harus menentukan ID AMI saat meluncurkan instance dengan template peluncuran ini.
- Parameter tidak divalidasi — Parameter templat peluncuran tidak sepenuhnya divalidasi saat Anda membuat templat peluncuran. Jika Anda menentukan nilai yang salah atau menggunakan kombinasi parameter yang tidak didukung, instance akan gagal diluncurkan menggunakan templat peluncuran ini. Untuk menghindari masalah, pastikan untuk menentukan nilai yang benar dan gunakan kombinasi parameter yang didukung. Misalnya, untuk meluncurkan sebuah instans di grup penempatan, Anda harus menentukan tipe instans yang didukung.
- Tag - Anda dapat menandai template peluncuran, tetapi Anda tidak dapat menandai versi template peluncuran.
- Tidak dapat diubah - Templat peluncuran tidak dapat diubah. Untuk memodifikasi templat peluncuran, Anda harus membuat templat peluncuran versi baru.
- Nomor versi – Versi templat peluncuran diberi nomor sesuai urutan pembuatannya. Saat membuat versi template peluncuran, Anda tidak dapat menentukan sendiri nomor versinya.

Izin IAM diperlukan untuk templat peluncuran Amazon EC2

Anda dapat menggunakan izin IAM untuk mengontrol apakah pengguna dapat membuat daftar, melihat, membuat, atau menghapus templat peluncuran atau meluncurkan versi templat.

> **Important**
>
> Anda tidak dapat menggunakan izin tingkat sumber daya untuk membatasi sumber daya yang dapat ditentukan pengguna dalam templat peluncuran saat mereka membuat templat peluncuran atau versi templat peluncuran. Oleh karena itu, pastikan bahwa hanya administrator tepercaya yang diberikan izin untuk membuat template peluncuran dan meluncurkan versi template.

Anda harus memberi siapa pun yang akan menggunakan template peluncuran izin yang diperlukan untuk membuat dan mengakses sumber daya yang ditentukan dalam template peluncuran. Contoh:

- Untuk meluncurkan instance dari Amazon Machine Image (AMI) pribadi bersama, pengguna harus memiliki izin peluncuran untuk AMI.
- Untuk membuat volume EBS dengan tag dari snapshot yang ada, pengguna harus memiliki akses baca ke snapshot, dan izin untuk membuat dan menandai volume.

Daftar Isi

- EC2: CreateLaunchTemplate
- EC2: DescribeLaunchTemplates
- EC2: DescribeLaunchTemplateVersions
- EC2: DeleteLaunchTemplate
- Mengontrol izin versioning
- Kontrol akses ke tanda pada templat peluncuran

EC2: CreateLaunchTemplate

Untuk membuat template peluncuran di konsol atau dengan menggunakan APIs, kepala sekolah harus memiliki `ec2:CreateLaunchTemplate` izin dalam kebijakan IAM. Kapan pun memungkinkan, gunakan tanda untuk membantu Anda mengontrol akses ke templat peluncuran di akun Anda.

Misalnya, pernyataan kebijakan IAM berikut memberikan izin kepada pengguna utama untuk membuat templat peluncuran hanya jika templat menggunakan tanda yang ditentukan (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Pengguna utama yang membuat templat peluncuran mungkin memerlukan beberapa izin terkait, seperti:

- ec2: CreateTags — Untuk menambahkan tag ke template peluncuran selama `CreateLaunchTemplate` operasi, `CreateLaunchTemplate` penelepon harus memiliki `ec2:CreateTags` izin dalam kebijakan IAM.
- ec2: RunInstances — Untuk meluncurkan instans EC2 dari template peluncuran yang mereka buat, kepala sekolah juga harus memiliki `ec2:RunInstances` izin dalam kebijakan IAM.

Untuk tindakan-tindakan yang digunakan untuk membuat sumber daya yang menerapkan tanda, para pengguna harus memiliki izin `ec2:CreateTags`. Pernyataan kebijakan IAM berikut menggunakan kunci syarat `ec2:CreateAction` agar para pengguna dapat membuat tanda hanya dalam konteks `CreateLaunchTemplate`. Pengguna tidak dapat menandai templat peluncuran yang ada atau sumber daya lainnya. Untuk informasi selengkapnya, lihat Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
    "Action": "ec2:CreateTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
```

```
        }
    }
}
```

Pengguna IAM yang membuat templat peluncuran tidak secara otomatis memiliki izin untuk menggunakan templat peluncuran yang mereka buat. Seperti pengguna utama lainnya, pembuat templat peluncuran perlu mendapatkan izin melalui kebijakan IAM. Jika pengguna IAM ingin meluncurkan instans EC2 dari templat peluncuran, mereka harus memiliki izin `ec2:RunInstances`. Saat memberikan izin ini, Anda dapat menentukan bahwa pengguna hanya dapat menggunakan templat peluncuran dengan tag tertentu atau spesifik. IDs Anda juga dapat mengontrol AMI dan sumber daya lain yang dapat dirujuk dan digunakan oleh siapa pun yang menggunakan templat peluncuran saat meluncurkan instans dengan menentukan izin tingkat sumber daya untuk panggilan `RunInstances` tersebut. Untuk kebijakan-kebijakan contoh, lihat Templat peluncuran.

EC2: DescribeLaunchTemplates

Untuk membuat daftar dan melihat templat peluncuran di akun, kepala sekolah harus memiliki `ec2:DescribeLaunchTemplates` izin dalam kebijakan IAM. Karena tindakan `Describe` tidak mendukung izin tingkat sumber daya, Anda harus menentukannya tanpa syarat dan nilai elemen sumber daya dalam kebijakan harus `"*"`.

Misalnya, pernyataan kebijakan IAM berikut memberikan izin utama untuk membuat daftar dan melihat semua templat peluncuran di akun.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
    "Resource": "*"
}
```

EC2: DescribeLaunchTemplateVersions

Kepala sekolah yang mencantumkan dan melihat templat peluncuran juga harus memiliki `ec2:DescribeLaunchTemplateVersions` izin untuk mengambil seluruh rangkaian atribut yang membentuk templat peluncuran.

Untuk membuat daftar dan melihat versi templat peluncuran di akun, kepala sekolah harus memiliki `ec2:DescribeLaunchTemplateVersions` izin dalam kebijakan IAM. Karena tindakan `Describe`

tidak mendukung izin tingkat sumber daya, Anda harus menentukannya tanpa syarat dan nilai elemen sumber daya dalam kebijakan harus "*".

Misalnya, pernyataan kebijakan IAM berikut memberikan izin utama untuk membuat daftar dan melihat semua versi template peluncuran di akun.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

EC2: DeleteLaunchTemplate

> **Important**
>
> Berhati-hatilah saat memberikan izin kepada pengguna utama untuk menghapus sumber daya. Menghapus template peluncuran dapat menyebabkan kegagalan dalam AWS sumber daya yang bergantung pada template peluncuran.

Untuk menghapus templat peluncuran, pengguna utama harus memiliki izin `ec2:DeleteLaunchTemplate` dalam kebijakan IAM. Sebisa mungkin, gunakan kunci syarat berbasis tanda untuk membatasi izin.

Misalnya, pernyataan kebijakan IAM berikut memberikan izin utama untuk menghapus template peluncuran hanya jika template memiliki tag yang ditentukan (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Atau, Anda dapat menggunakan ARNs untuk mengidentifikasi template peluncuran yang berlaku untuk kebijakan IAM.

Template peluncuran memiliki ARN berikut.

```
"Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/lt-09477bcd97b0d310e"
```

Anda dapat menentukan beberapa ARNs dengan melampirkannya dalam daftar, atau Anda dapat menentukan `Resource` nilai `"*"` tanpa `Condition` elemen untuk memungkinkan prinsipal menghapus template peluncuran apa pun di akun.

Mengontrol izin versioning

Untuk administrator tepercaya, Anda dapat memberikan akses untuk membuat dan menghapus versi templat peluncuran, dan untuk mengubah versi default templat peluncuran, dengan menggunakan kebijakan IAM yang mirip dengan contoh berikut.

Important

Berhati-hatilah saat memberikan izin kepada kepala sekolah untuk membuat versi template peluncuran atau memodifikasi templat peluncuran.

- Saat membuat versi templat peluncuran, Anda memengaruhi AWS sumber daya apa pun yang memungkinkan Amazon EC2 meluncurkan instans atas nama Anda dengan versi tersebut. `Latest`
- Saat Anda memodifikasi templat peluncuran, Anda dapat mengubah versi mana yang merupakan versi `Default` dan karenanya memengaruhi AWS sumber daya apa pun yang memungkinkan Amazon EC2 meluncurkan instans atas nama Anda dengan versi yang dimodifikasi ini.

Anda juga perlu berhati-hati dalam menangani AWS sumber daya yang berinteraksi dengan `Latest` atau `Default` meluncurkan versi template, seperti Armada EC2 dan Armada Spot. Ketika versi templat peluncuran yang berbeda digunakan `Latest` atau `Default`, Amazon EC2 tidak memeriksa kembali izin untuk tindakan yang harus diselesaikan saat meluncurkan instans baru untuk memenuhi kapasitas target armada karena tidak ada interaksi pengguna dengn sumber daya AWS . Dengan memberikan izin pengguna untuk memanggil `CreateLaunchTemplateVersion` dan `ModifyLaunchTemplate` APIs, pengguna secara efektif juga diberikan `iam:PassRole` izin jika mereka mengarahkan

armada ke versi template peluncuran yang berbeda yang berisi profil instance (wadah untuk peran IAM). Ini berarti bahwa pengguna berpotensi memperbarui template peluncuran untuk meneruskan peran IAM ke instans meskipun mereka tidak memiliki `iam:PassRole` izin. Anda dapat mengelola risiko ini dengan berhati-hati saat memberikan izin kepada siapa yang dapat membuat dan mengelola versi templat peluncuran.

EC2: CreateLaunchTemplateVersion

Untuk menghapus templat peluncuran versi baru, pengguna utama harus memiliki izin `ec2:CreateLaunchTemplateVersion` untuk templat peluncuran dalam kebijakan IAM.

Misalnya, pernyataan kebijakan IAM berikut memberikan izin kepada pengguna utama untuk membuat templat peluncuran hanya jika versi menggunakan tanda yang ditentukan (*`environment`*=*`production`*). Atau, Anda dapat menentukan satu atau beberapa template peluncuran ARNs, atau Anda dapat menentukan `Resource` nilai `"*"` tanpa `Condition` elemen untuk memungkinkan prinsipal membuat versi template peluncuran apa pun di akun.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

EC2: DeleteLaunchTemplateVersion

Important

Seperti biasa, Anda harus berhati-hati saat memberikan izin kepada pengguna utama untuk menghapus sumber daya. Menghapus versi template peluncuran dapat menyebabkan kegagalan pada AWS sumber daya yang bergantung pada versi template peluncuran.

Untuk menghapus versi templat peluncuran, pengguna utama harus memiliki izin `ec2:DeleteLaunchTemplateVersion` untuk templat peluncuran dalam kebijakan IAM.

Misalnya, pernyataan kebijakan IAM berikut memberikan izin kepada pengguna utama untuk menghapus templat peluncuran hanya jika versi menggunakan tanda yang ditentukan (*environment*=*production*). Atau, Anda dapat menentukan satu atau beberapa template peluncuran ARNs, atau Anda dapat menentukan `Resource` nilai `"*"` tanpa `Condition` elemen untuk memungkinkan prinsipal menghapus versi template peluncuran apa pun di akun.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

EC2: ModifyLaunchTemplate

Untuk mengubah versi `Default` yang dikaitkan dengan templat peluncuran, pengguna utama harus memiliki izin `ec2:ModifyLaunchTemplate` untuk templat peluncuran dalam kebijakan IAM.

Misalnya, pernyataan kebijakan IAM berikut memberikan izin kepada pengguna utama untuk memodifikasi templat peluncuran hanya jika templat menggunakan tanda yang ditentukan (*environment*=*production*). Atau, Anda dapat menentukan satu atau beberapa template peluncuran ARNs, atau Anda dapat menentukan `Resource` nilai `"*"` tanpa `Condition` elemen untuk memungkinkan prinsipal memodifikasi template peluncuran apa pun di akun.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
```

```
    }
}
```

Kontrol akses ke tanda pada templat peluncuran

Anda dapat menggunakan kunci syarat untuk membatasi izin penandaan jika sumber daya adalah templat peluncuran. Misalnya, kebijakan IAM berikut hanya mengizinkan penghapusan tanda dengan kunci *temporary* dari templat peluncuran di akun dan Wilayah yang ditentukan.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Untuk informasi selengkapnya tentang kunci syarat yang dapat Anda gunakan untuk mengontrol kunci tanda dan nilai tanda yang dapat diterapkan ke sumber daya Amazon EC2, lihat Mengendalikan akses ke tanda-tanda tertentu.

Gunakan templat peluncuran Amazon EC2 untuk mengontrol peluncuran instans Amazon EC2

Anda dapat mengontrol konfigurasi instans Amazon EC2 Anda dengan menentukan bahwa pengguna hanya dapat meluncurkan instans jika mereka menggunakan template peluncuran, dan bahwa mereka hanya dapat menggunakan template peluncuran tertentu. Anda juga dapat mengontrol siapa yang dapat membuat, memodifikasi, mendeskripsikan, dan menghapus templat peluncuran serta meluncurkan versi templat.

Gunakan templat peluncuran untuk mengontrol parameter peluncuran

Template peluncuran dapat berisi semua atau beberapa parameter untuk mengonfigurasi instance saat peluncuran. Namun, saat meluncurkan instance menggunakan template peluncuran, Anda dapat mengganti parameter yang ditentukan dalam template peluncuran. Atau, Anda dapat menentukan parameter tambahan yang tidak ada di templat peluncuran.

> **Note**
>
> Anda tidak dapat menghapus parameter template peluncuran selama peluncuran (misalnya, Anda tidak dapat menentukan nilai null untuk parameter). Untuk menghapus parameter, buat templat peluncuran versi baru tanpa parameter dan gunakan versi tersebut untuk meluncurkan instans.

Untuk meluncurkan instance, pengguna harus memiliki izin untuk menggunakan `ec2:RunInstances` tindakan. Pengguna juga harus memiliki izin untuk membuat atau menggunakan sumber daya yang dibuat atau dikaitkan dengan instans. Anda dapat menggunakan izin tingkat sumber daya untuk tindakan `ec2:RunInstances` untuk mengontrol parameter peluncuran yang dapat ditentukan pengguna. Atau, Anda dapat memberi pengguna izin untuk meluncurkan sebuah instans menggunakan templat peluncuran. Ini memungkinkan Anda untuk mengelola parameter peluncuran di templat peluncuran, bukan di kebijakan IAM, dan untuk menggunakan templat peluncuran sebagai sarana otorisasi untuk meluncurkan instans. Misalnya, Anda dapat menentukan bahwa pengguna hanya dapat meluncurkan instans menggunakan templat peluncuran, dan bahwa mereka hanya dapat menggunakan templat peluncuran tertentu. Anda juga dapat mengontrol parameter peluncuran yang dapat diganti pengguna di templat peluncuran. Misalnya kebijakan, lihat .Templat peluncuran

Mengontrol penggunaan templat peluncuran

Secara default, pengguna tidak memiliki izin untuk menggunakan templat peluncuran. Anda dapat membuat kebijakan yang memberikan izin kepada pengguna untuk membuat, memodifikasi, menjelaskan, dan menghapus templat peluncuran serta versi templat peluncuran. Anda juga dapat menerapkan izin tingkat sumber daya ke beberapa tindakan templat peluncuran untuk mengontrol kemampuan pengguna untuk menggunakan sumber daya tertentu untuk tindakan tersebut. Untuk informasi selengkapnya, lihat contoh kebijakan berikut ini: Contoh: Cara menggunakan templat peluncuran.

Berhati-hatilah saat memberikan izin kepada pengguna untuk menggunakan tindakan `ec2:CreateLaunchTemplate` dan `ec2:CreateLaunchTemplateVersion`. Anda tidak dapat menggunakan izin tingkat sumber daya untuk mengontrol sumber daya mana yang dapat ditentukan pengguna dalam templat peluncuran. Untuk membatasi sumber daya yang digunakan untuk meluncurkan sebuah instans, pastikan Anda memberikan izin untuk membuat templat peluncuran dan meluncurkan versi templat hanya untuk administrator yang sesuai.

Masalah keamanan penting saat menggunakan templat peluncuran dengan Armada EC2 atau Armada Spot

Untuk menggunakan templat peluncuran, Anda harus memberikan izin kepada pengguna untuk membuat, memodifikasi, mendeskripsikan, dan menghapus templat peluncuran dan versi templat peluncuran. Anda dapat mengontrol siapa yang dapat membuat templat peluncuran dan meluncurkan versi templat dengan mengontrol akses ke tindakan `ec2:CreateLaunchTemplate` dan `ec2:CreateLaunchTemplateVersion`. Anda juga dapat mengontrol siapa yang dapat memodifikasi templat peluncuran dengan mengontrol akses ke tindakan `ec2:ModifyLaunchTemplate`.

> **Important**
>
> Jika Armada EC2 atau Armada Spot dikonfigurasi untuk menggunakan versi templat peluncuran Terbaru atau Default, armada tidak mengetahui apakah Terbaru atau Default yang nantinya diubah untuk menunjuk ke versi templat peluncuran yang berbeda. Ketika versi templat peluncuran yang berbeda digunakan untuk Terbaru atau Default, Amazon EC2 tidak memeriksa kembali izin untuk tindakan yang harus diselesaikan saat meluncurkan instans baru untuk memenuhi kapasitas target armada. Ini adalah pertimbangan penting saat memberikan izin kepada siapa yang dapat membuat dan mengelola versi templat peluncuran, terutama tindakan `ec2:ModifyLaunchTemplate` yang memungkinkan pengguna untuk mengubah versi templat peluncuran default.

Dengan memberikan izin pengguna untuk menggunakan tindakan EC2 untuk template peluncuran APIs, pengguna juga secara efektif diberikan `iam:PassRole` izin jika mereka membuat atau memperbarui Armada EC2 atau Armada Spot untuk menunjuk ke versi template peluncuran berbeda yang berisi profil instance (wadah untuk peran IAM). Ini berarti bahwa pengguna berpotensi memperbarui template peluncuran untuk meneruskan peran IAM ke instans meskipun mereka tidak memiliki `iam:PassRole` izin. Untuk informasi selengkapnya dan contoh kebijakan IAM, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya, lihat Mengontrol penggunaan templat peluncuran dan Contoh: Cara menggunakan templat peluncuran.

Buat template peluncuran Amazon EC2

Anda dapat membuat template peluncuran Amazon EC2 dengan menentukan nilai Anda sendiri untuk parameter konfigurasi instans, atau dengan mendapatkan nilai dari template peluncuran yang ada atau instans Amazon EC2.

Anda tidak perlu menentukan nilai untuk setiap parameter dalam template peluncuran; Anda hanya perlu menentukan satu parameter konfigurasi instance untuk membuat template peluncuran. Untuk menunjukkan parameter yang Anda pilih untuk tidak ditentukan, pilih Jangan sertakan dalam templat peluncuran saat menggunakan konsol. Saat menggunakan alat baris perintah, jangan sertakan parameter untuk menunjukkan bahwa Anda memilih untuk tidak menentukannya di template peluncuran.

Jika Anda ingin menentukan AMI di template peluncuran, Anda dapat memilih AMI, atau menentukan parameter Systems Manager yang akan menunjuk ke AMI pada peluncuran instance.

Ketika sebuah instance diluncurkan dengan template peluncuran, nilai-nilai yang ditentukan dalam template peluncuran digunakan untuk mengkonfigurasi parameter instance yang sesuai. Jika nilai tidak ditentukan dalam template peluncuran, maka nilai default untuk parameter instance yang sesuai digunakan.

Tugas

- Buat template peluncuran dengan menentukan parameter
- Buat templat peluncuran dari templat peluncuran yang ada
- Buat templat peluncuran dari instans
- Gunakan parameter Systems Manager alih-alih ID AMI

Buat template peluncuran dengan menentukan parameter

Untuk membuat templat peluncuran, Anda harus menentukan nama templat peluncuran dan setidaknya satu parameter konfigurasi instans.

Untuk deskripsi setiap parameter, lihatReferensi untuk parameter konfigurasi EC2 instans Amazon.

Console

Untuk membuat templat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Di panel navigasi, pilih Templat Peluncuran, lalu pilih Buat templat peluncuran.
3. Di bawah Launch nama template dan deskripsi, lakukan hal berikut:

   a. Untuk Nama templat peluncuran, masukkan nama deskriptif untuk templat peluncuran.

   b. Untuk Deskripsi versi templat, berikan deskripsi singkat tentang versi templat peluncuran ini.

   c. Untuk menandai template peluncuran saat pembuatan, perluas tag Template, pilih Tambahkan tag baru, lalu masukkan kunci tag dan pasangan nilai. Pilih Tambahkan tanda baru lagi untuk setiap tanda tambahan yang akan ditambahkan.

   > **Note**
   >
   > Untuk menandai sumber daya yang dibuat saat instans diluncurkan, Anda harus menentukan tanda di bawah Tag sumber daya. Untuk informasi lebih lanjut, lihat Langkah 9 dalam prosedur ini.

4. Di bawah Gambar Aplikasi dan OS (Gambar Mesin Amazon), Anda dapat menyimpan Jangan sertakan dalam template peluncuran yang dipilih, atau memilih sistem operasi (OS) untuk instance, lalu pilih AMI. Atau, Anda dapat menentukan parameter Systems Manager alih-alih menentukan AMI. Untuk informasi selengkapnya, lihat Gunakan parameter Systems Manager alih-alih ID AMI.

   AMI adalah template yang berisi sistem operasi dan perangkat lunak yang diperlukan untuk meluncurkan sebuah instance.

5. Di bawah Jenis instans, Anda dapat menyimpan Jangan sertakan dalam templat peluncuran yang dipilih, atau memilih jenis instans, atau menentukan atribut instance dan membiarkan Amazon EC2 mengidentifikasi jenis instans dengan atribut tersebut.

   > **Note**
   >
   > Menentukan atribut instance hanya didukung jika template peluncuran digunakan oleh grup Auto Scaling, Armada EC2, dan Armada Spot untuk meluncurkan instans. Untuk informasi selengkapnya, lihat Membuat grup instance campuran menggunakan pemilihan tipe instans berbasis atribut dan. Tentukan atribut untuk pemilihan tipe contoh untuk Armada EC2 atau Armada Spot

Jika Anda berencana untuk menggunakan template peluncuran di wizard instance peluncuran atau dengan RunInstances API, Anda tidak dapat menentukan atribut tipe instance.

Jenis instans menentukan konfigurasi perangkat keras (CPU, memori, penyimpanan, dan kapasitas jaringan) dan ukuran komputer host yang digunakan untuk sebuah instance.

Jika Anda tidak yakin jenis instance mana yang harus dipilih, Anda dapat melakukan hal berikut:

- Pilih Bandingkan jenis instans untuk membandingkan jenis instans yang berbeda dengan atribut berikut: jumlah vCPUs, arsitektur, jumlah memori (GiB), jumlah penyimpanan (GB), jenis penyimpanan, dan kinerja jaringan.
- Pilih Dapatkan saran untuk mendapatkan panduan dan saran untuk jenis instans dari pencari jenis instans EC2. Untuk informasi selengkapnya, lihat Dapatkan rekomendasi dari pencari tipe instans EC2.

> **Note**
>
> Bergantung pada saat Anda membuat akun, Anda mungkin memenuhi syarat untuk menggunakan Amazon EC2 di bawah Tingkat Gratis.
> Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan usianya kurang dari 12 bulan, Anda dapat menggunakan Amazon EC2 di bawah Tingkat Gratis dengan memilih jenis instans t2.micro, atau jenis instans t3.micro di Wilayah di mana t2.micro tidak tersedia. Ketahuilah bahwa ketika Anda meluncurkan instans t3.micro, default ke mode Tidak Terbatas, yang mungkin dikenakan biaya tambahan berdasarkan penggunaan CPU. Jika jenis instans dapat digunakan di bawah Tingkat Gratis, itu diberi label Tingkat Gratis yang memenuhi syarat.
> Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, Anda dapat menggunakan jenis instans t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large, dan m7i-flex.large selama 6 bulan atau sampai kredit Anda habis.
> Untuk informasi selengkapnya, lihat Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025.

6. Di bawah Pasangan kunci (login), untuk nama pasangan Kunci, simpan Jangan sertakan dalam template peluncuran yang dipilih, atau pilih key pair yang ada, atau buat yang baru.

7. Di bawah Pengaturan jaringan, Anda dapat memilih Jangan sertakan dalam template peluncuran, atau Anda dapat menentukan nilai untuk berbagai pengaturan jaringan.
8. Di bawah Konfigurasi penyimpanan, jika Anda menentukan AMI dalam template peluncuran, AMI menyertakan satu atau lebih volume penyimpanan, termasuk volume root (Volume 1 (AMI Root). Anda dapat secara opsional menentukan volume tambahan untuk dilampirkan ke instance. Untuk menambahkan volume baru, pilih Tambahkan volume baru.
9. Di bawah Tag sumber daya, untuk menandai sumber daya yang dibuat saat instance diluncurkan, pilih Tambah tag, lalu masukkan kunci tag dan pasangan nilai. Untuk Tipe sumber daya, tentukan sumber daya yang akan ditandai pada pembuatan. Anda dapat menentukan tanda yang sama untuk semua sumber daya, atau menentukan tanda yang berbeda untuk sumber daya yang berbeda. Pilih Tambah tanda lagi untuk setiap tanda tambahan yang akan ditambahkan.

   Anda dapat menentukan tanda untuk sumber daya berikut yang dibuat saat templat peluncuran digunakan:

   - Instans
   - Volume
   - Grafik Elastic
   - Permintaan Instans Spot
   - Antarmuka jaringan

   > **Note**
   >
   > Untuk menandai templat peluncuran itu sendiri, Anda harus menentukan tag pada Tanda templat. Untuk informasi lebih lanjut, lihat Langkah 3 dalam prosedur ini.

10. Untuk detail lanjutan, perluas bagian untuk melihat bidang dan secara opsional tentukan parameter tambahan apa pun untuk instance Anda.
11. Gunakan panel Summary untuk meninjau konfigurasi template peluncuran Anda. Anda dapat menavigasi ke bagian mana pun dengan memilih tautannya dan kemudian membuat perubahan yang diperlukan.
12. Ketika Anda siap untuk membuat templat peluncuran Anda, pilih Buat templat peluncuran.

AWS CLI

Untuk membuat templat peluncuran

Gunakan perintah create-launch-template.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Berikut ini adalah contoh JSON yang menentukan data template peluncuran untuk konfigurasi instance. Simpan JSON ke file dan sertakan dalam `--launch-template-data` parameter seperti yang ditunjukkan pada perintah contoh.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

Berikut ini adalah output contoh.

```
{
```

```
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

PowerShell

Untuk membuat templat peluncuran

Gunakan New-EC2LaunchTemplatecmdlet.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-0abcdef1234567890'
    InstanceType = 'r5.4xlarge'
    NetworkInterfaces = @(

 [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-0abcdef1234567890'
        }
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
```

```
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' `
    -VersionDescription 'WebVersion1' `
    -LaunchTemplateData $launchTemplateData `
    -TagSpecification $tagSpecificationData
```

Berikut ini adalah output contoh.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Buat templat peluncuran dari templat peluncuran yang ada

Anda dapat mengklona templat peluncuran yang ada kemudian menyesuaikan parameter untuk membuat templat peluncuran baru. Namun, Anda hanya dapat melakukan ini saat menggunakan konsol Amazon EC2. AWS CLI Itu tidak mendukung kloning template. Untuk deskripsi setiap parameter, lihatReferensi untuk parameter konfigurasi EC2 instans Amazon.

Console

Untuk membuat templat peluncuran dari templat peluncuran yang ada

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Templat Peluncuran, lalu pilih Buat templat peluncuran.
3. Untuk Nama templat peluncuran, masukkan nama deskriptif untuk templat peluncuran.
4. Untuk Deskripsi versi templat, berikan deskripsi singkat tentang versi templat peluncuran ini.
5. Untuk menandai template peluncuran saat pembuatan, perluas tag Template, pilih Tambahkan tag baru, lalu masukkan kunci tag dan pasangan nilai.
6. Perluas Templat sumber, dan untuk Nama templat peluncuran, pilih templat peluncuran yang menjadi dasar templat peluncuran baru.

7. Untuk Versi templat sumber, pilih versi templat peluncuran yang menjadi dasar templat peluncuran baru.
8. Sesuaikan parameter peluncuran apa pun yang diperlukan, lalu pilih Buat templat peluncuran.

Buat templat peluncuran dari instans

Anda dapat mengkloning parameter instans Amazon EC2 yang ada dan kemudian menyesuaikan parameter untuk membuat template peluncuran. Untuk deskripsi setiap parameter, lihatReferensi untuk parameter konfigurasi EC2 instans Amazon.

Console

Untuk membuat templat peluncuran dari sebuah instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance, dan pilih Actions, Image and templates, Create template from instance.
4. Berikan nama, deskripsi, dan tanda, dan sesuaikan parameter peluncuran sesuai kebutuhan.

> **Note**
>
> Ketika Anda membuat template peluncuran dari sebuah instance, antarmuka jaringan instans IDs dan alamat IP tidak termasuk dalam template.

5. Pilih Buat templat peluncuran.

AWS CLI

Anda dapat menggunakan AWS CLI untuk membuat template peluncuran dari instance yang ada dengan terlebih dahulu mendapatkan data template peluncuran dari sebuah instance, dan kemudian membuat template peluncuran menggunakan data template peluncuran.

Untuk mendapatkan data templat peluncuran dari sebuah instans

- Gunakan perintah get-launch-template-data dan tentukan ID instans. Anda dapat menggunakan output sebagai basis untuk membuat templat peluncuran baru atau versi templat peluncuran. Secara default, output mencakup objek `LaunchTemplateData` tingkat

atas, yang tidak dapat ditentukan dalam data templat peluncuran Anda. Gunakan opsi `--query` untuk mengecualikan objek ini.

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

Berikut ini adalah contoh output.

```
    {
        "Monitoring": {},
        "ImageId": "ami-8c1be5f6",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "DeleteOnTermination": true
                }
            }
        ],
        "EbsOptimized": false,
        "Placement": {
            "Tenancy": "default",
            "GroupName": "",
            "AvailabilityZone": "us-east-1a"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "Description": "",
                "NetworkInterfaceId": "eni-35306abc",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateIpAddress": "10.0.0.72"
                    }
                ],
                "SubnetId": "subnet-7b16de0c",
                "Groups": [
                    "sg-7c227019"
                ],
                "Ipv6Addresses": [
```

```
                {
                    "Ipv6Address": "2001:db8:1234:1a00::123"
                }
            ],
            "PrivateIpAddress": "10.0.0.72"
        }
    ]
}
```

Anda dapat menulis output langsung ke file, misalnya:

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

Untuk membuat templat peluncuran menggunakan data templat peluncuran

- Gunakan create-launch-templateperintah untuk membuat template peluncuran menggunakan output dari prosedur sebelumnya. Untuk informasi selengkapnya tentang membuat template peluncuran menggunakan AWS CLI, lihatBuat template peluncuran dengan menentukan parameter.

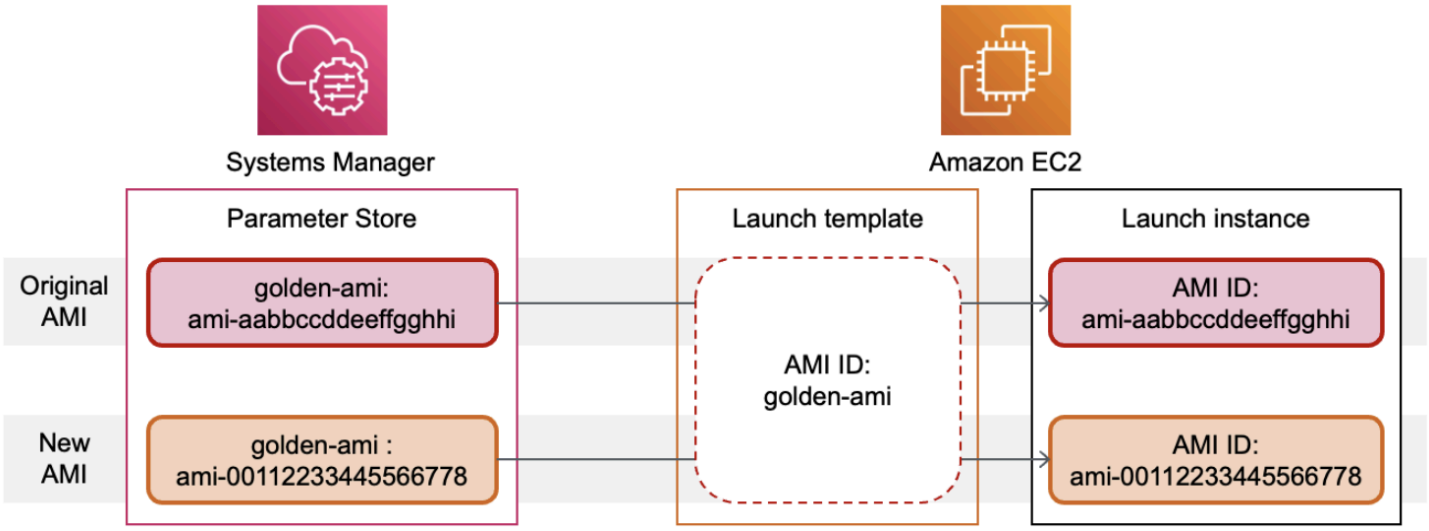
Gunakan parameter Systems Manager alih-alih ID AMI

Alih-alih menentukan ID AMI di templat peluncuran Anda, Anda dapat menentukan parameter AWS Systems Manager . Jika ID AMI berubah, Anda dapat memperbarui ID AMI di satu tempat dengan memperbarui parameter Systems Manager di Systems Manager Parameter Store. Parameter juga dapat dibagikan dengan yang lain Akun AWS. Anda dapat menyimpan dan mengelola parameter AMI secara terpusat dalam satu akun dan membagikannya dengan setiap akun lain yang perlu mereferensikannya. Dengan parameter Systems Manager, semua templat peluncuran Anda dapat diperbarui dalam satu tindakan.

Parameter Systems Manager adalah pasangan nilai kunci yang ditentukan pengguna yang Anda buat di Parameter Store.AWS Systems Manager Parameter Store menyediakan penyimpanan pusat untuk menyimpan nilai konfigurasi aplikasi Anda.

Dalam diagram berikut, parameter `golden-ami` terlebih dahulu dipetakan ke AMI asli `ami-aabbccddeeffgghhi` di Parameter Store. Dalam templat peluncuran, nilai untuk ID AMI adalah `golden-ami`. Saat instans diluncurkan menggunakan templat peluncuran ini, ID AMI akan

diselesaikan ke `ami-aabbccddeeffgghhi`. Kemudian, AMI diperbarui menghasilkan ID AMI baru. Di Parameter Store, parameter `golden-ami` dipetakan ke `ami-00112233445566778` yang baru. Templat peluncuran tetap tidak berubah. Saat instans diluncurkan menggunakan templat peluncuran ini, ID AMI akan diselesaikan ke `ami-00112233445566778` yang baru.



Format parameter Systems Manager untuk AMI IDs

Templat peluncuran mengharuskan parameter Systems Manager yang ditentukan pengguna mematuhi format berikut saat digunakan sebagai pengganti ID AMI:

- Tipe parameter: `String`
- Tipe data parameter: `aws:ec2:image` — Hal ini memastikan bahwa Parameter Store memvalidasi Anda memasukkan nilai dalam format yang tepat untuk ID AMI.

Untuk informasi selengkapnya tentang membuat parameter yang valid untuk ID AMI, lihat Membuat parameter Systems Manager di Panduan Pengguna AWS Systems Manager .

Format parameter Systems Manager dalam templat peluncuran

Untuk menggunakan parameter Systems Manager sebagai pengganti ID AMI dalam templat peluncuran, Anda harus menggunakan salah satu format berikut saat menentukan parameter dalam templat peluncuran:

Untuk mereferensikan parameter publik:

- `resolve:ssm:`*`public-parameter`*

Untuk mereferensikan parameter yang disimpan di akun yang sama:

- `resolve:ssm:parameter-name`
- `resolve:ssm:parameter-name:version-number` – Nomor versi itu sendiri adalah label default
- `resolve:ssm:parameter-name:label`

Untuk mereferensikan parameter yang dibagikan dari yang lain Akun AWS:

- `resolve:ssm:parameter-ARN`
- `resolve:ssm:parameter-ARN:version-number`
- `resolve:ssm:parameter-ARN:label`

Versi parameter

Parameter Systems Manager adalah sumber daya berversi. Saat Anda memperbarui parameter, Anda membuat versi parameter yang baru dan berurutan. Systems Manager mendukung label parameter yang dapat Anda petakan ke versi parameter tertentu.

Misalnya, parameter `golden-ami` dapat memiliki tiga versi:`1`, `2`, dan `3`. Anda dapat membuat label parameter `beta` yang memetakan ke versi `2`, dan label parameter `prod` yang memetakan ke versi `3`.

Dalam templat peluncuran, Anda dapat menentukan versi 3 parameter `golden-ami` dengan menggunakan salah satu format berikut:

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

Menentukan versi atau label bersifat opsional. Jika versi atau label tidak ditentukan, versi terbaru parameter yang digunakan.

Tentukan parameter Systems Manager di templat peluncuran

Anda dapat menentukan parameter Systems Manager di templat peluncuran, bukan ID AMI, saat Anda membuat templat peluncuran atau templat peluncuran versi baru.

Console

Untuk menentukan parameter Systems Manager dalam templat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Templat Peluncuran, lalu pilih Buat templat peluncuran.
3. Untuk Nama templat peluncuran, masukkan nama deskriptif untuk templat peluncuran.
4. Di bawah Gambar Aplikasi dan OS (Gambar Mesin Amazon), pilih Jelajahi lebih banyak AMIs.
5. Pilih tombol panah di sebelah kanan bilah pencarian, lalu pilih Tentukan berdasarkan nilai kustom/parameter Systems Manager.
6. Di kotak dialog Tentukan nilai kustom atau parameter Systems Manager, lakukan hal berikut:

   a. Untuk String parameter ID AMI atau Systems Manager, masukkan nama parameter Systems Manager menggunakan salah satu format berikut:

      Untuk mereferensikan parameter publik:

      - **resolve:ssm:*public-parameter***

      Untuk mereferensikan parameter yang disimpan di akun yang sama:

      - **resolve:ssm:*parameter-name***
      - **resolve:ssm:*parameter-name*:*version-number***
      - **resolve:ssm:*parameter-name*:*label***

      Untuk mereferensikan parameter yang dibagikan dari yang lain Akun AWS:

      - **resolve:ssm:*parameter-ARN***
      - **resolve:ssm:*parameter-ARN*:*version-number***
      - **resolve:ssm:*parameter-ARN*:*label***

   b. Pilih Simpan.
7. Tentukan parameter templat peluncuran lainnya sesuai kebutuhan, lalu pilih Buat templat peluncuran.

Untuk informasi selengkapnya, lihat Buat template peluncuran dengan menentukan parameter.

AWS CLI

Untuk menentukan parameter Systems Manager dalam templat peluncuran

- Gunakan create-launch-templateperintah untuk membuat template peluncuran. Untuk menentukan AMI yang akan digunakan, masukkan nama parameter Systems Manager yang menggunakan salah satu format berikut:

  Untuk mereferensikan parameter publik:

  - **resolve:ssm:*public-parameter***

  Untuk mereferensikan parameter yang disimpan di akun yang sama:

  - **resolve:ssm:*parameter-name***
  - **resolve:ssm:*parameter-name*:*version-number***
  - **resolve:ssm:*parameter-name*:*label***

  Untuk mereferensikan parameter yang dibagikan dari yang lain Akun AWS:

  - **resolve:ssm:*parameter-ARN***
  - **resolve:ssm:*parameter-ARN*:*version-number***
  - **resolve:ssm:*parameter-ARN*:*label***

  Contoh berikut membuat templat peluncuran yang menetapkan hal berikut:

  - Nama untuk templat peluncuran (*TemplateForWebServer*)
  - Nama untuk templat peluncuran (*purpose*=*production*)
  - Data untuk konfigurasi instans, yang ditentukan dalam file JSON:
    - AMI yang digunakan (`resolve:ssm:`*golden-ami*)
    - Tipe instans yang akan diluncurkan (*m5.4xlarge*)
    - Tanda untuk instans (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
```

```
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Berikut ini adalah contoh file JSON yang berisi data templat peluncuran untuk konfigurasi instans. Nilai untuk `ImageId` adalah nama parameter Systems Manager, yang dimasukkan dalam format `resolve:ssm:golden-ami` yang diperlukan.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Verifikasi bahwa template peluncuran mendapatkan ID AMI yang benar

Untuk menyelesaikan parameter Systems Manager ke ID AMI yang sebenarnya

Gunakan describe-launch-template-versionsperintah dan sertakan `--resolve-alias` parameternya.

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
    --resolve-alias
```

Tanggapan tersebut mencakup ID AMI untuk`ImageId`. Dalam contoh ini, ketika sebuah instance diluncurkan menggunakan template peluncuran ini, ID AMI akan menyelesaikannya. `ami-0ac394d6a3example`

```
{
    "LaunchTemplateVersions": [
        {
```

```
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Sumber daya terkait

Untuk informasi selengkapnya tentang bekerja dengan parameter Systems Manager, lihat materi referensi berikut dalam dokumentasi Systems Manager.

- Untuk informasi tentang cara mencari parameter publik AMI yang didukung oleh Amazon EC2, lihat Memanggil parameter publik AMI.
- Untuk informasi tentang berbagi parameter dengan AWS akun lain atau melalui AWS Organizations, lihat Bekerja dengan parameter bersama.
- Untuk informasi tentang pemantauan apakah parameter berhasil dibuat, lihat Dukungan parameter asli untuk Amazon Machine Image IDs.

Batasan

- Hanya Armada EC2 tipe yang `instant` mendukung menggunakan template peluncuran yang memiliki parameter Systems Manager yang ditentukan sebagai pengganti ID AMI.
- Armada EC2 jenis `maintain` dan`request`, dan Armada Spot tidak mendukung penggunaan template peluncuran yang memiliki parameter Systems Manager yang ditentukan sebagai pengganti ID AMI. Untuk jenis Armada EC2 `maintain` dan`request`, dan untuk Armada Spot, jika Anda menentukan AMI di template peluncuran, Anda harus menentukan ID AMI.
- Jika Anda menggunakan pemilihan instans berbasis atribut di Armada EC2, Anda tidak dapat menentukan parameter Systems Manager sebagai pengganti ID AMI. Saat menggunakan pemilihan instans berbasis atribut, Anda harus menentukan ID AMI.

- Amazon EC2 Auto Scaling memberikan batasan lain. Untuk informasi selengkapnya, lihat Menggunakan AWS Systems Manager parameter alih-alih AMI IDs dalam templat peluncuran di Panduan Pengguna Penskalaan Otomatis Amazon EC2.

Modifikasi templat peluncuran (mengelola versi templat peluncuran)

Template peluncuran tidak dapat diubah; setelah Anda membuat templat peluncuran, Anda tidak dapat memodifikasinya. Sebagai gantinya, Anda dapat membuat templat peluncuran versi baru yang menyertakan perubahan apa pun yang Anda butuhkan.

Anda dapat membuat versi template peluncuran yang berbeda, mengatur versi default, menjelaskan versi template peluncuran, dan menghapus versi yang tidak lagi Anda perlukan.

Tugas

- Buat versi templat peluncuran
- Menyetel versi templat peluncuran default
- Jelaskan versi templat peluncuran

Buat versi templat peluncuran

Saat Anda membuat versi templat peluncuran, Anda dapat menentukan parameter peluncuran baru atau menggunakan versi yang sudah ada sebagai dasar untuk versi baru. Untuk deskripsi setiap parameter, lihatReferensi untuk parameter konfigurasi EC2 instans Amazon.

Console

Untuk membuat versi templat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Templat Peluncuran.
3. Pilih templat peluncuran, lalu pilih Tindakan, Ubah templat (Buat versi baru).
4. Untuk Deskripsi versi templat, masukkan deskripsi untuk versi templat peluncuran ini.
5. (Opsional) Perluas Templat sumber dan pilih versi templat peluncuran yang akan digunakan sebagai dasar untuk versi templat peluncuran baru. Versi templat peluncuran baru mewarisi parameter peluncuran dari versi templat peluncuran ini.
6. Ubah parameter peluncuran sesuai kebutuhan.

7. Pilih Buat templat peluncuran.

AWS CLI

Untuk membuat versi templat peluncuran

Gunakan perintah create-launch-template-version. Anda dapat menentukan versi sumber yang menjadi dasar versi baru. Versi baru mewarisi parameter peluncuran dari versi ini, dan Anda dapat mengganti parameter menggunakan `--launch-template-data`. Contoh berikut membuat versi baru berdasarkan templat peluncuran versi 1 dan menentukan ID AMI yang berbeda.

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-0abcdef1234567890"
```

PowerShell

Untuk membuat versi templat peluncuran

Gunakan New-EC2LaunchTemplateVersionCmdlet. Anda dapat menentukan versi sumber yang menjadi dasar versi baru. Versi baru mewarisi parameter peluncuran dari versi ini, dan Anda dapat mengganti parameter menggunakan `LaunchTemplateData`. Contoh berikut membuat versi baru berdasarkan templat peluncuran versi 1 dan menentukan ID AMI yang berbeda.

```
New-EC2LaunchTemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -VersionDescription WebVersion2 `
    -SourceVersion 1 `
    -LaunchTemplateData (
        New-Object `
            -TypeName Amazon.EC2.Model.RequestLaunchTemplateData `
            -Property @{ImageId = 'ami-0abcdef1234567890'}
    )
```

Menyetel versi templat peluncuran default

Anda dapat mengatur versi default untuk templat peluncuran. Saat Anda meluncurkan sebuah instans dari templat peluncuran dan tidak menentukan versinya, instans tersebut diluncurkan menggunakan parameter versi default.

Console

Untuk mengatur versi templat peluncuran default

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Templat Peluncuran.
3. Pilih templat peluncuran dan pilih Tindakan, Setel versi default.
4. Untuk Versi templat, pilih nomor versi yang akan ditetapkan sebagai versi default dan pilih Setel sebagai versi default.

AWS CLI

Untuk mengatur versi templat peluncuran default

Gunakan perintah modify-launch-template.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

PowerShell

Untuk mengatur versi templat peluncuran default

Gunakan Edit-EC2LaunchTemplatecmdlet.

```
Edit-EC2LaunchTemplate `
    -LaunchTemplateId lt-0abcd290751193123 `
    -DefaultVersion 2
```

Jelaskan versi templat peluncuran

Dengan menggunakan konsol, Anda dapat melihat semua versi templat peluncuran yang dipilih, atau mendapatkan daftar templat peluncuran yang versi terbaru atau default-nya cocok dengan

nomor versi tertentu. Dengan menggunakan AWS CLI, Anda dapat menjelaskan semua versi, versi individual, atau rentang versi templat peluncuran yang ditentukan. Anda juga dapat mendeskripsikan semua versi terbaru atau semua versi default dari semua templat peluncuran di akun Anda.

Console

Untuk menjelaskan versi templat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Templat Peluncuran.
3. Anda dapat melihat versi templat peluncuran tertentu, atau mendapatkan daftar templat peluncuran yang versi terbaru atau versi default-nya cocok dengan nomor versi tertentu.
   - Untuk melihat versi templat peluncuran: Pilih templat peluncuran. Pada tab Versi, dari Versi, pilih versi untuk melihat detailnya.
   - Untuk mendapatkan daftar semua templat peluncuran yang versi terbarunya cocok dengan nomor versi tertentu: Dari bilah pencarian, pilih Versi terbaru, lalu pilih nomor versi.
   - Untuk mendapatkan daftar semua templat peluncuran yang versi default-nya cocok dengan nomor versi tertentu: Dari bilah pencarian, pilih Versi default, lalu pilih nomor versi.

AWS CLI

Untuk menjelaskan versi templat peluncuran

Gunakan describe-launch-template-versionsperintah dan tentukan nomor versi. Dalam contoh berikut, versi *1* dan *3* ditentukan.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

Untuk menjelaskan versi template peluncuran terbaru dan default di akun Anda

Gunakan describe-launch-template-versionsperintah dan tentukan`$Latest`,`$Default`, atau keduanya. Anda harus menghilangkan ID dan nama templat peluncuran dalam panggilan. Anda tidak dapat menentukan nomor versi.

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

PowerShell

Untuk menjelaskan versi templat peluncuran

Gunakan Get-EC2TemplateVersionCmdlet dan tentukan nomor versi. Dalam contoh berikut, versi *1* dan *3* ditentukan.

```
Get-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1,3
```

Untuk menjelaskan versi template peluncuran terbaru dan default di akun Anda

Gunakan Get-EC2TemplateVersionCmdlet dan tentukan`$Latest`,`$Default`, atau keduanya. Anda harus menghilangkan ID dan nama templat peluncuran dalam panggilan. Anda tidak dapat menentukan nomor versi.

```
Get-EC2TemplateVersion `
    -Version '$Latest','$Default'
```

Menghapus template peluncuran atau versi template peluncuran

Jika Anda tidak lagi memerlukan templat peluncuran, Anda dapat menghapusnya. Menghapus templat peluncuran akan menghapus semua versinya. Jika Anda hanya ingin menghapus versi tertentu dari template peluncuran, Anda dapat melakukannya sambil mempertahankan versi lain dari template peluncuran.

Menghapus template peluncuran atau versi template peluncuran tidak memengaruhi instance apa pun yang telah Anda luncurkan dari template peluncuran.

Hapus template peluncuran dan semua versinya

Jika Anda tidak lagi memerlukan template peluncuran, termasuk semua versinya, Anda dapat menghapus template peluncuran. Menghapus templat peluncuran akan menghapus semua versinya.

Console

Untuk menghapus template peluncuran dan semua versinya

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Templat Peluncuran.
3. Pilih templat peluncuran dan pilih Tindakan, Hapus templat.
4. Masukkan **`Delete`** untuk mengonfirmasi penghapusan, lalu pilih Hapus.

AWS CLI

Untuk menghapus template peluncuran dan semua versinya

Gunakan delete-launch-templateperintah dan tentukan template peluncuran.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

PowerShell

Untuk menghapus template peluncuran dan semua versinya

Gunakan perintah Remove-EC2LaunchTemplate(AWS Tools for PowerShell) dan tentukan template peluncuran. Jika `-Force` dihilangkan, minta PowerShell konfirmasi.

```
Remove-EC2LaunchTemplate -LaunchTemplateId lt-0123456789example -Force
```

Hapus versi templat peluncuran

Jika Anda tidak lagi memerlukan versi templat peluncuran, Anda dapat menghapusnya.

Pertimbangan-pertimbangan

- Anda tidak dapat mengganti nomor versi setelah Anda menghapusnya.
- Anda tidak dapat menghapus template peluncuran versi default; Anda harus terlebih dahulu menetapkan versi yang berbeda sebagai default. Jika versi default adalah satu-satunya versi untuk templat peluncuran, Anda harus menghapus seluruh templat peluncuran.
- Saat menggunakan konsol, Anda dapat menghapus satu versi templat peluncuran pada satu waktu. Saat menggunakan AWS CLI, Anda dapat menghapus hingga 200 versi template

peluncuran dalam satu permintaan. Untuk menghapus lebih dari 200 versi dalam satu permintaan, Anda dapat menghapus templat peluncuran, yang juga menghapus semua versinya.

Console

Untuk menghapus versi templat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Templat Peluncuran.
3. Pilih templat peluncuran dan pilih Tindakan, Hapus versi templat.
4. Pilih versi yang akan dihapus lalu pilih Hapus.

AWS CLI

Untuk menghapus versi templat peluncuran

Gunakan delete-launch-template-versionsperintah dan tentukan nomor versi yang akan dihapus. Anda dapat menentukan hingga 200 versi templat peluncuran yang akan dihapus dalam satu permintaan.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

PowerShell

Untuk menghapus versi templat peluncuran

Gunakan Remove-EC2TemplateVersioncmdlet dan tentukan nomor versi yang akan dihapus. Anda dapat menentukan hingga 200 versi templat peluncuran yang akan dihapus dalam satu permintaan.

```
Remove-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1
```

Luncurkan instans Amazon EC2

Instance adalah server virtual di AWS Cloud. Anda meluncurkan instans dari Amazon Machine Image (AMI). AMI menyediakan sistem operasi, server aplikasi, dan aplikasi untuk instans Anda.

Saat Anda membuat Akun AWS, Anda dapat memulai dengan Amazon EC2 secara gratis menggunakan. AWS Tingkat Gratis Manfaat Tingkat Gratis Anda bergantung pada saat Anda membuat Akun AWS. Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan usianya kurang dari 12 bulan, Anda dapat menggunakan Tingkat Gratis untuk meluncurkan dan menggunakan `t2.micro` instance secara gratis (di Wilayah yang tidak `t2.micro` tersedia, Anda dapat menggunakan `t3.micro` instance di bawah Tingkat Gratis).Anda dikenakan biaya untuk instans atau penggunaan yang diperhitungkan terhadap batas Tingkat Gratis Anda saat instans berjalan, meskipun instans tetap menganggur. Untuk informasi selengkapnya, lihat Harga Amazon EC2. Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, Anda dapat menggunakan`t3.micro`,,`t3.small`,`t4g.micro`,`t4g.small`,`c7i-flex.large`, dan jenis `m7i-flex.large` instans selama 6 bulan atau hingga kredit Anda habis. Untuk informasi selengkapnya, lihat Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025.

Saat Anda meluncurkan instans, Anda dapat meluncurkan instans di subnet yang terkait dengan salah satu sumber daya berikut:

- Availability Zone — Opsi ini adalah default.
- Zona Lokal — Untuk meluncurkan instance di Zona Lokal, Anda harus ikut serta ke Zona Lokal, lalu buat subnet di zona tersebut. Untuk informasi selengkapnya, lihat Memulai Local Zones.
- Zona Wavelength — Untuk meluncurkan instance di Wavelength Zone, Anda harus memilih masuk ke Wavelength Zone, lalu membuat subnet di zona tersebut. Untuk informasi tentang cara meluncurkan instance di Wavelength Zone, lihat Memulai. AWS Wavelength
- Pos Luar — Untuk meluncurkan instance di Outpost, Anda harus membuat Outpost. Untuk informasi tentang cara membuat Outpost, lihat Memulai AWS Outposts.

Setelah meluncurkan instans, Anda dapat terhubung ke instans tersebut dan menggunakannya. Untuk memulai, status instans adalah `pending`. Ketika status instans adalah `running`, instans telah mulai boot. Mungkin ada waktu singkat sebelum Anda dapat terhubung ke instans. Perhatikan bahwa tipe instans bare metal mungkin membutuhkan waktu lebih lama untuk diluncurkan.

Bergantung pada bagaimana Anda berencana untuk terhubung ke instans Anda, Anda mungkin ingin membuat konfigurasi tertentu saat meluncurkan instance Anda. Konfigurasi ini dapat mencakup

menentukan aturan grup keamanan masuk untuk lalu lintas tertentu atau mengaitkan peran profil instance. Untuk informasi selengkapnya tentang metode koneksi yang dapat Anda gunakan untuk menghubungkan dan persyaratannya, lihatConnect ke instans EC2.

Instans menerima nama DNS publik yang dapat Anda gunakan untuk menghubungi instans dari internet. Instans juga menerima nama DNS privat yang dapat digunakan oleh instans lain dalam VPC yang sama untuk menghubungi instans.

Setelah Anda selesai dengan sebuah instance, untuk menghindari biaya yang tidak perlu, pastikan untuk menghentikannya. Untuk informasi selengkapnya, lihat Mengakhiri instans Amazon EC2.

Jika Anda perlu meluncurkan sejumlah besar instans, menggunakan beberapa jenis instans, atau menggunakan beberapa opsi pembelian seperti Instans Sesuai Permintaan, Instans Cadangan, dan Instans Spot, pertimbangkan untuk menggunakan Armada EC2. Untuk informasi selengkapnya, lihat Armada EC2 dan Armada Spot.

Jika Anda ingin mengotomatiskan siklus hidup instans Anda, termasuk penskalaan otomatis, pemeriksaan kesehatan, dan penggantian instans yang tidak sehat, pertimbangkan untuk menggunakan Amazon EC2 Auto Scaling.

Metode berikut adalah beberapa cara Anda dapat meluncurkan sebuah instance.

Metode	Alat	Dokumentasi
Gunakan wizard instance peluncuran untuk menentukan parameter peluncuran.	Konsol Amazon EC2	Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol
Buat template peluncuran dan luncurkan instance dari template peluncuran.	Konsol Amazon EC2	Luncurkan instans EC2 menggunakan template peluncuran
Gunakan contoh yang ada sebagai basis.	Konsol Amazon EC2	Luncurkan instans EC2 menggunakan detail dari instans yang ada
Gunakan AMI yang Anda beli dari AWS Marketplace.	Konsol Amazon EC2	Luncurkan instans Amazon EC2 dari AMI AWS Marketplace

Metode	Alat	Dokumentasi
Gunakan AMI yang Anda tentukan.	AWS CLI	Meluncurkan, mencantumkan, dan menghapus instans Amazon EC2 di AWS CLI
Gunakan AMI yang Anda tentukan.	AWS Tools for Windows PowerShell	Luncurkan Instans Amazon EC2 Menggunakan Windows PowerShell
Gunakan Armada EC2 untuk menyediakan kapasitas di berbagai jenis instans EC2 dan Availability Zone, dan di seluruh opsi pembelian Instans Sesuai Permintaan, Instans Cadangan, dan Instans Spot.	AWS CLI	Armada EC2 dan Armada Spot
Gunakan CloudFormation template untuk menentukan instance.	AWS CloudFormation	AWS::EC2::Instance di Panduan Pengguna AWS CloudFormation
Gunakan AWS SDK khusus bahasa untuk meluncurkan instance.	AWS SDK	AWS SDK for .NET AWS SDK for C++ AWS SDK for Go AWS SDK for Java AWS SDK untuk JavaScript AWS SDK for PHP V3 AWS SDK untuk Python AWS SDK for Ruby V3

Tutorial untuk meluncurkan instans EC2

Ada berbagai cara untuk meluncurkan dan mengonfigurasi instans Amazon EC2. Metode dan konfigurasi yang Anda gunakan tergantung pada kasus penggunaan spesifik Anda.

Tutorial berikut dapat membantu Anda mempelajari cara meluncurkan instans EC2. Jika Anda baru mengenal Amazon EC2, kami sarankan Anda memulai dengan tutorial pertama. Tutorial dimulai dengan memperkenalkan Anda pada dasar-dasar, dan membantu Anda membangun dasar-dasar dengan memperkenalkan lebih banyak opsi konfigurasi.

Tujuan	Tautan ke tutorial
Luncurkan instans EC2 pertama saya Pelajari cara meluncurkan instans Amazon EC2 dengan cepat menggunakan pengaturan default di wizard instans peluncuran Amazon EC2. Pelajari juga cara meninjau bidang konfigurasi instance dan menghentikan instance. Durasi: 10 menit	Tutorial 1: Luncurkan instans Amazon EC2 pertama saya
Luncurkan instance EC2 pengujian dan sambungkan ke sana Pelajari cara meluncurkan instans Amazon EC2 yang dapat Anda gunakan untuk tujuan pengujian. Instance ini tidak akan memiliki konfigurasi lanjutan dan tidak akan menyimpan informasi sensitif. Anda juga akan belajar tentang pengaturan konfigurasi instans penting, cara menghubungkan ke instance, dan cara menghentikannya. Durasi: 30 menit	Tutorial 2: Luncurkan instance EC2 uji dan sambungkan ke sana

Mencari tutorial lainnya?

- Tutorial: Instal server LAMP di AL2023
- Tutorial: Konfigurasikan SSL/TLS pada AL2023
- Tutorial: Tuan rumah WordPress blog di AL2023
- Tutorial: Selesaikan konfigurasi yang diperlukan untuk terhubung ke instans Anda menggunakan EC2 Instance Connect
- Tutorial: Hubungkan instans Amazon EC2 ke basis data Amazon RDS

Tutorial 1: Luncurkan instans Amazon EC2 pertama saya

Tujuan tutorial	Pelajari cara meluncurkan instans Amazon EC2 dengan cepat menggunakan pengaturan default di wizard instans peluncuran Amazon EC2. Pelajari juga cara meninjau bidang konfigurasi instance dan menghentikan instance.
Pengalaman EC2	Pemula
Durasi	10 menit
Biaya	Tingkat Gratis memenuhi syarat Saat Anda membuat Akun AWS, Anda dapat memulai dengan Amazon EC2 secara gratis menggunakan. AWS Tingkat Gratis Jika Anda membuat Akun AWS sebelum 15 Juli 2025, usianya kurang dari 12 bulan, dan Anda belum melampaui manfaat Tingkat Gratis untuk Amazon EC2, Anda tidak akan dikenakan biaya apa pun untuk menyelesaikan tutorial ini, karena kami membantu Anda memilih opsi yang ada dalam manfaat Tingkat Gratis. Jika tidak, Anda akan dikenakan biaya penggunaan Amazon EC2 standar sejak Anda meluncurkan

	instans (meskipun instans tetap menganggur) hingga Anda menghentikannya. Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, usianya kurang dari 6 bulan, dan Anda belum menghabiskan semua kredit Anda, tidak akan dikenakan biaya apa pun untuk menyelesaikan tutorial ini, karena kami membantu Anda memilih opsi yang ada dalam manfaat Tingkat Gratis. Untuk informasi tentang cara menentuka n apakah Anda memenuhi syarat untuk Tingkat Gratis, lihatthe section called “Melacak penggunaan Tingkat Gratis Anda”.
Prasyarat	• Anda harus memiliki AWS akun, mengkonfi gurasi pengguna dengan akses administr ator, dan menggunakan pengguna administr ator untuk masuk ke Konsol Manajemen AWS. Tidak yakin bagaimana melakukan ini? Coba tutorial ini: Menyiapkan AWS Lingkungan Anda • Anda harus memiliki keakraban umum dengan AWS konsol. Tidak yakin harus mulai dari mana? Coba panduan memulai ini: Memulai dengan Konsol Manajemen AWS

Gambaran umum tutorial

Tutorial ini dirancang untuk pemula tanpa pengalaman sebelumnya menggunakan Amazon EC2. Kami akan memandu Anda melalui langkah-langkah untuk membuat — kami menyebutnya peluncuran — instans EC2 pertama Anda menggunakan konsol EC2. Instance pada dasarnya adalah server web di AWS Cloud. Setelah meluncurkan instans Anda, kami akan menunjukkan cara menemukannya di konsol. Terakhir, untuk membantu Anda mengelola biaya, kami akan menunjukkan cara menghapus—kami menyebutnya terminate —instance Anda.

Tutorial ini dibagi menjadi tugas-tugas singkat berikut. Anda harus menyelesaikan setiap tugas sebelum pindah ke yang berikutnya.

- Tugas 1: Luncurkan instans Anda
- Tugas 2: Temukan instance Anda
- Tugas 3: Lihat konfigurasi instans Anda
- Tugas 4: Hentikan instans Anda

Tugas 1: Luncurkan instans Anda

Dalam tugas ini, Anda akan mengambil jalan tercepat untuk meluncurkan instance Anda dengan hanya melakukan hal-hal penting. Kami akan menggunakan wizard instans peluncuran EC2, formulir berbasis web yang menyediakan semua bidang untuk mengonfigurasi dan meluncurkan instance Anda. Ini menyederhanakan proses dengan memberikan nilai default untuk bidang konfigurasi instance.

Sebelum Anda mulai

Pastikan Anda telah menyelesaikan prasyarat yang tercantum dalam tabel sebelumnya, termasuk masuk ke dengan pengguna administrator Anda. Konsol Manajemen AWS

Ikuti langkah-langkah ini untuk meluncurkan instans Anda dengan cepat

1. Buka konsol Amazon EC2:

   Kunjungi https://console.aws.amazon.com/ec2/.
2. Buka wizard instans peluncuran EC2:

   Dari dasbor EC2, pilih Launch instance.

   Formulir berbasis web Launch an instance terbuka. Ini adalah wizard instans peluncuran EC2.
3. Beri nama instance Anda:

   Di bawah Nama dan tag, untuk Nama, masukkan nama deskriptif seperti**`My first EC2 instance`**.

   Meskipun penamaan instance Anda tidak diperlukan, ini membantu mengidentifikasi instance Anda nanti.
4. Lanjutkan tanpa key pair:

Di bawah Key pair (login), untuk nama Key pair, pilih Proceed without a key pair (Tidak disarankan).

Sebuah key pair dapat digunakan untuk login aman. Namun, karena kita tidak akan masuk ke instance dalam tutorial ini, Anda tidak memerlukan key pair untuk saat ini.

5. Luncurkan instance Anda:

   Di panel Ringkasan di sebelah kanan, pilih Luncurkan instans.

   Amazon EC2 dengan cepat meluncurkan instans Anda menggunakan pengaturan default. Spanduk Sukses mengkonfirmasi peluncuran.

Selamat!Anda telah berhasil meluncurkan instans EC2 pertama Anda!

Tugas 2: Temukan instance Anda

Dalam tugas ini, Anda akan menemukan instance yang baru saja Anda luncurkan di konsol EC2.

Ikuti langkah-langkah berikut untuk menemukan instans Anda di konsol EC2

1. Buka halaman Instans:

   Jika Anda masih berada di halaman sukses, pilih Instans di breadcrumb di bagian atas layar. Anda mungkin perlu memilih tiga elips terlebih dahulu untuk mengaksesnya.

   Jika Anda telah menavigasi, pilih Instans dari panel navigasi.

2. Temukan instance Anda:

   Di kolom Nama, temukan contoh Anda dengan nama yang Anda berikan.

Tugas 3: Lihat konfigurasi instans Anda

Dalam tugas ini, Anda akan terbiasa melihat detail konfigurasi instans Anda.

Ikuti langkah-langkah ini untuk melihat konfigurasi instans Anda

1. Temukan ID instance:

   Di kolom ID Instance, catat ID unik instans Anda. Dimulai dengan i— diikuti oleh 17 karakter alfanumerik, misalnya, i-01aeed690c9fb5322.

ID instans secara otomatis ditetapkan ke instance Anda saat diluncurkan.

2. Buka halaman detail instance:

   Di kolom ID Instance, pilih tautan ID untuk membuka halaman detail instance tempat Anda dapat meninjau konfigurasinya.

3. Jelajahi detail konfigurasi instance:

   Luangkan beberapa menit untuk menjelajahi detail konfigurasi instans Anda. Dalam tutorial berikutnya, kita akan menyelam lebih dalam ke konfigurasi. Untuk saat ini, gunakan waktu ini untuk membiasakan diri dengan halaman detail instance.

   Tip: Untuk menemukan bidang dengan cepat, tekan Ctrl+F atau Command+F pada keyboard Anda.

   a. Jenis instans: Dapatkah Anda menemukan tipe instance? Mungkin t3.micro, misalnya.
   b. IPv4 Alamat publik: Dapatkah Anda menemukan IPv4 alamat publik yang dialokasikan untuk instans Anda? Ini dalam format yang mirip dengan contoh berikut: 34.242.148.128.
   c. Pemilik instans: Dapatkah Anda mengidentifikasi pemilik instance ini? Ini kau! Akun AWS Nomor Anda tercantum di bawah bidang Pemilik.
   d. Instance tags: Nama yang Anda berikan instance Anda sebenarnya adalah sebuah tag. Bisakah Anda menemukan tag instance Anda? Pilih tab Tanda. Kuncinya adalah Nama, dan nilainya adalah nama yang Anda berikan.
   e. Waktu peluncuran: Dapatkah Anda menemukan ketika Anda meluncurkan instans Anda? Pilih tab Detail dan temukan bidang Waktu peluncuran.
   f. Status instans: Dapatkah Anda memverifikasi status instans Anda? Itu harus berjalan.

Luangkan beberapa menit lagi untuk menjelajahi bidang konfigurasi instance lainnya. Ketika Anda siap, lanjutkan ke tugas berikutnya.

Tugas 4: Hentikan instans Anda

> ⚠ Warning
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi

untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Dalam tugas ini, Anda akan menghapus instans Anda untuk mempertahankan manfaat Tingkat Gratis Anda. Di EC2, terminate adalah istilah yang digunakan untuk menghapus instance.

Ikuti langkah-langkah ini untuk menghentikan instans Anda

1. Memulai penghentian:

   Jika Anda masih berada di halaman detail instance, pilih menu status Instance (kanan atas), lalu pilih Terminate (delete) instance.

   Jika Anda telah menavigasi, pilih Instans dari panel navigasi. Kemudian, pada halaman Instances, pilih kotak centang di sebelah nama instance Anda, lalu pilih menu status Instance (kanan atas), dan pilih Terminate (delete) instance.
2. Konfirmasikan penghentian:

   Di jendela Instance Terminate (delete) yang terbuka, pilih tombol Terminate (delete) untuk mengonfirmasi bahwa Anda ingin menghentikan instance Anda.
3. Memantau status instance:

   Pada halaman Instances, periksa kolom Instance state. Status instans Anda berubah menjadi Shutting-down. Jika Anda tidak melihat teks lengkapnya, coba lebarkan kolom.

   Setelah instance dimatikan, Amazon EC2 menghapus instance, dan menghilang dari halaman Instans.

Takeaways kunci

Dalam tutorial ini, Anda membahas konsep-konsep kunci berikut:

- Instance mengacu pada server web Amazon EC2 di Cloud. AWS
- Peluncuran mengacu pada pembuatan instans EC2.
- Mengakhiri mengacu pada menghapus instans EC2.

- Wizard instans peluncuran EC2 berisi nilai default untuk konfigurasi instans, memungkinkan peluncuran instans yang cepat dan mudah.
- ID instans adalah pengidentifikasi unik yang secara otomatis ditetapkan ke instans Anda, sedangkan nama instance adalah tag opsional yang dapat Anda tetapkan untuk identifikasi yang lebih mudah.

Langkah selanjutnya

Untuk membangun kepercayaan diri dalam meluncurkan dan mengakhiri instance, pertimbangkan untuk mengulangi langkah-langkah dalam tutorial ini. Pastikan untuk menghentikan setiap instance yang Anda luncurkan untuk mempertahankan manfaat Tingkat Gratis Anda.

Setelah Anda merasa nyaman dengan dasar-dasar ini, lanjutkan ke tutorial berikutnya, yang menyediakan penyelaman lebih dalam ke bidang konfigurasi instance kunci.

Tutorial 2: Luncurkan instance EC2 uji dan sambungkan ke sana

Tujuan tutorial	Pelajari cara meluncurkan instans Amazon EC2 yang dapat Anda gunakan untuk tujuan pengujian. Instance ini tidak akan memiliki konfigurasi lanjutan dan tidak akan menyimpan informasi sensitif. Anda juga akan belajar tentang pengaturan konfigurasi instans penting, cara menghubungkan ke instance, dan cara menghentikannya.
Pengalaman EC2	Pemula
Durasi	30 menit
Biaya	Tingkat Gratis memenuhi syarat Saat Anda membuat Akun AWS, Anda dapat memulai dengan Amazon EC2 secara gratis menggunakan. AWS Tingkat Gratis Jika Anda membuat Akun AWS sebelum 15 Juli 2025, usianya kurang dari 12 bulan, dan

	Anda belum melampaui manfaat Tingkat Gratis untuk Amazon EC2, Anda tidak akan dikenakan biaya apa pun untuk menyelesaikan tutorial ini, karena kami membantu Anda memilih opsi yang ada dalam manfaat Tingkat Gratis. Jika tidak, Anda akan dikenakan biaya penggunaan Amazon EC2 standar sejak Anda meluncurkan instans (meskipun instans tetap menganggur) hingga Anda menghentikannya. Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, usianya kurang dari 6 bulan, dan Anda belum menghabiskan semua kredit Anda, tidak akan dikenakan biaya apa pun untuk menyelesaikan tutorial ini, karena kami membantu Anda memilih opsi yang ada dalam manfaat Tingkat Gratis. Untuk informasi tentang cara menentuka n apakah Anda memenuhi syarat untuk Tingkat Gratis, lihatthe section called “Melacak penggunaan Tingkat Gratis Anda”.
Prasyarat	Selesaikan Tutorial 1: Luncurkan instans Amazon EC2 pertama saya.

Gambaran umum tutorial

Tutorial ini dirancang untuk pemula yang ingin meluncurkan instans EC2 yang dapat mereka gunakan untuk tujuan pengujian.

Kami akan menjelaskan bidang konfigurasi instance kunci, dan kemudian memandu Anda melalui langkah-langkah untuk meluncurkan instance pengujian menggunakan nilai default di konsol EC2. Setelah meluncurkan instans Anda, kami akan menunjukkan cara masuk ke — kami menyebutnya terhubung ke —instance Anda. Kami juga akan menunjukkan cara membuat key pair, yang diperlukan untuk menghubungkan ke instance Anda dalam tutorial ini. Terakhir, untuk membantu mengelola biaya, kami akan menunjukkan kepada Anda untuk menghentikan instans Anda untuk menghindari biaya penggunaan.

Anda akan meluncurkan instance Linux dalam tutorial ini. Sementara langkah-langkah dalam tutorial ini dapat digunakan untuk meluncurkan instance dengan sistem operasi lain, instruksi untuk menghubungkan ke instance khusus untuk instance Linux.

Tutorial ini dibagi menjadi tugas-tugas singkat berikut. Anda harus menyelesaikan setiap tugas sebelum pindah ke yang berikutnya.

- Tugas 1: Biasakan diri Anda dengan komponen kunci untuk meluncurkan instance
- Tugas 2: Tinjau diagram teknis
- Tugas 3: Buat key pair
- Tugas 4: Luncurkan instance pengujian Anda
- Tugas 5: Temukan instance Anda
- Tugas 6: Lihat konfigurasi instans
- Tugas 7: Biasakan diri Anda dengan komponen kunci untuk menghubungkan ke sebuah instance
- Tugas 8: Connect ke instans Anda
- Tugas 9: Hentikan instans Anda

Tugas 1: Biasakan diri Anda dengan komponen kunci untuk meluncurkan instance

Dalam tugas ini, Anda akan menjelajahi komponen kunci yang diperlukan untuk meluncurkan instans EC2. Ini adalah AMI, tipe instance, key pair, grup keamanan, jaringan (VPC dan subnet), dan volume Amazon EBS. Anda juga akan menjelajahi komponen opsional, tag Nama.

Untuk membantu memvisualisasikan komponen-komponen ini, pikirkan contoh seperti rumah sewa. Sama seperti menyewa rumah memberi Anda tempat tinggal tanpa Anda harus memiliki dan memelihara properti, instans EC2 menyediakan daya komputasi tanpa Anda harus memiliki dan memelihara infrastruktur yang mendasarinya.

Saat memutuskan jenis instance yang akan diluncurkan, Anda akan mempertimbangkan kriteria konfigurasi untuk instance tersebut, sama seperti Anda akan mempertimbangkan kriteria yang Anda inginkan dari sebuah rumah. Meskipun analogi ini menyederhanakan banyak hal, ia menawarkan cara yang bermanfaat untuk memvisualisasikan komponen sampai Anda lebih akrab dengannya.

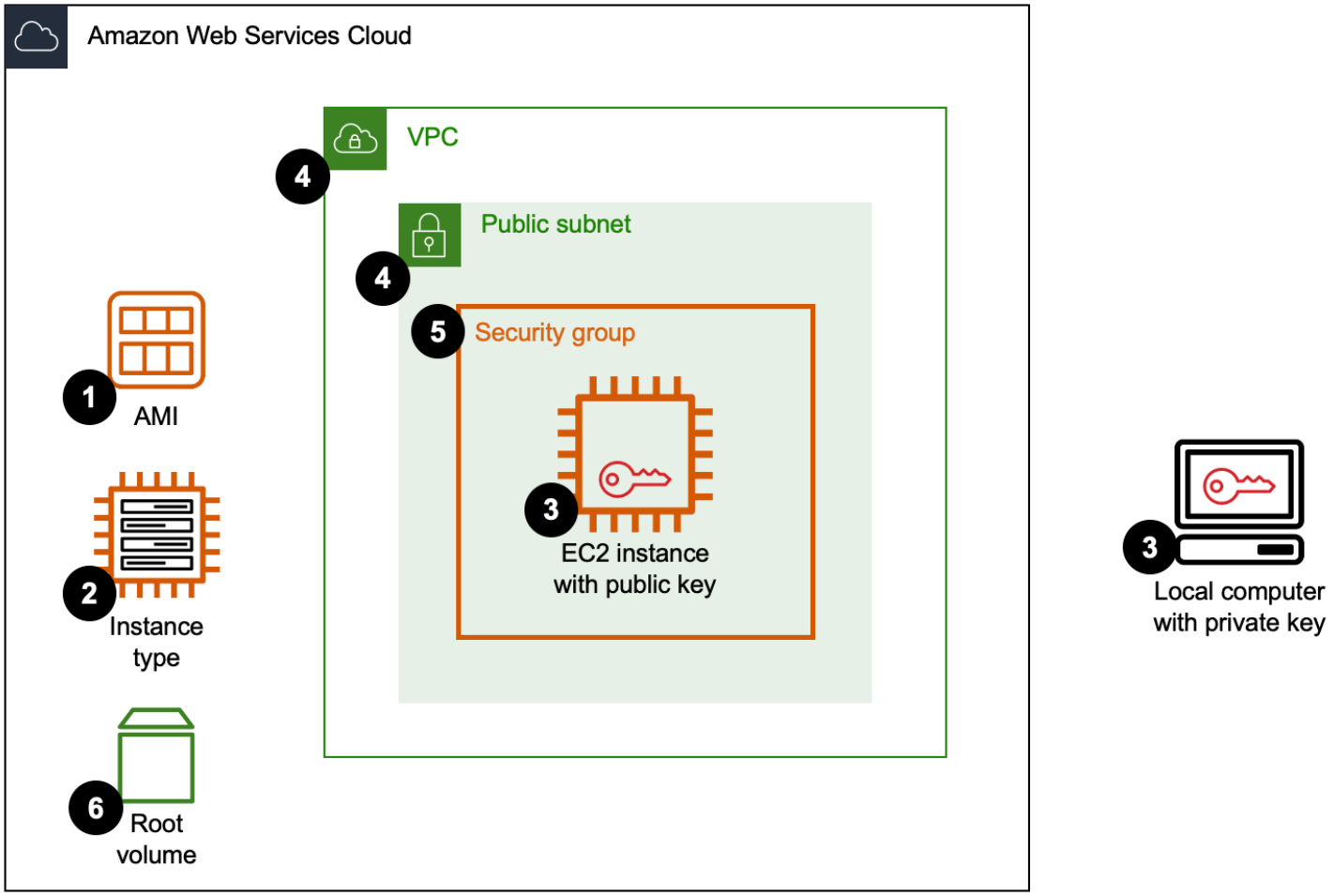
- AMI — Bahan dan fasilitas bangunan rumah: Amazon Machine Image (AMI) menentukan sistem operasi dan aplikasi yang dimulai dengan instans Anda. Ini seperti memilih bahan bangunan (seperti batu bata, baja, atau kayu) dan fasilitas (seperti peralatan dan perabotan) rumah Anda.

AMI dasar seperti rumah tanpa perabotan dengan peralatan dasar, sedangkan AMI khusus dengan perangkat lunak pra-instal seperti rumah berperabotan lengkap.

- Jenis instans — Ukuran dan daya rumah: Jenis instans menentukan ukuran dan kemampuan instans EC2 Anda, seperti memilih ukuran rumah, jumlah kamar, dan kapasitas energi. Setiap jenis instans menentukan jumlah CPU, memori, penyimpanan, dan kapasitas jaringan instans Anda. AMI yang dipilih mungkin membatasi jenis instans yang dapat Anda pilih.
- Pasangan kunci — Kunci pintu depan: Sebuah key pair seperti kunci dan kunci ke pintu depan rumah Anda. Kunci publik bertindak sebagai kunci pada instans Anda, sedangkan kunci pribadi adalah kunci yang harus Anda simpan dengan aman di komputer lokal Anda. Jika orang lain memegang kunci pribadi Anda, mereka dapat mengakses contoh Anda, seperti bagaimana seseorang dengan kunci pintu depan Anda dapat memasuki rumah Anda.
- Jaringan (VPC dan subnet) — Batas properti, area yang dipotong, dan nomor rumah: Virtual Private Cloud (VPC) Anda seperti seluruh properti tempat rumah Anda berada, dan subnet adalah area terpisah di sekitar rumah. Jika Anda memiliki beberapa rumah (contoh) di properti Anda, Anda mungkin ingin membaginya menjadi area yang berbeda (subnet yang berbeda) tergantung pada tujuannya. Beberapa rumah memungkinkan pengunjung untuk berkeliaran bebas melalui taman (subnet publik dengan akses internet), sementara yang lain memiliki taman berpagar untuk membatasi masuk (subnet pribadi tanpa akses internet). Setiap subnet berisi berbagai alamat IP, seperti nomor rumah, yang dapat ditetapkan ke instance dalam subnet.
- Kelompok keamanan — Penjaga gerbang: Kelompok keamanan bertindak seperti penjaga gerbang, mengendalikan siapa yang diizinkan mengunjungi rumah Anda. Ini memberlakukan seperangkat aturan yang mengontrol lalu lintas apa yang diizinkan untuk mencapai instans Anda. Misalnya, aturan yang memungkinkan lalu lintas SSH dari alamat IP tertentu seperti penjaga gerbang yang mengizinkan hanya orang tertentu untuk mengirimkan bahan makanan. Demikian pula, mengizinkan lalu lintas HTTPS dari mana saja seperti membiarkan publik datang dan melihat bagian luar rumah Anda.
- Volume Amazon EBS — Unit penyimpanan: Volume EBS seperti unit penyimpanan tempat Anda dapat menyimpan barang-barang Anda. Setiap instance memiliki volume root (tempat AMI disimpan), dan Anda dapat menambahkan lebih banyak volume (penyimpanan) kapan saja sesuai kebutuhan.
- Tag nama — Nama rumah: Tag nama berfungsi seperti tanda di rumah, membantu Anda dengan mudah mengidentifikasi siapa yang tinggal di sana. Meskipun tag Nama membuatnya lebih mudah untuk membedakan antara instance, itu tidak diperlukan saat meluncurkan instance.

Tugas 2: Tinjau diagram teknis

Dalam tugas ini, Anda akan terbiasa dengan diagram teknis khas yang kami gunakan dalam AWS dokumentasi. Diagram berikut mewakili konfigurasi untuk contoh pengujian yang akan Anda luncurkan dalam tutorial ini. Dalam tugas sebelumnya, kami memperkenalkan komponen-komponen ini menggunakan analogi rumah sewaan. Sekarang, kita akan fokus pada komponen EC2 yang sebenarnya itu sendiri. Label bernomor sesuai dengan deskripsi berikut.



1. AMI - AMI adalah gambar yang Anda pilih saat meluncurkan instance. Ini adalah template yang berisi sistem operasi dan perangkat lunak untuk dijalankan pada instance Anda. Misalnya, jika Anda ingin meluncurkan instance Linux, Anda dapat memilih Amazon Linux 2023 AMI. Atau, jika Anda ingin meluncurkan instance Windows, Anda dapat memilih Microsoft Windows Server 2022 Base AMI. Katalog AMI di konsol Amazon EC2 berisi ribuan gambar untuk dipilih.
2. Jenis instans — Jenis instans adalah perangkat keras yang menentukan CPU, memori, penyimpanan, dan kapasitas jaringan komputer host yang digunakan untuk instance Anda. Amazon EC2 menawarkan lebih dari 600 jenis instans untuk dipilih, masing-masing bervariasi

dalam konfigurasi dan ukuran perangkat keras, memungkinkan Anda memilih yang paling sesuai dengan kebutuhan aplikasi Anda.

3. Key pair - Sebuah key pair adalah kumpulan kredenal keamanan yang Anda gunakan untuk membuktikan identitas Anda saat menghubungkan ke instans Anda. Kunci publik ada di instans Anda dan kunci pribadi ada di komputer lokal Anda.

   Di EC2, menghubungkan ke instans Anda mengacu pada masuk ke instans Anda dari komputer lokal Anda. Meskipun ada cara lain untuk terhubung dengan aman ke instans Anda, dalam tutorial ini kita menggunakan key pair.

4. Jaringan — Jaringan terdiri dari VPC dan satu atau lebih subnet. VPC adalah jaringan virtual di dalam. AWS Cloud Setiap AWS pelanggan memiliki VPC mereka sendiri yang didedikasikan untuk mereka. Akun AWS Anda akan meluncurkan instance Anda ke subnet di VPC Anda. Subnet adalah berbagai alamat IP dalam VPC. Subnet default Anda adalah subnet publik, yang berarti akan menetapkan alamat IP publik dan memberikan akses internet ke instans Anda dari luar jaringan Amazon.
5. Grup keamanan — Grup keamanan bertindak sebagai firewall untuk mengontrol lalu lintas ke instans Anda. Grup keamanan berisi aturan yang memungkinkan jenis lalu lintas tertentu masuk ke instans Anda. Untuk terhubung melalui SSH dari komputer lokal Anda ke instans Anda (menggunakan key pair Anda), Anda memerlukan aturan yang memungkinkan lalu lintas SSH dari komputer lokal Anda.
6. Volume EBS - Volume Amazon EBS adalah perangkat penyimpanan yang berfungsi seperti hard drive fisik. Instans Anda dilengkapi dengan volume root, yang merupakan volume EBS khusus yang menyimpan AMI dengan sistem operasi dan perangkat lunak yang diperlukan untuk mem-boot instance Anda. Anda dapat menambahkan volume data secara opsional. Namun, karena instance pengujian Anda tidak akan menyimpan data sensitif apa pun, Anda tidak memerlukan volume data terenkripsi tambahan.

Selamat! Anda telah menyelesaikan tugas-tugas konseptual dalam tutorial ini. Dalam tugas berikut, Anda akan menggunakan konsol Amazon EC2 untuk membuat komponen yang telah Anda pelajari.

Tugas 3: Buat key pair

Dalam tugas ini, Anda akan membuat key pair. Sebuah key pair terdiri dari dua bagian: kunci publik, yang akan Anda tambahkan ke instance Anda, dan kunci pribadi yang cocok, yang akan Anda gunakan untuk terhubung dengan aman ke instance Anda. Pada tugas berikutnya, Anda akan memilih key pair ini saat meluncurkan instance Anda, yang secara otomatis menambahkan kunci

publik ke instance. Sangat penting untuk menyimpan kunci pribadi dengan aman di komputer lokal Anda, karena siapa pun yang memiliki akses ke sana dapat terhubung ke instans Anda.

Jika Anda lebih suka menggunakan key pair yang ada saat meluncurkan instance pengujian, silakan lewati tugas ini. Jika tidak, lanjutkan untuk membuat key pair baru.

Sebelum Anda mulai

Pastikan Anda telah menyelesaikan prasyarat yang tercantum dalam tabel sebelumnya, termasuk masuk ke dengan pengguna administrator Anda. Konsol Manajemen AWS

Ikuti langkah-langkah berikut untuk membuat key pair

1. Buka konsol Amazon EC2:

   Kunjungi https://console.aws.amazon.com/ec2/.
2. Arahkan ke halaman Konsol pasangan kunci:

   Pada panel navigasi, di Jaringan & Keamanan, pilih Pasangan Kunci.

   - Jika sebelumnya Anda membuat pasangan kunci, mereka muncul di tabel.
   - Jika tidak ada pasangan kunci, tabel kosong.
3. Buat key pair baru:

   Pilih tombol Create key pair (kanan atas) untuk membuka formulir berbasis web Create key pair, dan masukkan detail key pair Anda, sebagai berikut:

   a. Beri nama key pair Anda: Untuk Nama, masukkan nama yang akan membantu Anda mengenali key pair, seperti**`test-instance-key-pair`**.

      Namanya bisa mencapai 255 karakter ASCII. Tidak boleh mengandung spasi di depan maupun belakang.

   b. Pilih jenis key pair: Untuk tipe Key pair, pilih ED25519.

      Instans Linux mendukung RSA dan tipe ED25519 kunci, sedangkan instance Windows hanya mendukung RSA. Karena Anda akan meluncurkan instance Linux dalam tutorial ini, Anda dapat menggunakan ED25519 kunci.

   c. Pilih format file kunci pribadi: Untuk format file kunci pribadi, pilih.pem.

      Ini adalah format di mana file kunci pribadi Anda akan disimpan.

4. Simpan kunci publik ke Amazon EC2 dan unduh kunci pribadi:

   Pilih tombol Create key pair (kanan bawah).

   Amazon EC2 menyimpan kunci publik, sementara browser Anda mengunduh file kunci pribadi secara otomatis ke komputer lokal Anda. File ini dinamai sesuai dengan nama yang Anda tentukan untuk key pair, dan ekstensi adalah format file yang Anda pilih. Pindahkan file kunci pribadi ke lokasi yang aman di komputer Anda.

   > **Important**
   >
   > Ini adalah satu-satunya kesempatan Anda harus menyimpan file kunci pribadi.

5. Tetapkan izin pada kunci (untuk pengguna macOS dan Linux):

   Jika Anda berencana untuk terhubung ke instans menggunakan SSH di komputer macOS atau Linux, Anda harus mengatur izin yang benar untuk file kunci pribadi Anda. Buka jendela terminal dan jalankan perintah berikut, ganti *test-instance-key-pair* dengan nama key pair Anda:

   ```
   chmod 400 test-instance-key-pair.pem
   ```

   Perintah ini memastikan bahwa hanya Anda yang dapat membaca file kunci pribadi, yang diperlukan untuk membuat koneksi aman ke instance Anda. Tanpa izin ini, Anda tidak akan dapat terhubung menggunakan key pair ini.

Selamat! Anda telah berhasil membuat key pair!

Tugas 4: Luncurkan instance pengujian Anda

Dalam tugas ini, Anda akan segera meluncurkan instance pengujian menggunakan wizard instans peluncuran EC2. Anda akan mengkonfigurasi pengaturan konfigurasi instans utama untuk instance Linux dan menggunakan nilai default untuk bidang lainnya.

Untuk membantu Anda mengelola biaya, sebaiknya pilih komponen yang memenuhi syarat tingkat gratis.

Ikuti langkah-langkah ini untuk meluncurkan instance pengujian

1. Buka konsol Amazon EC2:

Kunjungi https://console.aws.amazon.com/ec2/.

2. Buka wizard instans peluncuran EC2:

   Dari dasbor EC2, pilih Launch instance.

   Formulir berbasis web Launch an instance terbuka. Ini adalah wizard instans peluncuran EC2.

3. Beri nama instance Anda:

   Di bawah Nama dan tag, untuk Nama, masukkan nama deskriptif seperti**`Test instance`**.

   Nama instans adalah tanda, di mana kuncinya adalah Name, dan nilainya adalah nama yang Anda tentukan.

   Tip: Untuk contoh pengujian, tag nama sudah cukup. Namun, untuk instans produksi, praktik terbaik adalah membuat kebijakan penandaan untuk menstandarisasi penandaan di semua sumber daya Anda.

4. Pilih sistem operasi dan perangkat lunak Anda—Amazon Machine Image (AMI):

   Di bawah Gambar Aplikasi dan OS (Gambar Mesin Amazon), untuk Amazon Machine Image (AMI), pilihan default adalah Amazon Linux 2023 AMI. AMI ini ditandai Tingkat gratis yang memenuhi syarat. Dalam tutorial ini, Anda akan meluncurkan instance Linux, jadi biarkan pengaturan default tetap di bawah batas Tingkat Gratis.

5. Pilih perangkat keras Anda—jenis instans:

   Di bawah tipe Instance, untuk tipe Instance, pertahankan pilihan default untuk tutorial ini. Jenis instans default dapat digunakan di bawah Tingkat Gratis dan perangkat kerasnya cocok untuk instance pengujian Anda.

6. Bersiaplah untuk login aman dengan key pair:

   Di bawah Key pair (login), untuk nama Key pair, pilih key pair yang Anda buat di tugas sebelumnya. Jika Anda tidak melihat key pair dalam daftar, pilih ikon refresh (di sebelah kanan daftar).

   Ketika instance Anda diluncurkan, itu akan menempatkan kunci publik pada instance. Untuk terhubung ke instans Anda setelah diluncurkan, Anda akan menggunakan kunci pribadi terkait yang Anda unduh di tugas sebelumnya.

7. Konfigurasikan pengaturan jaringan untuk mengaktifkan akses internet:

Di bawah Pengaturan jaringan, bidang Jaringan (VPC Anda) dan Subnet dikonfigurasi secara default. Pertahankan pengaturan default untuk tutorial ini untuk membantu Anda memulai dengan cepat. Jika Anda belum memodifikasi subnet default Anda, instans Anda akan memiliki akses internet.

Tip: Subnet default Anda adalah subnet publik, yang berarti akan menetapkan alamat IP publik dan memberikan akses internet ke instans Anda dari luar jaringan Amazon. Untuk contoh pengujian, tidak apa-apa untuk menggunakan pengaturan subnet default yang menyediakan akses internet. Namun, untuk instance produksi, praktik terbaik adalah hanya menetapkan alamat IP publik dan menggunakan subnet dengan akses internet bila benar-benar diperlukan.

8. Siapkan firewall instance (grup keamanan):

   Di bawah Pengaturan jaringan, di bawah Firewall (grup keamanan), simpan kotak centang Izinkan lalu lintas SSH dari mana saja (0.0.0.0) dipilih. Ini akan membuat grup keamanan baru untuk instance pengujian Anda yang memungkinkan lalu lintas SSH dari alamat IP apa pun.

   Grup keamanan bertindak sebagai firewall untuk mengontrol lalu lintas ke instans Anda. Untuk terhubung melalui SSH dari komputer lokal Anda ke instans Anda, Anda memerlukan aturan yang memungkinkan lalu lintas SSH dari komputer lokal Anda.

   Tip: Alamat IP komputer lokal Anda mungkin berubah seiring waktu jika penyedia layanan internet Anda menggunakan penetapan IP dinamis. Kami berasumsi bahwa ketika Anda menggunakan instance untuk tujuan pengujian, Anda tidak akan menggunakan instans untuk menyimpan informasi sensitif, dan oleh karena itu langkah-langkah keamanan dapat menjadi kurang membatasi. Untuk contoh pengujian, umumnya dapat diterima untuk mengizinkan lalu lintas dari alamat IP apa pun (`0.0.0.0/0`) sehingga Anda selalu dapat terhubung meskipun alamat IP Anda berubah. Namun, untuk instance produksi, terutama yang memiliki data sensitif, praktik terbaik adalah mengizinkan lalu lintas hanya dari alamat IP yang diketahui.

9. Konfigurasikan penyimpanan instance:

   Di bawah Konfigurasi penyimpanan, bidang volume Root (Terenkripsi) dikonfigurasi secara default. Biarkan pengaturan sebagaimana adanya untuk tetap di bawah batas Tingkat Gratis.

   Karena instance pengujian kami tidak akan menyimpan data sensitif apa pun, kami tidak memerlukan volume data terenkripsi tambahan.

10. Tinjau konfigurasi instance:

Di panel Summary di sebelah kanan, Anda dapat meninjau pengaturan tingkat tinggi sebelum meluncurkan instans Anda.

11. Luncurkan instance Anda:

    Ketika Anda siap untuk meluncurkan instance Anda, di panel Summary, pilih Launch instance.

    Amazon EC2 dengan cepat meluncurkan instans Anda menggunakan pengaturan yang Anda tentukan. Jika Anda tidak menentukan pengaturan, default akan digunakan. Spanduk Sukses mengkonfirmasi peluncuran.

Selamat!Anda telah berhasil meluncurkan instance pengujian Anda!

Tugas 5: Temukan instance Anda

Dalam tugas ini, Anda akan menemukan instance yang baru saja Anda luncurkan di konsol EC2.

Ikuti langkah-langkah berikut untuk menemukan instans Anda di konsol EC2

1. Buka halaman Instans:

    Jika Anda masih berada di halaman sukses, pilih ID instans di spanduk Sukses.

    Jika Anda telah menavigasi, pilih Instans dari panel navigasi.

2. Temukan instance Anda:

    Di kolom Nama, temukan contoh Anda dengan nama yang Anda berikan.

Tugas 6: Lihat konfigurasi instans

Dalam tugas ini, Anda akan terbiasa melihat detail konfigurasi instans Anda.

Ikuti langkah-langkah ini untuk melihat konfigurasi instans Anda

1. Temukan instance Anda:

    Di kolom Nama, temukan contoh Anda dengan nama yang Anda berikan.

2. Buka halaman detail instance:

Pilih kotak centang di sebelah nama instans Anda, lalu pilih menu Tindakan (kanan atas), dan pilih Lihat detail untuk membuka halaman detail instance tempat Anda dapat meninjau konfigurasinya.

Dalam tutorial sebelumnya, Anda memilih link ID instance untuk membuka halaman detail instance. Anda akan menemukan bahwa ada lebih dari satu cara untuk menyelesaikan tugas di konsol EC2.

3. Jelajahi detail konfigurasi instance:

   Luangkan beberapa menit untuk menjelajahi detail konfigurasi instans Anda.

   Tip: Untuk menemukan bidang dengan cepat, tekan Ctrl+F atau Command+F pada keyboard Anda.

   a. AMI: Dapatkah Anda menemukan AMI yang Anda gunakan untuk meluncurkan instans Anda? Anda dapat menemukan informasi di ID AMI dan nama AMI di tab Detail.
   b. Jenis instans: Dapatkah Anda menemukan tipe instance? Mungkin t3.micro, misalnya.
   c. Pasangan kunci: Dapatkah Anda menemukan key pair yang Anda pilih saat meluncurkan instans Anda? Ini ditentukan untuk pasangan Kunci yang ditetapkan saat peluncuran. Perhatikan bahwa jika Anda mengubah key pair di masa depan, nilai di sini tidak akan berubah.
   d. VPC: Dapatkah Anda menemukan ID VPC Anda? Anda akan menemukan semua pengaturan konfigurasi terkait jaringan pada tab Jaringan. ID VPC dalam format yang mirip dengan contoh berikut: vpc-1a2b3c4d
   e. Subnet: Dapatkah Anda menemukan ID subnet tempat Anda meluncurkan instance Anda? Ini dalam format yang mirip dengan contoh berikut: subnet-1a2b3c4d
   f. IPv4 Alamat publik: Dapatkah Anda menemukan IPv4 alamat publik yang dialokasikan untuk instans Anda? Ini dalam format yang mirip dengan contoh berikut: 34.242.148.128.
   g. Grup keamanan: Dapatkah Anda menemukan aturan masuk yang dibuat untuk mengizinkan lalu lintas SSH dari mana saja (0.0.0.0./0)? Anda akan menemukan semua pengaturan konfigurasi terkait keamanan di tab Keamanan.
   h. Penyimpanan: Dapatkah Anda menemukan volume yang dibuat untuk instance ini? Anda akan menemukan semua pengaturan konfigurasi terkait penyimpanan di tab Penyimpanan.

i. Instance tags: Nama yang Anda berikan instance Anda sebenarnya adalah sebuah tag. Bisakah Anda menemukan tag instance Anda? Pilih tab Tanda. Kuncinya adalah Nama, dan nilainya adalah nama yang Anda berikan.

j. Status instans: Dapatkah Anda memverifikasi status instans Anda? Itu harus berjalan.

Luangkan beberapa menit lagi untuk menjelajahi bidang konfigurasi instance lainnya. Ketika Anda siap, lanjutkan ke tugas berikutnya.

Tugas 7: Biasakan diri Anda dengan komponen kunci untuk menghubungkan ke sebuah instance

Dalam tugas ini, Anda akan menjelajahi komponen kunci yang diperlukan untuk terhubung ke instans EC2. Ini adalah protokol koneksi, DNS publik, grup keamanan, key pair, dan nama pengguna instance.

Untuk membantu memvisualisasikan komponen-komponen ini, pikirkan untuk menghubungkan ke contoh seperti pergi ke rumah Anda:

- Protokol koneksi — Moda transportasi Anda: Sama seperti memilih cara pulang, Anda memilih protokol koneksi yang akan membawa Anda ke instans Anda. Dalam tutorial ini, kita akan menggunakan SSH (Secure Shell), yang menciptakan terowongan aman untuk menghubungkan komputer Anda ke instance Anda melalui internet.
- DNS Publik — Alamat rumah: Sama seperti rumah Anda memiliki alamat unik, instans EC2 Anda memiliki nama DNS publik sendiri (misalnya,). `ec2-18-201-118-201.eu-west-1.compute.amazonaws.com` Nama DNS publik ini memungkinkan SSH untuk terhubung langsung ke instans Anda.
- Kelompok keamanan — Penjaga gerbang: Bayangkan rumah Anda memiliki penjaga gerbang yang mengontrol siapa yang mungkin masuk atau pergi. Demikian pula, instans EC2 memiliki grup keamanan yang bertindak seperti penjaga gerbang, mengendalikan jenis lalu lintas jaringan mana yang diizinkan masuk atau keluar dari instance Anda. Hanya lalu lintas yang Anda izinkan secara eksplisit (misalnya, lalu lintas SSH dari alamat IP komputer Anda) yang diizinkan masuk.
- Kunci pribadi — Kunci pintu depan Anda: Ketika Anda meluncurkan instance, Anda menentukan key pair. Kunci publik ditempatkan pada instance, dan Anda menyimpan kunci pribadi di komputer Anda. Kunci pribadi bertindak sebagai kunci pintu depan Anda—tanpanya, Anda tidak bisa masuk ke instance Anda.
- Nama pengguna instans — Penduduk: Ketika Anda tiba di rumah Anda, Anda perlu mengidentifikasi diri Anda untuk membuktikan bahwa Anda adalah penduduk. Demikian pula, saat menghubungkan ke sebuah instance, Anda memberikan nama pengguna. Contoh yang berbeda

memiliki nama pengguna default yang berbeda, tergantung pada sistem operasinya. Misalnya, instans Amazon Linux digunakan `ec2-user` sebagai nama pengguna default.

Perintah koneksi

Untuk terhubung ke instans EC2 Anda, gunakan perintah berikut di jendela terminal:

```
ssh -i "test-instance-key-pair.pem" ec2-user@ec2-18-201-118-201.eu-
west-1.compute.amazonaws.com
```

Berikut adalah rincian dari apa yang dilakukan perintah:

- `ssh`— Perintah ini menentukan protokol koneksi, memulai koneksi SSH (Secure Shell) ke instance Anda.
- `-i "test-instance-key-pair.pem"`- `-i` Bendera menunjukkan file kunci pribadi yang diperlukan untuk mengautentikasi koneksi. File kunci pribadi ini harus cocok dengan key pair yang Anda tentukan saat meluncurkan instance. Jika file kunci pribadi Anda disimpan dalam folder tertentu, tentukan jalur lengkap ke file tersebut.
- `ec2-user`— Ini adalah nama pengguna untuk masuk ke instance. Untuk instance Amazon Linux, nama pengguna defaultnya adalah`ec2-user`. Lainnya AMIs mungkin menggunakan nama pengguna default yang berbeda, seperti `ubuntu` untuk instance Ubuntu.
- `@`— Simbol ini memisahkan nama pengguna dari alamat instans.
- `ec2-18-201-118-201.eu-west-1.compute.amazonaws.com`— Ini adalah alamat publik instans Anda (DNS publik), yang mencakup IPv4 alamat publik dan. AWS Region Ini secara unik mengidentifikasi instance.

Apa yang terjadi ketika Anda menjalankan perintah

Setelah Anda menjalankan perintah, SSH membuat terowongan aman dan mengautentikasi dengan kunci pribadi Anda. Jika grup keamanan instans mengizinkan lalu lintas, Anda mendapatkan akses ke instans EC2 Anda. Anda sekarang dapat mengontrol instance dari komputer Anda seolah-olah Anda sedang duduk tepat di depannya. Anda dapat menjalankan perintah, menginstal perangkat lunak, dan mengelola file — seperti yang Anda lakukan pada mesin lokal Anda.

Tugas 8: Connect ke instans Anda

Dalam tugas ini, Anda akan terhubung ke instans Anda menggunakan klien SSH di komputer Anda. Dalam tugas sebelumnya, kami memperkenalkan komponen untuk menghubungkan ke

sebuah instance menggunakan analogi pergi ke rumah Anda. Sekarang, kita akan fokus pada menghubungkan ke instans EC2 yang sebenarnya.

Ada berbagai cara untuk terhubung ke sebuah instance. Metode yang Anda gunakan untuk menghubungkan tergantung pada sistem operasi instans. Karena Anda telah meluncurkan instance Linux, Anda akan menggunakan klien SSH di komputer lokal Anda.

Pertama, periksa apakah komputer Anda memiliki klien SSH yang diinstal

Sebagian besar komputer dilengkapi dengan klien SSH yang sudah diinstal sebelumnya. Untuk memeriksa, buka jendela terminal di komputer Anda dan jalankan perintah berikut:

```
ssh
```

Jika perintah dikenali, Anda siap untuk terhubung.

Jika perintah tidak dikenali, Anda harus menginstal klien SSH. Petunjuk untuk menginstal klien SSH berada di luar cakupan tutorial ini. Jika Anda memerlukan bantuan, lihat Prasyarat koneksi SSH di panduan pengguna ini atau cari secara online untuk petunjuk tentang cara menginstal klien SSH di sistem operasi Anda.

Ikuti langkah-langkah ini untuk terhubung ke instans Anda

1. Mulai menghubungkan:

   Jika Anda berada di halaman detail instans di konsol Amazon EC2, pilih tombol Connect (kanan atas).

   Jika Anda telah menavigasi, pilih Instans dari panel navigasi. Kemudian, pada halaman Instances, pilih kotak centang di sebelah nama instans Anda dan pilih tombol Connect (kanan atas).

   Ini membuka halaman Connect to instance.
2. Pilih metode koneksi:

   Pada halaman Connect to instance, pilih tab SSH client.

   Luangkan waktu sejenak untuk meninjau teks di halaman ini, karena ini adalah langkah-langkah yang akan Anda ikuti selanjutnya.
3. Tinjau perintah SSH:

Di bawah Contoh, Anda akan melihat perintah yang dibuat secara otomatis dan disesuaikan dengan detail instans Anda. Nama kunci pribadi berasal dari nama kunci publik yang ditentukan saat peluncuran.

Perintahnya terlihat seperti ini:

```
ssh -i "test-instance-key-pair.pem" ec2-user@ec2-18-201-118-201.eu-
west-1.compute.amazonaws.com
```

4. Salin perintah SSH:

   Pilih ikon salin di sebelah contoh perintah SSH.

5. Buka jendela terminal:

   Di komputer lokal Anda, buka jendela terminal.

6. Tempel dan jalankan perintah SSH:

   Tempelkan perintah SSH ke jendela terminal. Jika Anda menyimpan file kunci pribadi Anda di folder tertentu, edit perintah untuk menyertakan jalur file lengkap.

   Tekan Enter pada keyboard Anda.

   Anda akan melihat respons yang mirip dengan berikut ini:

```
The authenticity of host 'ec2-18-201-118-201.eu-west-1.compute.amazonaws.com
 (18-201-118-201)' can't be established.
ED25519 key fingerprint is SHA256:examplehxj9aOr1MogvKOoMNskVVIRBQBoq0example.This
 key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

7. Selesaikan koneksi:

   Masuk **`yes`** dan tekan Return pada keyboard Anda.

   Memverifikasi sidik jari berada di luar cakupan tutorial ini. Untuk mempelajari selengkapnya, lihat (Opsional) Dapatkan sidik jari instans.

   Setelah koneksi berhasil, prompt terminal berubah untuk menampilkan DNS publik instans Anda.

Selamat! Anda telah berhasil terhubung ke instans Anda!

Tugas 9: Hentikan instans Anda

Dalam tugas ini, Anda akan menghentikan instans Anda untuk mempertahankan manfaat Tingkat Gratis Anda. Ketika instance Anda dihentikan, Anda berhenti mengeluarkan biaya untuk itu. Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan memenuhi syarat untuk Tingkat Gratis, Anda akan terus mengeluarkan biaya untuk penyimpanan EBS.

Ikuti langkah-langkah ini untuk menghentikan instans Anda

1. Mulai berhenti:

   Jika Anda masih berada di halaman Connect to instance, pilih Instances dari breadcrumb. Jika Anda telah menavigasi, pilih Instans dari panel navigasi.

   Kemudian, pada halaman Instances, pilih kotak centang di sebelah nama instance Anda, lalu pilih menu status Instance (kanan atas), dan pilih Stop instance. Saat diminta, pilih Berhenti.
2. Memantau status instance:

   Pada halaman Instances, periksa kolom Instance state. Status instans Anda berubah menjadi Berhenti dan kemudian Berhenti. Jika Anda tidak melihat teks lengkapnya, coba lebarkan kolom.

   Jika menurut Anda status instans telah berubah dari Berhenti menjadi Berhenti, tetapi Anda belum melihatnya, pilih ikon penyegaran (di atas tabel) untuk menyegarkan tabel Instances.

Takeaways kunci

Dalam tutorial ini, Anda membahas konsep-konsep kunci berikut:

- AMI mengacu pada Amazon Machine Image, yang merupakan template yang berisi sistem operasi dan perangkat lunak yang diperlukan untuk meluncurkan instance.
- Jenis instans mengacu pada perangkat keras komputer host yang digunakan untuk instance Anda. Ini menentukan CPU, memori, penyimpanan, dan kapasitas jaringan instans Anda.
- Pasangan kunci mengacu pada kumpulan kunci publik dan pribadi yang dapat Anda gunakan untuk menghubungkan dengan aman ke instans Anda.
- Jaringan mengacu pada VPC (cloud pribadi virtual yang didedikasikan untuk akun Anda di dalam AWS Cloud) dan subnet (berbagai alamat IP dalam VPC Anda).
- Grup keamanan mengacu pada seperangkat aturan yang mengontrol lalu lintas apa yang dapat mencapai instans Anda.

- Volume EBS mengacu pada penyimpanan data untuk instans Anda. Setiap instance memiliki volume root untuk menyimpan AMI dan satu atau lebih volume data opsional.
- Tag adalah metadata yang dapat Anda tetapkan secara opsional ke instance Anda. Nama instance adalah tag, yang Key adalah Name, dan Value adalah pilihan Anda.
- Menghubungkan mengacu pada mengakses instans Anda melalui internet.
- SSH mengacu pada protokol koneksi Secure Shell yang dapat Anda gunakan untuk terhubung ke instans Anda.
- DNS publik adalah alamat publik unik instans Anda.
- Nama pengguna instans ditentukan oleh sistem operasi instans Anda dan diperlukan untuk menghubungkan.
- Menghentikan instans Anda menghentikan biaya untuk instans, tetapi biaya penyimpanan EBS terus berlanjut.

Langkah selanjutnya

Untuk membangun kepercayaan diri dalam meluncurkan, menghubungkan ke, dan menghentikan instance, pertimbangkan untuk mengulangi langkah-langkah dalam tutorial ini. Pastikan untuk menghentikan setiap instance yang Anda luncurkan untuk mempertahankan manfaat Tingkat Gratis Anda.

Setelah Anda merasa nyaman dengan dasar-dasar ini, Anda dapat menjelajahi tutorial yang lebih canggih. Untuk tutorial lainnya, lihat Mencari tutorial lainnya?

Jika Anda membuat Akun AWS sebelum 15 Juli 2025, pertimbangkan untuk menonton video 6 menit berikut: Bagaimana saya bisa menghindari tagihan di akun saya saat menggunakan layanan AWS Tingkat Gratis

Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, pertimbangkan untuk meninjau informasi berikut: Jelajahi AWS layanan dengan Tingkat AWS Gratis di Panduan Pengguna AWS Billing

Referensi untuk parameter konfigurasi EC2 instans Amazon

Wizard instance peluncuran dan template peluncuran di EC2 konsol Amazon menyediakan semua parameter untuk mengonfigurasi EC2 instans Amazon.

Kecuali untuk key pair, wizard instance peluncuran memberikan nilai default untuk setiap parameter. Anda dapat menerima salah satu atau semua default, atau mengonfigurasi instance dengan nilai

Anda sendiri. Saat membuat template peluncuran, parameternya opsional. Jika Anda menggunakan template peluncuran untuk meluncurkan instance, parameter yang ditentukan dalam template peluncuran akan mengganti nilai default di wizard instance peluncuran. Parameter apa pun yang tidak ditentukan dalam template peluncuran akan default ke nilai yang disediakan oleh wizard instance peluncuran.

Parameter dikelompokkan dalam wizard instance peluncuran dan template peluncuran. Deskripsi berikut disajikan sesuai dengan pengelompokan parameter di konsol.

Parameter untuk konfigurasi instans

- Nama dan tanda
- Aplikasi dan Gambar OS (Gambar Mesin Amazon)
- Tipe instans
- Pasangan kunci (login)
- Pengaturan jaringan
- Mengonfigurasi penyimpanan
- Detail lanjutan
- Ringkasan

Nama dan tanda

Nama instans adalah tanda, di mana kuncinya adalah Name, dan nilainya adalah nama yang Anda tentukan. Anda dapat menandai instance, volume, dan antarmuka jaringan. Untuk Instans Spot, Anda hanya dapat menandai permintaan Instans Spot. Untuk informasi tentang tanda, lihat Tandai sumber daya Amazon EC2 Anda.

Menentukan nama instans dan tanda tambahan bersifat opsional.

- Untuk Nama, masukkan nama deskriptif untuk instans tersebut. Jika Anda tidak menentukan nama, instans dapat diidentifikasi berdasarkan ID-nya, yang secara otomatis dihasilkan saat Anda meluncurkan instans tersebut.
- Untuk menambahkan tanda tambahan, pilih Tambahkan tanda tambahan. Pilih Tambahkan tanda, lalu masukkan kunci dan nilai, lalu pilih jenis sumber daya yang akan diberi tanda. Pilih Tambah tanda lagi untuk setiap tanda tambahan yang akan ditambahkan.

Anda hanya dapat menentukan nama instance saat meluncurkan instance. Anda tidak dapat memberi nama instance saat membuat template peluncuran, tetapi Anda dapat menambahkan tag untuk sumber daya yang dibuat saat instance diluncurkan.

Aplikasi dan Gambar OS (Gambar Mesin Amazon)

Amazon Machine Image (AMI) berisi informasi yang diperlukan untuk membuat instans. Misalnya, AMI mungkin berisi perangkat lunak yang diperlukan untuk bertindak sebagai server web, seperti Linux, Apache, dan situs web Anda.

Anda dapat menemukan AMI yang cocok sebagai berikut. Dengan setiap opsi untuk menemukan AMI, Anda dapat memilih Batal (di kanan atas) untuk kembali ke wizard peluncuran instans tanpa memilih AMI.

Bilah pencarian

Untuk mencari semua yang tersedia AMIs, masukkan kata kunci di bilah pencarian AMI dan kemudian tekan Enter. Untuk memilih AMI, pilih Pilih.

Terbaru

AMIs Yang baru saja Anda gunakan.

Pilih Baru diluncurkan atau Saat ini sedang digunakan, kemudian pilih AMI dari Amazon Machine Image (AMI).

Saya AMIs

Pribadi AMIs yang Anda miliki, atau pribadi AMIs yang telah dibagikan dengan Anda.

Pilih Milik saya atau Dibagikan dengan saya, kemudian pilih AMI dari Amazon Machine Image (AMI).

Mulai Cepat

AMIs dikelompokkan berdasarkan sistem operasi (OS) untuk membantu Anda memulai dengan cepat.

Pertama, pilih OS yang Anda butuhkan, lalu pilih AMI dari Amazon Machine Image (AMI). Untuk memilih AMI yang dapat digunakan di bawah Tingkat AWS Gratis, pastikan AMI ditandai Tingkat Gratis yang memenuhi syarat.

Jelajahi lebih AMIs

Pilih Jelajahi lebih banyak AMIs untuk menelusuri katalog AMI lengkap.

- Untuk mencari melalui semua yang tersedia AMIs, masukkan kata kunci di bilah pencarian dan kemudian tekan Enter.
- Untuk menemukan AMI dengan menggunakan parameter Systems Manager, pilih tombol panah di sebelah kanan bilah pencarian, lalu pilih parameter Cari berdasarkan Systems Manager. Untuk informasi selengkapnya, lihat Referensi AMIs menggunakan parameter Systems Manager.
- Untuk mencari berdasarkan kategori, pilih Mulai Cepat AMIs, Saya AMIs AWS Marketplace AMIs, atau Komunitas AMIs.

  AWS Marketplace Ini adalah toko online tempat Anda dapat membeli perangkat lunak yang berjalan AWS, termasuk AMIs. Untuk informasi selengkapnya tentang meluncurkan instance dari AWS Marketplace, lihatLuncurkan instans Amazon EC2 dari AMI AWS Marketplace.
  Di Komunitas AMIs, Anda dapat menemukan AMIs bahwa anggota AWS komunitas telah menyediakan untuk digunakan orang lain. AMIsdari Amazon atau mitra terverifikasi ditandai Penyedia terverifikasi.
- Untuk memfilter daftar AMIs, pilih satu atau beberapa kotak centang di bawah Perbaiki hasil di sebelah kiri layar. Opsi filter berbeda tergantung pada kategori pencarian yang dipilih.
- Periksa Tipe perangkat root yang terdaftar untuk setiap AMI. Perhatikan jenis AMIs yang Anda butuhkan: ebs (didukung oleh Amazon EBS) atau instance-store (didukung oleh toko instance). Untuk informasi selengkapnya, lihat Tipe volume root.
- Periksa Ttipe virtualisasi yang tercantum untuk setiap AMI. Perhatikan jenis mana AMIs yang Anda butuhkan: baik hvm atau paravirtual. Sebagai contoh, beberapa tipe instans memerlukan HVM. Untuk informasi selengkapnya tentang jenis virtualisasi Linux, lihatTipe virtualisasi.
- Periksa Mode booting yang terdaftar untuk setiap AMI. Perhatikan mana yang AMIs menggunakan mode boot yang Anda butuhkan: baik legacy-bios, uefi, atau uefi-preferen. Untuk informasi selengkapnya, lihat Perilaku peluncuran instans dengan mode boot Amazon EC2.
- Pilih AMI yang memenuhi kebutuhan Anda, lalu pilih Pilih.

Peringatan saat mengganti AMI

Ketika Anda meluncurkan instance, jika Anda mengubah konfigurasi volume atau grup keamanan apa pun yang terkait dengan AMI yang dipilih, dan kemudian Anda memilih AMI yang berbeda, sebuah jendela terbuka untuk memperingatkan Anda bahwa beberapa pengaturan Anda saat ini akan diubah atau dihapus. Anda dapat meninjau perubahan pada grup keamanan dan volume. Selanjutnya, Anda dapat memilih untuk melihat volume mana yang akan ditambahkan dan dihapus,

atau hanya melihat volume yang akan ditambahkan. Peringatan ini tidak muncul saat membuat template peluncuran.

Tipe instans

Tipe instans mendefinisikan konfigurasi perangkat keras dan ukuran instans. Tipe instans yang lebih besar memiliki lebih banyak CPU dan memori. Untuk informasi selengkapnya, lihat jenis EC2 instans Amazon.

- Tipe Instans: Pastikan bahwa tipe instans kompatibel dengan AMI yang Anda tentukan. Untuk informasi selengkapnya, lihat Tipe instans Amazon EC2.

  Tingkat Gratis — Anda dapat menggunakan jenis instans yang diberi label Tingkat gratis yang memenuhi syarat secara gratis di bawah Tingkat Gratis. Jenis instans spesifik bergantung pada saat Anda membuat Akun AWS.

  Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan usianya kurang dari 12 bulan, Anda dapat menggunakan Amazon EC2 di bawah Tingkat Gratis dengan memilih jenis instans t2.micro, atau jenis instans t3.micro di Wilayah di mana t2.micro tidak tersedia. Ketahuilah bahwa ketika Anda meluncurkan instans t3.micro, default ke mode Tidak Terbatas, yang mungkin dikenakan biaya tambahan berdasarkan penggunaan CPU.

  Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, Anda dapat menggunakan jenis instans t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large, dan m7i-flex.large selama 6 bulan atau sampai kredit Anda habis.

  Untuk informasi selengkapnya, lihat Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025.
- Bandingkan jenis instans: Anda dapat membandingkan jenis instans yang berbeda dengan atribut berikut: jumlah vCPUs, arsitektur, jumlah memori (GiB), jumlah penyimpanan (GB), jenis penyimpanan, dan kinerja jaringan.
- Dapatkan saran: Anda bisa mendapatkan panduan dan saran untuk jenis instance dari pencari jenis EC2 instance. Untuk informasi selengkapnya, lihat Dapatkan rekomendasi dari pencari tipe instans EC2.
- (Hanya meluncurkan templat) Lanjutan: Untuk menentukan atribut instance dan membiarkan Amazon EC2 mengidentifikasi jenis instance dengan atribut tersebut, pilih Lanjutan, lalu pilih Tentukan atribut tipe instance.

- Jumlah v CPUs: Masukkan jumlah minimum dan maksimum v CPUs untuk persyaratan komputasi Anda. Untuk menunjukkan tidak ada batas, masukkan minimum **0**, dan biarkan maksimum kosong.
- Jumlah memori (MiB): Masukkan jumlah memori minimum dan maksimum, dalam MiB, untuk kebutuhan komputasi Anda. Untuk menunjukkan tidak ada batas, masukkan minimum **0**, dan biarkan maksimum kosong.
- Perluas atribut tipe instans opsional dan pilih Tambahkan atribut untuk mengekspresikan persyaratan komputasi Anda secara lebih detail. Untuk informasi tentang setiap atribut, lihat InstanceRequirementsRequestdi Referensi Amazon EC2 API.
- Tipe instans yang dihasilkan: Anda dapat melihat pratinjau tipe instans yang cocok dengan atribut yang ditentukan. Untuk mengecualikan tipe instans, pilih Tambahkan atribut, dan dari daftar Atribut, pilih Tipe instans yang dikecualikan. Dari daftar Nilai atribut, pilih tipe instans yang akan dikecualikan.

Pasangan kunci (login)

Untuk Nama pasangan kunci, pilih pasangan kunci yang ada, atau pilih Buat pasangan kunci baru untuk membuat yang baru. Untuk informasi selengkapnya, lihat Pasangan kunci Amazon EC2 dan instans Amazon EC2.

> **Important**
>
> Jika Anda memilih opsi Lanjutkan tanpa pasangan kunci (Tidak direkomendasikan), Anda tidak akan dapat terhubung ke instans tersebut, kecuali Anda memilih sebuah AMI yang dikonfigurasi agar pengguna dapat masuk dengan cara lain.

Pengaturan jaringan

Pengaturan jaringan menentukan alamat IP, grup keamanan, dan antarmuka jaringan untuk instance Anda. Anda dapat menggunakan pengaturan jaringan default atau mengkonfigurasinya sesuai kebutuhan.

- (Hanya Luncurkan wizard instance) VPC: Pilih VPC yang ada untuk instance Anda. VPC default untuk Wilayah dipilih secara default. Atau, Anda dapat memilih VPC yang Anda buat atau yang dibagikan dengan Anda. Untuk informasi selengkapnya, lihat Virtual private cloud untuk EC2 instans Anda.

- Subnet: Pilih subnet untuk instans Anda atau pilih Buat subnet baru untuk membuat subnet baru menggunakan konsol Amazon VPC.
  - Anda dapat membuat subnet di Availability Zone, Local Zone, Wavelength Zone, atau Outpost Zone untuk VPC yang dipilih.
  - Untuk meluncurkan instance di subnet IPv6 -only, instance harus berupa instance berbasis Nitro.
- (Hanya luncurkan wizard instans) Tetapkan otomatis IP Publik: Aktifkan atau nonaktifkan penetapan otomatis alamat publik. IPv4 Saat meluncurkan instance ke subnet default, nilai defaultnya adalah Aktifkan. Saat meluncurkan instance ke subnet nondefault, nilai defaultnya adalah Nonaktifkan. Untuk informasi selengkapnya, lihat IPv4 Alamat publik.

  Anda tidak dapat mengaktifkan opsi ini untuk subnet nondefault jika Anda menambahkan antarmuka jaringan sekunder. Untuk informasi selengkapnya, lihat the section called “Tetapkan IPv4 alamat publik saat peluncuran”.
- (Hanya luncurkan wizard instance) Tetapkan otomatis IPv6 IP: Aktifkan atau nonaktifkan penetapan alamat secara otomatis. IPv6 Untuk informasi selengkapnya, lihat IPv6 alamat.
- Firewall (grup keamanan): Pilih grup keamanan yang ada atau buat yang baru. Pastikan grup keamanan Anda memiliki aturan yang memungkinkan lalu lintas ke dan dari instans Anda. Semua lalu lintas lainnya diabaikan.

  Jika Anda membuat grup keamanan baru, kami secara otomatis membuat aturan masuk yang memungkinkan Anda terhubung ke instans Anda dari semua alamat IP melalui SSH (instance Linux) atau RDP (instance Windows. Anda dapat menghapus atau memodifikasi aturan ini sesuai kebutuhan. Anda dapat menambahkan aturan sesuai kebutuhan. Untuk informasi selengkapnya, lihat Mengonfigurasi aturan grup keamanan.

  > **Warning**
  >
  > Aturan yang memungkinkan semua alamat IP untuk mengakses instans Anda melalui SSH atau RDP dapat diterima jika Anda meluncurkan instance pengujian sebentar dan akan menghentikan atau menghentikannya setelah waktu yang singkat. Mereka tidak aman untuk lingkungan produksi. Anda harus mengotorisasi hanya rentang alamat IP tertentu untuk mengakses instans Anda.

Grup keamanan ini ditambahkan ke antarmuka jaringan utama dan antarmuka jaringan sekunder apa pun. Anda dapat memilih grup keamanan tambahan untuk antarmuka jaringan Anda, tetapi Anda tidak dapat menghapus salah satu yang Anda pilih di sini.

- Konfigurasi jaringan lanjutan - Anda dapat mengkonfigurasi antarmuka jaringan utama sesuai kebutuhan. Untuk menambahkan antarmuka jaringan sekunder, pilih Tambahkan antarmuka jaringan. Jumlah antarmuka jaringan yang dapat Anda tambahkan tergantung pada jenis instance yang Anda pilih. Perhatikan bahwa bagian ini hanya tersedia jika Anda memilih subnet.
  - Indeks perangkat: Indeks perangkat. Antarmuka jaringan utama harus ditetapkan ke indeks 0.
  - Antarmuka jaringan: Antarmuka jaringan. Pilih Antarmuka baru untuk memungkinkan Amazon EC2 membuat antarmuka baru, atau pilih antarmuka jaringan yang ada dan tersedia. Jika Anda memilih antarmuka jaringan yang ada sebagai antarmuka jaringan utama, Anda tidak dapat mengaktifkan Auto-assign IP Publik untuk subnet nondefault.
  - Deskripsi: Deskripsi untuk antarmuka jaringan baru.
  - Subnet: Subnet tempat membuat antarmuka jaringan baru. Instance diluncurkan di subnet yang sama dengan antarmuka jaringan utama.

    Anda harus memilih subnet untuk antarmuka jaringan sekunder dari Availability Zone yang sama dengan subnet untuk antarmuka jaringan utama. Jika Anda memilih subnet dari VPC lain, label Multi-VPC muncul di sebelah antarmuka jaringan. Ini memungkinkan Anda membuat instance multi-homed VPCs dengan konfigurasi jaringan dan keamanan yang berbeda.

    Untuk meluncurkan EC2 instance ke subnet IPv6 -only, Anda harus menggunakan instance berbasis Nitro. Saat meluncurkan instance IPv6 -only, ada kemungkinan bahwa DHCPv6 mungkin tidak segera menyediakan instance dengan server nama IPv6 DNS. Selama penundaan awal ini, instance mungkin tidak menyelesaikan domain publik. Anda dapat mengubah file konfigurasi dan gambar ulang AMI Anda sehingga file tersebut memiliki alamat server nama IPv6 DNS segera saat booting.
  - Grup keamanan: Grup keamanan untuk diasosiasikan dengan antarmuka jaringan. Anda harus memilih grup keamanan dari VPC yang sama dengan subnet untuk antarmuka jaringan.
  - (Hanya meluncurkan templat) Tetapkan IP publik secara otomatis: Tentukan apakah instans Anda menerima alamat publik IPv4 . Secara default, instance di subnet default menerima IPv4 alamat publik dan instance di subnet nondefault tidak. Anda dapat memilih Aktifkan atau Nonaktifkan untuk mengganti pengaturan default subnet. Untuk informasi selengkapnya, lihat IPv4 Alamat publik.

- IP Primer: IPv4 Alamat pribadi dari kisaran subnet Anda. Biarkan kosong untuk membiarkan Amazon EC2 memilih IPv4 alamat pribadi untuk Anda.
- IP Sekunder: IPv4 Alamat pribadi tambahan dari kisaran subnet Anda. Pilih Tetapkan secara manual dan masukkan IPv4 alamat. Pilih Tambahkan IP untuk menambahkan IPv4 alamat lain. Atau, pilih Tetapkan secara otomatis dan masukkan nilai untuk menunjukkan jumlah IPv4 alamat yang EC2 dipilih Amazon untuk Anda.
- (IPv6-only) IPv6 IPs: IPv6 alamat dari kisaran subnet. Pilih Tetapkan secara manual dan masukkan IPv6 alamat. Pilih Tambahkan IP untuk menambahkan IPv6 alamat lain. Atau, pilih Tetapkan secara otomatis dan masukkan nilai untuk menunjukkan jumlah IPv6 alamat yang EC2 dipilih Amazon untuk Anda.
- IPv4 Awalan: IPv4 Awalan untuk antarmuka jaringan. Pilih Tetapkan secara manual dan masukkan IPv4 awalan. Atau, pilih Tetapkan secara otomatis dan masukkan nilai untuk menunjukkan jumlah IPv4 awalan yang EC2 dipilih Amazon untuk Anda.
- IPv6 Awalan: IPv6 Awalan untuk antarmuka jaringan. Pilih Tetapkan secara manual dan masukkan IPv6 awalan. Atau, pilih Tetapkan secara otomatis dan masukkan nilai untuk menunjukkan jumlah IPv6 awalan yang EC2 dipilih Amazon untuk Anda.
- (Dual-stack dan IPv6 -only) Tetapkan IPv6 IP Primer: Jika Anda memilih subnet dual-stack atau IPv6 -only, tetapkan alamat utama. IPv6 Ini membantu mencegah gangguan lalu lintas ke instance atau antarmuka jaringan. Aktifkan opsi ini jika Anda mengandalkan IPv6 alamat yang tidak berubah. Anda tidak dapat menghapus IPv6 alamat utama nanti. Ketika Anda mengaktifkan alamat IPv6 GUA menjadi primer IPv6, IPv6 GUA pertama menjadi IPv6 alamat utama sampai instance dihentikan atau antarmuka jaringan terlepas. Jika Anda memiliki beberapa IPv6 alamat yang terkait dengan antarmuka jaringan dan Anda membiarkan Amazon EC2 menetapkan IPv6 alamat utama, alamat IPv6 GUA pertama yang terkait dengan antarmuka jaringan adalah IPv6 alamat utama.
- Hapus saat penghentian: Menunjukkan apakah antarmuka jaringan dihapus saat instance dihapus.
- Jenis antarmuka: Jenis antarmuka jaringan:
  - ENA: Antarmuka jaringan berkinerja tinggi yang dirancang untuk menangani throughput dan packet-per-second tingkat tinggi untuk TCP/IP protokol sambil meminimalkan penggunaan CPU. Ini adalah nilai default. Untuk informasi lebih lanjut tentang ENA, lihat Adaptor Jaringan Elastis.

    - EFA dengan ENA: Antarmuka jaringan yang mendukung perangkat ENA dan EFA untuk transportasi TCP/IP berbasis tradisional bersama dengan transportasi berbasis SRD. Untuk informasi lebih lanjut tentang EFA, lihat Adaptor Kain Elastis.
    - Khusus EFA: Antarmuka jaringan berkinerja tinggi yang dirancang untuk menangani throughput tinggi, komunikasi antar-node latensi rendah untuk transportasi berbasis SRD sambil melewati tumpukan sistem operasi. Antarmuka jaringan khusus EFA tidak mendukung alamat IP. Untuk informasi lebih lanjut tentang EFA, lihat Adaptor Kain Elastis.
- Elastic Fabric Adapter: Menunjukkan apakah antarmuka jaringan adalah Elastic Fabric Adapter. Untuk informasi selengkapnya, lihat Adaptor Kain Elastis untuk AI/ML dan beban kerja HPC di Amazon EC2.
- Indeks Kartu Jaringan: Indeks kartu jaringan. Antarmuka jaringan primer harus ditetapkan ke indeks kartu jaringan 0. Beberapa tipe instans mendukung banyak kartu jaringan.
- ENA Express: ENA Express didukung oleh teknologi AWS Scalable Reliable Datagram (SRD). Teknologi SRD menggunakan mekanisme penyemprotan paket untuk mendistribusikan beban dan menghindari kemacetan jaringan. Mengaktifkan ENA Ekspres memungkinkan instans yang didukung untuk berkomunikasi menggunakan SRD di atas lalu lintas TCP reguler bila memungkinkan. Wizard instance peluncuran atau template peluncuran tidak menyertakan konfigurasi ENA Express untuk instance kecuali Anda memilih Aktifkan atau Nonaktifkan dari daftar.
- ENA Express UDP: Jika Anda telah mengaktifkan ENA Ekspres, Anda dapat menggunakannya secara opsional untuk lalu lintas UDP. Wizard instance peluncuran atau template peluncuran tidak menyertakan konfigurasi ENA Express untuk instance kecuali Anda memilih Aktifkan atau Nonaktifkan.

Mengonfigurasi penyimpanan

AMI yang Anda pilih mencakup satu atau lebih volume penyimpanan, termasuk volume root. Anda dapat menentukan volume tambahan untuk dilampirkan ke instans.

(Hanya luncurkan wizard contoh) Anda dapat menggunakan tampilan Sederhana atau Lanjutan. Dengan tampilan Sederhana, Anda menentukan ukuran dan tipe volume. Untuk menentukan semua parameter volume, pilih tampilan Lanjutan (di kanan atas kartu).

Dengan menggunakan tampilan Lanjutan, Anda dapat mengonfigurasi setiap volume sebagai berikut:

- Tipe penyimpanan: Pilih volume Amazon EBS atau penyimpanan instans untuk dikaitkan dengan instans Anda. Tipe volume yang tersedia di daftar tergantung pada tipe instans yang telah Anda

pilih. Untuk informasi selengkapnya, lihat Instans menyimpan penyimpanan blok sementara untuk instans EC2 dan volume Amazon EBS.

- Nama perangkat: Pilih dari daftar nama perangkat yang tersedia untuk volume.
- Snapshot: Pilih snapshot yang akan digunakan untuk memulihkan volume. Anda dapat mencari snapshot bersama dan publik yang tersedia dengan memasukkan teks ke dalam bidang Snapshot.
- Ukuran (GiB): Untuk volume EBS, Anda dapat menentukan ukuran penyimpanan.
- Tipe volume: Untuk volume EBS, pilih tipe volume. Untuk informasi selengkapnya, lihat Jenis volume Amazon EBS di Panduan Pengguna Amazon EBS.
- IOPS: Jika Anda telah memilih jenis volume io1, io2, atau gp3, maka Anda dapat memasukkan jumlah I/O operasi per detik (IOPS) yang dapat didukung volume. Diperlukan untuk volume io1, io2, dan gp3. Tidak didukung untuk gp2, st1, sc1, atau volume standar. Jika Anda menghilangkan paramater ini untuk templat peluncuran, Anda harus menentukan nilai untuk itu saat Anda meluncurkan sebuah instans dari templat peluncuran.
- Hapus saat pengakhiran: Untuk volume Amazon EBS, pilih Ya untuk menghapus volume saat instans diakhiri, atau pilih Tidak untuk mempertahankan volume. Untuk informasi selengkapnya, lihat Pertahankan data saat instans diakhiri.
- Terenkripsi: Jika tipe instans mendukung enkripsi EBS, Anda dapat memilih Ya untuk mengaktifkan enkripsi untuk volume tersebut. Jika Anda telah mengaktifkan enkripsi secara default di Wilayah ini, enkripsi diaktifkan untuk Anda. Untuk informasi selengkapnya, lihat enkripsi Amazon EBS di Panduan Pengguna Amazon EBS.
- Kunci KMS: Jika Anda memilih Ya untuk Terenkripsi, maka Anda harus memilih kunci yang dikelola pelanggan untuk digunakan untuk mengenkripsi volume. Jika Anda telah mengaktifkan enkripsi secara default di Wilayah ini, kunci yang dikelola pelanggan secara default akan dipilihkan untuk Anda. Anda dapat memilih kunci yang berbeda atau menentukan ARN dari kunci yang dikelola pelanggan mana pun yang Anda buat.
- Throughput: Jika Anda telah memilih jenis gp3 volume, maka Anda dapat memasukkan throughput, dalam MIB/s, yang dapat didukung volume.
- Tingkat inisialisasi volume: Jika Anda telah memilih snapshot, Anda dapat menentukan tingkat inisialisasi volume secara opsional, di Mib/s, di mana blok snapshot akan diunduh dari Amazon S3 ke volume. Untuk informasi selengkapnya, lihat Menggunakan Tarif yang Disediakan Amazon EBS untuk Inisialisasi Volume. Untuk menggunakan tingkat inisialisasi default atau pemulihan snapshot cepat (jika diaktifkan untuk snapshot yang dipilih), jangan tentukan tarif.
- Sistem file: Pasang sistem FSx file Amazon EFS atau Amazon ke instans. Untuk informasi selengkapnya tentang pemasangan sistem file Amazon EFS, lihat Menggunakan Amazon EFS

dengan instans Amazon EC2 Linux. Untuk informasi selengkapnya tentang pemasangan sistem FSx file Amazon, lihat Gunakan Amazon FSx dengan EC2 instans Amazon

Detail lanjutan

Untuk Detail lanjutan, perluas bagian untuk melihat kolom dan menentukan parameter tambahan apa pun untuk instans.

- (Hanya panduan peluncuran instance) Direktori gabungan domain: Pilih Directory Service direktori (domain) tempat instance Anda bergabung setelah peluncuran. Jika Anda memilih domain, Anda harus memilih peran IAM dengan izin yang diperlukan. Untuk informasi selengkapnya tentang penggabungan domain, lihat Menggabungkan instans Amazon EC2 Linux dengan mulus ke direktori AD Microsoft AWS Terkelola (instance Linux) dan bergabung dengan instans Amazon EC2 Windows ke direktori AD AWS Microsoft Terkelola (instance Windows) dengan mulus.
- Profil instans IAM: Pilih profil instans IAM untuk dikaitkan dengan instance. Ini adalah wadah untuk peran IAM. Untuk informasi selengkapnya, lihat IAM role untuk Amazon EC2.
- Jenis nama host: Pilih apakah nama host OS tamu dari instans akan menyertakan nama sumber daya atau nama IP. Untuk informasi selengkapnya, lihat Nama host dan domain instans EC2.
- Nama Host DNS: Menentukan apakah permintaan DNS ke nama sumber daya atau nama IP (tergantung pada apa yang Anda pilih untuk jenis Hostname) akan merespons dengan alamat (catatan A), IPv4 alamat (catatan AAAA), IPv6 atau keduanya. Untuk informasi selengkapnya, lihat Nama host dan domain instans EC2.
- Pemulihan otomatis instans: Saat diaktifkan, pulihkan instans Anda jika pemeriksaan status sistem gagal. Pengaturan ini diaktifkan secara default saat peluncuran untuk jenis instans yang didukung. Untuk informasi selengkapnya, lihat Konfigurasikan pemulihan otomatis yang disederhanakan pada instans Amazon EC2.
- Perilaku pematian: Pilih apakah instans harus berhenti atau diakhiri saat dimatikan. Untuk informasi selengkapnya, lihat Ubah perilaku shutdown yang dimulai instance.
- Berhenti - Perilaku hibernasi: Untuk mengaktifkan hibernasi, pilih Aktifkan. Bidang ini hanya tersedia jika instans Anda memenuhi prasyarat hibernasi. Untuk informasi selengkapnya, lihat Hibernasi instans Amazon EC2 Anda.
- Perlindungan pengakhiran: Untuk mencegah pengakhiran yang tidak disengaja, pilih Aktifkan. Untuk informasi selengkapnya, lihat Ubah perlindungan penghentian instance.
- Perlindungan penghentian: Untuk mencegah penghentian yang tidak disengaja, pilih Aktifkan. Untuk informasi selengkapnya, lihat Aktifkan perlindungan penghentian.

- CloudWatch Pemantauan terperinci: Pilih Aktifkan untuk mengaktifkan pemantauan mendetail instans Anda menggunakan Amazon CloudWatch. Biaya tambahan berlaku. Untuk informasi selengkapnya, lihat Pantau instans Anda menggunakan CloudWatch.
- Spesifikasi kredit: Pilih Tak Terbatas agar aplikasi dapat melonjak di atas acuan selama diperlukan. Bidang ini hanya valid untuk instans T. Biaya tambahan mungkin berlaku. Untuk informasi selengkapnya, lihat Instance performa yang dapat melonjak.
- Grup penempatan: Tentukan grup penempatan untuk meluncurkan instance. Anda dapat memilih grup penempatan yang sudah ada, atau membuat grup yang baru. Tidak semua tipe instans mendukung peluncuran instans dalam grup penempatan. Untuk informasi selengkapnya, lihat Grup penempatan untuk EC2 instans Amazon Anda.
- Instans dengan pengoptimalan EBS: Instans yang dioptimalkan untuk Amazon EBS menggunakan tumpukan konfigurasi yang dioptimalkan dan menyediakan kapasitas khusus tambahan untuk I/O Amazon EBS. Jika tipe instans mendukung fitur ini, pilih Aktifkan untuk mengaktifkannya. Biaya tambahan berlaku. Untuk informasi selengkapnya, lihat the section called “Optimisasi EBS”.
- Konfigurasi bandwidth instans: Anda dapat meningkatkan bandwidth jaringan atau bandwidth EBS Anda. Hanya untuk jenis instance yang didukung. Untuk informasi selengkapnya, lihat EC2 konfigurasi pembobotan bandwidth contoh.
- Opsi pembelian: Pilih Instans Spot untuk meminta Instans Spot pada harga Spot, dibatasi pada harga Sesuai Permintaan, dan pilih opsi Sesuaikan Instans Spot untuk mengubah pengaturan Instans Spot default. Anda dapat menetapkan harga maksimum (tidak disarankan), dan mengubah tipe permintaan, durasi permintaan, dan perilaku interupsi. Jika Anda tidak meminta Instans Spot, Amazon akan EC2 meluncurkan Instans Sesuai Permintaan secara default. Untuk informasi selengkapnya, lihat Mengelola Instans Spot Anda.
- Reservasi Kapasitas: Tentukan apakah akan meluncurkan instans ke Reservasi Kapasitas apa pun yang terbuka (Open), Reservasi Kapasitas tertentu (Target berdasarkan ID), atau grup Reservasi Kapasitas (Target berdasarkan group). Untuk menentukan bahwa Reservasi Kapasitas tidak boleh digunakan, pilih Tidak Ada. Untuk informasi selengkapnya, lihat Luncurkan instans ke dalam Reservasi Kapasitas yang ada.
- Penghunian: Pilih apakah akan menjalankan instans Anda pada perangkat keras bersama (Dibagikan), perangkat keras terisolasi dan khusus (Khusus), atau pada Host Khusus (Host Khusus). Jika Anda memilih untuk meluncurkan instans ke Host Khusus, Anda dapat menentukan apakah akan meluncurkan instans ke grup sumber daya host atau Anda dapat menargetkan Host Khusus tertentu. Biaya tambahan mungkin berlaku. Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon dan Host Khusus Amazon EC.

- ID disk RAM: (Hanya berlaku untuk paravirtual (PV) AMIs) Pilih disk RAM untuk instance. Jika Anda telah memilih kernel, Anda mungkin perlu memilih RAM disk tertentu dengan driver untuk mendukungnya.
- ID Kernel: (Hanya berlaku untuk paravirtual (PV) AMIs) Pilih kernel untuk instance.
- Nitro Enclave: Memungkinkan Anda membuat lingkungan eksekusi terisolasi, yang disebut enclaves, dari instans Amazon. EC2 Pilih Aktifkan untuk mengaktifkan instance untuk AWS Nitro Enclave. Untuk informasi lebih lanjut, lihat Apa itu Enklaf AWS Nitro? di Panduan Pengguna AWS Nitro Enclave.
- Konfigurasi lisensi: Anda dapat meluncurkan instans berdasarkan konfigurasi lisensi yang ditentukan untuk melacak penggunaan lisensi Anda. Untuk informasi selengkapnya, lihat Buat konfigurasi lisensi dalam Panduan Pengguna AWS License Manager.
- Tentukan opsi CPU: Di wizard instance peluncuran, bidang ini hanya terlihat jika jenis instans yang dipilih mendukung penentuan opsi CPU. Pilih Tentukan opsi CPU untuk menentukan nomor kustom v CPUs selama peluncuran. Atur jumlah inti CPU dan thread per inti. Untuk informasi selengkapnya, lihat Opsi CPU untuk instans Amazon EC2.
- Metadata dapat diakses: Anda dapat mengaktifkan atau menonaktifkan akses ke Layanan Metadata Instans (IMDS). Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans baru.
- IPv6 Titik akhir metadata: Anda dapat mengaktifkan instance untuk menggunakan IPv6 alamat `[fd00:ec2::254]` IMDS untuk mengambil metadata instance. Opsi ini hanya tersedia jika Anda meluncurkan instance berbasis Nitro ke subnet yang IPv6 didukung -support (tumpukan ganda atau hanya). IPv6 Untuk informasi selengkapnya tentang pengambilan metadata instans, lihat Akses metadata instans untuk instans EC2.
- Versi metadata: Jika Anda mengaktifkan akses ke IMDS, Anda dapat memilih untuk meminta penggunaan Layanan Metadata Instans Versi 2 saat meminta metadata instans. Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans baru.
- Batas lompatan respons metadata: Jika Anda mengaktifkan IMDS, maka Anda dapat mengatur jumlah lompatan jaringan yang diizinkan untuk token metadata. Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans baru.
- Izinkan tanda dalam metadata: Jika Anda memilih Aktifkan, instans akan mengizinkan akses ke semua tanda dari metadatanya. Jika tidak ada nilai yang ditentukan, maka secara default, akses ke tanda dalam metadata instans tidak diperbolehkan. Untuk informasi selengkapnya, lihat Aktifkan akses ke tag dalam metadata contoh.

- Data pengguna: Anda dapat menentukan data pengguna untuk mengonfigurasi instans selama peluncuran, atau untuk menjalankan skrip konfigurasi. Untuk informasi selengkapnya tentang data pengguna untuk instance Linux, lihatJalankan perintah saat Anda meluncurkan instans EC2 dengan input data pengguna. Untuk informasi selengkapnya tentang data pengguna untuk instance Windows, lihatBagaimana Amazon EC2 menangani data pengguna untuk instans Windows.

Ringkasan

Gunakan panel Ringkasan untuk menentukan jumlah instans yang akan diluncurkan, untuk meninjau konfigurasi instans Anda, dan untuk meluncurkan instans.

- Jumlah instans: Masukkan jumlah instans yang akan diluncurkan. Semua instans akan diluncurkan dengan konfigurasi yang sama.

> **Tip**
>
> Untuk memastikan instans diluncurkan lebih cepat, bagi permintaan besar menjadi beberapa kelompok yang lebih kecil. Misalnya, buat lima permintaan peluncuran terpisah untuk masing-masing 100 instans, bukan satu permintaan peluncuran untuk 500 instans.

- (Opsional) Jika Anda menentukan lebih dari satu instance, untuk membantu memastikan bahwa Anda mempertahankan jumlah instans yang benar untuk menangani permintaan pada aplikasi Anda, Anda dapat memilih mempertimbangkan EC2 Auto Scaling untuk membuat template peluncuran dan grup Auto Scaling. Auto Scaling menskalakan jumlah instans dalam grup sesuai dengan spesifikasi Anda. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon EC2 Auto Scaling.

> **Note**
>
> Jika Amazon EC2 Auto Scaling menandai instance yang ada di grup Auto Scaling sebagai tidak sehat, instans secara otomatis dijadwalkan untuk diganti di mana instans dihentikan dan instans lainnya diluncurkan, dan Anda kehilangan data pada instans asli. Sebuah instans ditandai sebagai tidak sehat jika Anda menghentikan atau melakukan boot ulang instans, atau jika peristiwa lain menandai instans sebagai tidak sehat. Untuk informasi selengkapnya, lihat Health memeriksa instans di grup Auto Scaling di Panduan Pengguna Amazon Auto EC2 Scaling.

- Tinjau detail instans Anda, dan buat perubahan yang diperlukan. Anda dapat menavigasi langsung ke bagian dengan memilih tautannya di panel Ringkasan.
- Ketika Anda siap untuk meluncurkan instans Anda, pilih Launch instans.

Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol

Anda dapat meluncurkan instans Amazon EC2 menggunakan wizard instans peluncuran di konsol Amazon EC2. Wizard menyediakan nilai default untuk parameter peluncuran, yang dapat Anda terima atau modifikasi agar sesuai dengan kebutuhan Anda. Satu-satunya parameter yang tidak ditentukan adalah key pair. Jika Anda memilih untuk menerima nilai default, Anda dapat dengan cepat meluncurkan instance dengan memilih hanya key pair.

> **Important**
>
> Anda dikenakan biaya untuk instance saat instance dalam `running` keadaan, bahkan jika itu tetap menganggur. Namun, jika Anda memenuhi syarat untuk Tingkat Gratis, Anda mungkin tidak dikenakan biaya. Untuk informasi selengkapnya, lihat Lacak penggunaan Tingkat Gratis Anda untuk Amazon EC2.

Untuk deskripsi setiap parameter dalam wizard instance peluncuran, lihatReferensi untuk parameter konfigurasi EC2 instans Amazon.

Topik

- Meluncurkan instans dengan cepat
- Luncurkan sebuah instans menggunakan parameter yang ditentukan

Meluncurkan instans dengan cepat

Untuk menyiapkan instans dengan cepat untuk tujuan pengujian, ikuti langkah-langkah ini. Anda akan memilih sistem operasi dan pasangan kunci Anda, serta menerima nilai default. Kecuali untuk pasangan kunci, wizard peluncuran instans memberikan nilai default untuk semua parameter. Anda dapat menerima salah satu atau semua default, atau mengonfigurasi instans dengan menentukan nilai Anda sendiri untuk setiap parameter.

Untuk deskripsi setiap parameter dalam wizard instance peluncuran, lihatReferensi untuk parameter konfigurasi EC2 instans Amazon.

Untuk meluncurkan instance dengan cepat menggunakan wizard instance peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di bilah navigasi di bagian atas layar, AWS Wilayah saat ini ditampilkan (misalnya, AS Timur (Ohio)). Jika diperlukan, pilih Wilayah yang berbeda untuk meluncurkan instance.
3. Dari dasbor konsol Amazon EC2, pilih Luncurkan instans.
4. (Opsional) Pada Nama dan tanda, untuk Nama, masukkan nama deskriptif untuk instans Anda.
5. Di bawah Gambar Aplikasi dan OS (Amazon Machine Image), pilih Mulai Cepat, lalu pilih sistem operasi (OS) untuk instans Anda.
6. Di bawah Pasangan kunci (login), untuk Nama pasangan kunci, pilih pasangan kunci yang ada atau buat yang baru.
7. Di panel Ringkasan, pilih Luncurkan instans.

Luncurkan sebuah instans menggunakan parameter yang ditentukan

Jika Anda meluncurkan instance yang akan Anda gunakan dalam produksi, Anda harus mengonfigurasi instance agar sesuai dengan kebutuhan Anda. Untuk deskripsi setiap parameter dalam wizard instance peluncuran, lihatReferensi untuk parameter konfigurasi EC2 instans Amazon.

Untuk meluncurkan instance dengan mendefinisikan semua parameter peluncuran menggunakan wizard instance peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di bilah navigasi di bagian atas layar, AWS Wilayah saat ini ditampilkan (misalnya, AS Timur (Ohio)). Jika diperlukan, pilih Wilayah yang berbeda untuk meluncurkan instance.
3. Dari dasbor konsol Amazon EC2, pilih Luncurkan instans.
4. (Opsional) Di bawah Nama dan tag, untuk Nama, masukkan nama deskriptif untuk instance Anda sehingga Anda dapat dengan mudah melacaknya.

   Nama instans adalah tanda, di mana kuncinya adalah Name, dan nilainya adalah nama yang Anda tentukan.
5. Di bawah Application and OS Images (Amazon Machine Image), pilih sistem operasi (OS) untuk instans Anda, lalu pilih AMI.

   AMI adalah template yang berisi sistem operasi dan perangkat lunak yang diperlukan untuk meluncurkan instance Anda.

6. Di bawah jenis Instance, pilih jenis instance.

   Jenis instans menentukan konfigurasi perangkat keras (CPU, memori, penyimpanan, dan kapasitas jaringan) dan ukuran komputer host yang digunakan untuk instance Anda.

   Jika Anda tidak yakin jenis instance mana yang harus dipilih, Anda dapat melakukan hal berikut:

   - Pilih Bandingkan jenis instans untuk membandingkan jenis instans yang berbeda dengan atribut berikut: jumlah vCPUs, arsitektur, jumlah memori (GiB), jumlah penyimpanan (GB), jenis penyimpanan, dan kinerja jaringan.
   - Pilih Dapatkan saran untuk mendapatkan panduan dan saran untuk jenis instans dari pencari jenis instans EC2. Untuk informasi selengkapnya, lihat Dapatkan rekomendasi dari pencari tipe instans EC2.

   > **Note**
   >
   > Bergantung pada saat Anda membuat akun, Anda mungkin dapat menggunakan jenis instans secara gratis di bawah Tingkat Gratis. Jenis instans ini diberi label Tingkat gratis yang memenuhi syarat.
   > Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan usianya kurang dari 12 bulan, Anda dapat menggunakan Amazon EC2 di bawah Tingkat Gratis dengan memilih jenis instans t2.micro, atau jenis instans t3.micro di Wilayah di mana t2.micro tidak tersedia. Ketahuilah bahwa ketika Anda meluncurkan instans t3.micro, default ke mode Tidak Terbatas, yang mungkin dikenakan biaya tambahan berdasarkan penggunaan CPU.
   > Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, Anda dapat menggunakan jenis instans t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large, dan m7i-flex.large selama 6 bulan atau sampai kredit Anda habis.
   > Untuk informasi selengkapnya, lihat Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025.

7. Di bawah Pasangan kunci (login), untuk Nama pasangan kunci, pilih pasangan kunci yang sudah ada atau buat yang baru. Jika Anda tidak memerlukan key pair untuk terhubung ke instans Anda, Anda dapat memilih Proceed without a key pair (tidak disarankan).
8. Di bawah Pengaturan jaringan, Anda dapat menyimpan default jika meluncurkan instance pengujian. Jika Anda meluncurkan instans produksi, praktik terbaik adalah mengontrol lalu lintas masuk dan keluar dari instans Anda menggunakan pengaturan jaringan dan grup keamanan yang Anda tentukan.

9. Di bawah Konfigurasi penyimpanan, Anda dapat menyimpan default atau menentukan penyimpanan tambahan. AMI yang Anda pilih mencakup satu atau lebih volume penyimpanan, termasuk volume root. Anda dapat menentukan volume tambahan untuk dilampirkan ke instans.

   Anda dapat menggunakan tampilan Sederhana atau Lanjutan. Dengan tampilan Sederhana, Anda menentukan ukuran dan tipe volume. Untuk menentukan semua parameter volume, pilih tampilan Lanjutan (di kanan atas kartu).
10. Untuk detail lanjutan, perluas bagian untuk melihat bidang dan tentukan parameter tambahan apa pun untuk instance Anda.
11. Di panel Ringkasan, Anda dapat melakukan hal berikut:

    a. Tentukan jumlah instance yang akan diluncurkan.
    b. Tinjau konfigurasi instans Anda, dan arahkan langsung ke bagian dengan memilih tautannya.
    c. Ketika Anda siap untuk meluncurkan instans Anda, pilih Launch instans.

    Jika instans gagal diluncurkan atau status langsung menjadi `terminated`, bukan `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.
12. (Opsional) Anda dapat membuat peringatan penagihan untuk instans tersebut. Pada layar konfirmasi, pada Langkah Berikutnya, pilih Buat peringatan tagihan dan ikuti petunjuknya. Peringatan penagihan juga dapat dibuat setelah Anda meluncurkan instans. Untuk informasi selengkapnya, lihat Membuat alarm penagihan untuk memantau perkiraan AWS tagihan Anda di Panduan CloudWatch Pengguna Amazon.

Luncurkan instans EC2 menggunakan template peluncuran

Template peluncuran Amazon EC2 menyimpan parameter peluncuran instans sehingga Anda tidak perlu menentukannya setiap kali meluncurkan instance.

Beberapa layanan peluncuran instans secara opsional dapat menggunakan templat peluncuran saat meluncurkan instance, sedangkan untuk layanan lain, seperti Armada EC2, instance tidak dapat diluncurkan kecuali templat peluncuran digunakan. Topik ini menjelaskan cara menggunakan templat peluncuran saat meluncurkan instans menggunakan wizard peluncuran instans EC2, Amazon EC2 Auto Scaling, Armada EC2, dan Armada Spot.

Untuk informasi selengkapnya tentang template peluncuran, termasuk cara membuat template peluncuran, lihatSimpan parameter peluncuran instans di templat peluncuran Amazon EC2.

Topik

- Luncurkan instans Amazon EC2 menggunakan template peluncuran
- Luncurkan instans dalam grup Amazon EC2 Auto Scaling menggunakan template peluncuran
- Luncurkan Armada EC2 menggunakan template peluncuran
- Luncurkan Armada Spot menggunakan template peluncuran

Luncurkan instans Amazon EC2 menggunakan template peluncuran

Anda dapat menggunakan parameter yang terdapat dalam template peluncuran untuk meluncurkan instans Amazon EC2. Setelah memilih template peluncuran, tetapi sebelum meluncurkan instance, Anda dapat memodifikasi parameter peluncuran.

Instans yang diluncurkan menggunakan templat peluncuran secara otomatis diberi dua tanda dengan kunci `aws:ec2launchtemplate:id` dan `aws:ec2launchtemplate:version`. Anda tidak dapat menghapus atau mengedit tag ini.

Console

Untuk meluncurkan instance menggunakan template peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Gunakan salah satu opsi berikut untuk memilih template peluncuran:
   - Dari dasbor konsol Amazon EC2, pilih panah bawah di sebelah Launch instance, pilih Launch instance dari template, lalu untuk Source template, pilih template peluncuran.
   - Di panel navigasi, pilih Launch Templates, pilih template peluncuran, dan pilih Actions, Launch instance from template.
3. Untuk Versi templat sumber, pilih versi templat peluncuran yang akan digunakan.
4. (Opsional) Anda dapat memodifikasi nilai untuk salah satu parameter peluncuran. Jika Anda tidak mengubah nilai, nilai yang ditentukan oleh template peluncuran akan digunakan. Jika tidak ada nilai yang ditentukan dalam template peluncuran, nilai default untuk parameter digunakan.
5. Di panel Ringkasan, untuk Jumlah instance, tentukan jumlah instance yang akan diluncurkan.
6. Pilih Luncurkan instans.

   Jika instans gagal diluncurkan atau status langsung menjadi `terminated`, bukan `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

AWS CLI

Untuk meluncurkan instance dari template peluncuran

- Gunakan perintah run-instances dan tentukan parameter `--launch-template`. Secara opsional, tentukan versi templat peluncuran yang akan digunakan. Jika Anda tidak menentukan versinya, versi default akan digunakan.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Untuk mengganti parameter templat peluncuran, tentukan parameter di perintah run-instances. Contoh berikut menggantikan tipe instans yang ditentukan di templat peluncuran (jika ada).

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Jika Anda menentukan parameter bersarang yang merupakan bagian dari struktur kompleks, instans akan diluncurkan menggunakan struktur kompleks seperti yang ditentukan dalam templat peluncuran ditambah parameter bersarang tambahan yang Anda tentukan.

  Dalam contoh berikut, instans diluncurkan dengan tanda *Owner*=*TeamA* serta tanda lainnya yang ditentukan di templat peluncuran. Jika templat peluncuran sudah memiliki tanda dengan kunci *Owner*, nilainya akan diganti dengan *TeamA*.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

  Dalam contoh berikut, instans diluncurkan dengan volume dengan nama perangkat */dev/xvdb* serta pemetaan perangkat blok lainnya yang ditentukan dalam template peluncuran. Jika templat peluncuran sudah memiliki volume yang ditentukan untuk */dev/xvdb*, nilainya akan diganti dengan nilai yang ditentukan.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --block-device-mappings "DeviceName=/dev/
xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Jika instance gagal diluncurkan atau status langsung beralih ke `terminated` dari pada `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

PowerShell

Untuk meluncurkan instance dari template peluncuran menggunakan AWS Tools for PowerShell

- Gunakan perintah New-EC2Instance dan tentukan parameter `-LaunchTemplate`. Secara opsional, tentukan versi templat peluncuran yang akan digunakan. Jika Anda tidak menentukan versinya, versi default akan digunakan.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Untuk mengganti parameter template peluncuran, tentukan parameter dalam New-EC2Instanceperintah. Contoh berikut menggantikan tipe instans yang ditentukan di templat peluncuran (jika ada).

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Jika Anda menentukan parameter bersarang yang merupakan bagian dari struktur kompleks, instans akan diluncurkan menggunakan struktur kompleks seperti yang ditentukan dalam templat peluncuran ditambah parameter bersarang tambahan yang Anda tentukan.

Dalam contoh berikut, instans diluncurkan dengan tanda *Owner*=*TeamA* serta tanda lainnya yang ditentukan di templat peluncuran. Jika templat peluncuran sudah memiliki tanda dengan kunci *Owner*, nilainya akan diganti dengan *TeamA*.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

Dalam contoh berikut, instans diluncurkan dengan volume dengan nama perangkat */dev/xvdb* serta pemetaan perangkat blok lainnya yang ditentukan dalam template peluncuran. Jika templat peluncuran sudah memiliki volume yang ditentukan untuk */dev/xvdb*, nilainya akan diganti dengan nilai yang ditentukan.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
```

```
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Jika instance gagal diluncurkan atau status langsung beralih ke `terminated` dari pada `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

Luncurkan instans dalam grup Amazon EC2 Auto Scaling menggunakan template peluncuran

Anda dapat membuat grup Auto Scaling dan menentukan templat peluncuran yang akan digunakan untuk grup tersebut. Saat Amazon EC2 Auto Scaling meluncurkan instans di grup Auto Scaling, layanan ini menggunakan parameter peluncuran yang ditentukan di templat peluncuran terkait.

Sebelum Anda dapat membuat grup Auto Scaling menggunakan template peluncuran, Anda harus terlebih dahulu membuat template peluncuran yang menyertakan parameter yang diperlukan untuk meluncurkan instance dalam grup Auto Scaling. Beberapa parameter diperlukan, seperti ID AMI, dan beberapa parameter tidak tersedia untuk digunakan dengan grup Auto Scaling. Konsol menyediakan panduan untuk membantu Anda membuat template yang dapat Anda gunakan dengan Amazon EC2 Auto Scaling.

Untuk membuat grup Auto Scaling dengan template peluncuran menggunakan konsol

- Untuk petunjuknya, lihat Membuat grup Auto Scaling menggunakan templat peluncuran di Panduan Pengguna Amazon EC2 Auto Scaling.

Untuk membuat atau memperbarui grup Auto Scaling dengan template peluncuran menggunakan AWS CLI

- Gunakan update-auto-scaling-groupperintah create-auto-scaling-groupatau dan tentukan `--launch-template` parameternya.

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna Amazon EC2 Auto Scaling:

- Buat templat peluncuran untuk grup Auto Scaling
- Buat template peluncuran menggunakan pengaturan lanjutan
- Contoh untuk membuat dan mengelola template peluncuran dengan AWS Command Line Interface (AWS CLI) — Memberikan contoh yang menunjukkan cara membuat template peluncuran dengan berbagai kombinasi parameter.
- Buat grup Auto Scaling menggunakan template peluncuran
- Memperbarui grup Auto Scaling

Luncurkan Armada EC2 menggunakan template peluncuran

Template peluncuran adalah persyaratan saat membuat permintaan Armada EC2. Saat Amazon EC2 memenuhi permintaan Armada EC2, layanan ini menggunakan parameter peluncuran yang ditentukan di templat peluncuran terkait. Anda dapat mengganti beberapa parameter yang ditentukan di templat peluncuran. Untuk informasi selengkapnya, lihat Membuat Armada EC2.

Untuk membuat Armada EC2 dengan template peluncuran menggunakan AWS CLI

- Gunakan perintah create-fleet. Gunakan parameter `--launch-template-configs` untuk menentukan templat peluncuran dan setiap penggantian untuk templat peluncuran.

Luncurkan Armada Spot menggunakan template peluncuran

Template peluncuran bersifat opsional saat membuat permintaan Spot Fleet. Jika Anda tidak menggunakan template peluncuran, Anda dapat menentukan parameter peluncuran secara manual. Jika Anda menggunakan templat peluncuran, saat Amazon EC2 memenuhi permintaan Armada Spot, templat tersebut menggunakan parameter peluncuran yang ditentukan dalam templat peluncuran terkait. Anda dapat mengganti beberapa parameter yang ditentukan di templat peluncuran. Untuk informasi selengkapnya, lihat Membuat Armada Spot.

Untuk membuat permintaan Spot Fleet menggunakan template peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih Minta Instans Spot.
4. Di bawah Parameter peluncuran, pilih Gunakan templat peluncuran.

5. Untuk Templat peluncuran, pilih templat peluncuran, dan kemudian, dari bidang ke kanan, pilih versi templat peluncuran.
6. Konfigurasikan Armada Spot Anda dengan memilih opsi yang berbeda di layar ini. Untuk informasi lebih lanjut tentang opsi, lihat Membuat permintaan Armada Spot menggunakan parameter yang ditentukan.
7. Saat Anda siap membuat Armada Spot, pilih Luncurkan.

Untuk membuat permintaan Spot Fleet menggunakan template peluncuran

- Gunakan perintah request-spot-fleet. Gunakan parameter `LaunchTemplateConfigs` untuk menentukan templat peluncuran dan setiap penggantian untuk templat peluncuran.

Luncurkan instans EC2 menggunakan detail dari instans yang ada

Konsol Amazon EC2 menyediakan opsi Lincurkan lebih banyak seperti ini yang memungkinkan Anda menggunakan instans saat ini sebagai dasar untuk meluncurkan instans lainnya. Opsi ini secara otomatis mengisi wizard peluncuran instans Amazon EC2 dengan detail konfigurasi tertentu dari instans yang dipilih.

Pertimbangan-pertimbangan

- Kami tidak mengklonakan instans Anda; kami hanya mereplikasi beberapa detail konfigurasi. Untuk membuat salinan instans Anda, pertama-tama buat AMI darinya, lalu luncurkan lebih banyak instans dari AMI. Buat templat peluncuran untuk memastikan bahwa Anda meluncurkan instans menggunakan detail peluncuran yang sama.
- Instans saat ini harus berada dalam status `running`.

Detail yang disalin

Detail konfigurasi berikut disalin dari instans yang dipilih dari wizard peluncuran instans:

- ID AMI
- Jenis instans
- Zona Ketersediaan, atau VPC dan subnet tempat instans yang dipilih berada

- IPv4 Alamat publik. Jika instance yang dipilih saat ini memiliki IPv4 alamat publik, instans baru menerima IPv4 alamat publik, terlepas dari pengaturan IPv4 alamat publik default instans yang dipilih. Untuk informasi selengkapnya tentang IPv4 alamat publik, lihatIPv4 Alamat publik.
- Grup penempatan, jika ada
- Peran IAM yang terkait dengan instans, jika berlaku
- Pengaturan perilaku pematian (berhenti atau berakhir)
- Pengaturan perlindungan pemutusan hubungan kerja (benar atau salah)
- CloudWatch pemantauan (diaktifkan atau dinonaktifkan)
- Pengaturan pengoptimalan Amazon EBS (benar atau salah)
- Pengaturan penghunian, jika diluncurkan ke VPC (bersama atau khusus)
- ID Kernel dan ID disk RAM, jika ada
- Data pengguna, jika ditentukan
- Tanda yang terkait dengan instans, jika ada
- Grup keamanan yang terkait dengan instans
- [Contoh Windows] Informasi asosiasi. Jika instans yang dipilih dikaitkan dengan file konfigurasi, file yang sama secara otomatis dikaitkan dengan instans baru. Jika file konfigurasi menyertakan konfigurasi domain gabungan, instans baru akan digabungkan ke domain yang sama. Untuk informasi selengkapnya tentang bergabung dengan domain, lihat Menggabungkan instans Windows EC2 dengan mulus ke Direktori Aktif AWS Microsoft AD Terkelola dalam Panduan AWS Directory Service Administrasi.

Detail tidak disalin

Detail konfigurasi berikut tidak disalin dari instans yang Anda pilih. Sebaliknya, wizard menerapkan pengaturan atau perilaku default mereka:

- Jumlah antarmuka jaringan – Default-nya adalah satu antarmuka jaringan, yang merupakan antarmuka jaringan utama (eth0).
- Penyimpanan – Konfigurasi penyimpanan default ditentukan oleh AMI dan tipe instans.

Untuk meluncurkan lebih banyak instans seperti instans yang ada

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.

3. Pilih instans, lalu pilih Tindakan, Gambar dan templat, Luncurkan lebih banyak yang seperti ini.
4. Wizard peluncuran instans akan terbuka. Anda dapat membuat perubahan yang diperlukan pada konfigurasi instans dengan memilih opsi yang berbeda di layar ini.

   Ketika Anda siap untuk meluncurkan instans Anda, pilih Luncurkan instans.
5. Jika instans gagal diluncurkan atau status langsung menjadi `terminated`, bukan `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

Luncurkan instans Amazon EC2 dari AMI AWS Marketplace

Anda dapat berlangganan AWS Marketplace AMI dan meluncurkan instance darinya menggunakan konsol Amazon EC2 atau alat baris perintah. Untuk informasi lebih lanjut tentang AWS Marketplace AMIs, lihatAMIs Dibayar AWS Marketplace untuk instans Amazon EC2.

Untuk membatalkan langganan AMI setelah peluncuran, Anda harus terlebih dahulu menghentikan semua instance yang diluncurkan dari AMI. Untuk informasi selengkapnya, lihat Kelola AWS Marketplace langganan Anda.

Untuk meluncurkan instance dari AWS Marketplace AMI menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari dasbor konsol Amazon EC2, pilih Luncurkan instans.
3. (Opsional) Pada Nama dan tanda, untuk Nama, masukkan nama deskriptif untuk instans Anda.
4. Di bawah Application and OS Images (Amazon Machine Image) AMIs, pilih Browse more, lalu pilih AWS Marketplace AMIstab. Temukan AMI yang sesuai dengan menelusuri kategori, atau menggunakan fungsi pencarian. Untuk memilih produk, pilih Pilih.
5. Sebuah jendela terbuka dengan ikhtisar produk yang Anda pilih. Anda dapat melihat informasi harga, serta informasi lain yang disediakan vendor. Saat Anda siap, pilih Berlangganan dan luncurkan. Ini akan segera memulai langganan Anda. Saat berlangganan sedang berlangsung, Anda dapat mengonfigurasi instance dengan melanjutkan langkah-langkah dalam prosedur ini. Jika ada masalah dengan detail kartu kredit Anda, Anda akan diminta untuk memperbarui detail akun Anda.

> **Note**
>
> Anda tidak dikenai biaya untuk menggunakan produk hingga Anda meluncurkan instans dengan AMI. Catat harga untuk setiap tipe instans yang didukung saat Anda memilih tipe instans. Pajak tambahan mungkin juga berlaku pada produk.

6. Untuk Tipe instans, pilih tipe instans untuk instans Anda. Tipe instans menentukan konfigurasi perangkat keras dan ukuran instans yang akan diluncurkan.
7. Di bawah Pasangan kunci (login), untuk Nama pasangan kunci, pilih pasangan kunci yang ada atau buat yang baru.
8. Di bawah Pengaturan Jaringan, untuk Firewall (grup keamanan), perhatikan grup keamanan baru yang dibuat sesuai dengan spesifikasi vendor untuk produk tersebut. Grup keamanan mungkin menyertakan aturan yang memungkinkan semua IPv4 alamat (`0.0.0.0/0`) akses pada SSH (port 22) di Linux atau RDP (port 3389) pada Windows. Kami menyarankan Anda menyesuaikan aturan ini untuk mengizinkan hanya alamat atau rentang alamat tertentu yang bisa mengakses instans Anda melalui port tersebut.
9. Anda dapat menggunakan bidang lain di layar untuk mengonfigurasi instans Anda, menambahkan penyimpanan, dan menambahkan tanda. Untuk informasi tentang berbagai opsi yang dapat Anda konfigurasikan, lihat Referensi untuk parameter konfigurasi EC2 instans Amazon.
10. Di panel Ringkasan, pada Gambar Perangkat Lunak (AMI), periksa detail AMI tempat Anda akan meluncurkan instans. Periksa juga detail konfigurasi lain yang Anda tentukan. Ketika Anda siap untuk meluncurkan instans Anda, pilih Launch instans.
11. Tergantung pada produk langganan Anda, instans mungkin memerlukan waktu beberapa menit atau lebih untuk diluncurkan. Jika ada masalah dengan detail kartu kredit Anda, Anda akan diminta untuk memperbarui detail akun Anda. Saat halaman konfirmasi peluncuran ditampilkan, pilih Lihat semua instans untuk membuka halaman Instans.

> **Note**
>
> Anda akan dikenai harga langganan selama instans Anda dalam status `running`, meskipun sedang idle. Jika instans Anda dihentikan, Anda mungkin masih dikenai biaya untuk penyimpanan.

12. Saat instans Anda ada dalam status `running`, Anda dapat menyambungkannya. Untuk melakukan ini, pilih instans Anda di daftar, pilih Hubungkan, dan pilih opsi koneksi. Untuk informasi selengkapnya tentang terhubung ke instans Anda, lihat Connect ke instans EC2.

    > **Important**
    >
    > Periksa petunjuk penggunaan vendor dengan hati-hati, karena Anda mungkin perlu menggunakan nama pengguna tertentu untuk terhubung ke instans Anda. Untuk informasi tentang mengakses detail langganan Anda, lihat Kelola AWS Marketplace langganan Anda.

13. Jika instans gagal diluncurkan atau status langsung menjadi `terminated`, bukan `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

Untuk meluncurkan instance dari AWS Marketplace AMI menggunakan alat baris perintah

Untuk meluncurkan instance dari AWS Marketplace produk menggunakan alat baris perintah, pertama-tama pastikan bahwa Anda berlangganan produk. Anda kemudian dapat meluncurkan sebuah instans dengan ID AMI produk menggunakan metode berikut:

Metode	Dokumentasi
AWS CLI	Gunakan perintah run-instance, atau lihat topik berikut untuk informasi selengkapnya: Luncurkan instance Anda di Panduan Pengguna.AWS Command Line Interface
AWS Tools for Windows PowerShell	Gunakan New-EC2Instanceperintah, atau lihat topik berikut untuk informasi selengkapnya: Luncurkan Instans Amazon EC2 Menggunakan Windows PowerShell
API Kueri	MenggunakanRunInstances permintaan.

Connect ke instans EC2

Instans Amazon EC2 Anda adalah server virtual di file. AWS Cloud Untuk masuk ke instans Anda, Anda harus membuat koneksi ke instance. Bagaimana Anda terhubung ke instans Anda tergantung

pada sistem operasi instance dan sistem operasi pada komputer yang Anda gunakan untuk terhubung ke instance. Tabel berikut merinci persyaratan untuk setiap metode koneksi.

Opsi koneksi	Sistem operasi instans	Aturan lalu lintas masuk	Izin IAM	Peran profil instance	Perangkat lunak pada contoh	Perangkat lunak pada sistem penghubung	Pasangan kunci
Klien SSH	Linux	Ya	Tidak	Tidak	Tidak	Ya	Ya
EC2 Instance Connect	Linux	Ya	Ya	Tidak	Ya [1]	Tidak	Tidak
PuTTY	Linux	Ya	Tidak	Tidak	Tidak	Ya	Ya
Klien RDP	Windows	Ya	Tidak	Tidak	Tidak	Ya	Ya [1]
Fleet Manager	Windows	Tidak	Ya	Ya	Ya [1]	Tidak	Ya
Manajer Sesi	Linux, Windows	Tidak	Ya	Ya	Ya [1]	Tidak	Tidak
Titik Akhir EC2 Instance Connect	Linux, Windows	Ya	Ya	Tidak	Tidak	Tidak	Tidak ada [3]

[1] Perangkat lunak yang diperlukan hanya pra-instal pada tertentu AMIs. Anda dapat menginstal perangkat lunak yang diperlukan secara manual sesuai kebutuhan pada sistem operasi yang didukung.

[2] Key pair hanya diperlukan jika Anda menggunakan kata sandi yang dibuat secara acak untuk akun pengguna Administrator lokal.

[3] Sebuah key pair diperlukan jika Anda menggunakan metode koneksi SSH.

Untuk informasi selengkapnya, lihat dokumentasi untuk opsi koneksi yang ingin Anda gunakan.

Opsi koneksi

- Hubungkan ke instans Linux Anda menggunakan klien SSH
- Connect ke instans Linux Anda menggunakan Putty
- Connect ke instans Windows Anda menggunakan klien RDP
- Hubungkan ke instans Windows Anda menggunakan Fleet Manager
- Terhubung menggunakan Session Manager
- Connect menggunakan IP publik dan EC2 Instance Connect
- Connect menggunakan IP pribadi dan EC2 Instance Connect Endpoint

Prasyarat koneksi umum

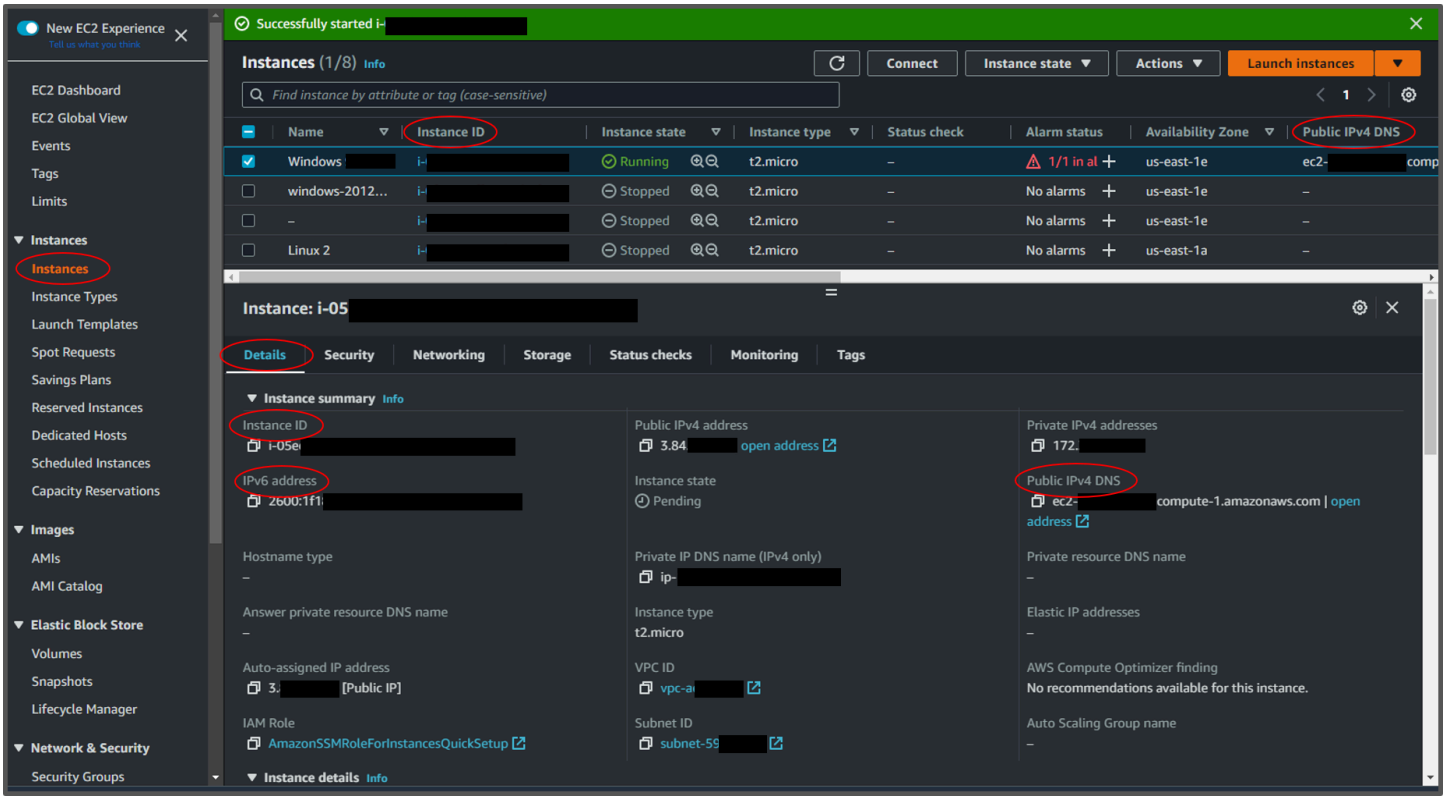
Berikut ini adalah prasyarat umum untuk terhubung ke sebuah instance. Perhatikan bahwa mungkin ada prasyarat tambahan yang khusus untuk opsi koneksi yang Anda pilih.

Prasyarat umum

- Periksa apakah pesan Anda telah lulus pemeriksaan statusnya. Diperlukan beberapa menit agar sebuah instans siap menerima permintaan koneksi. Untuk informasi selengkapnya, lihat Melihat pemeriksaan status.
- Dapatkan detail instance yang diperlukan.
- Temukan kunci pribadi dan atur izin.
- (Opsional) Dapatkan sidik jari instans.

Dapatkan detail instance yang diperlukan

Untuk mempersiapkan untuk terhubung ke instans Anda, dapatkan informasi berikut dari konsol Amazon EC2 atau dengan menggunakan baris perintah.



- Dapatkan nama DNS publik dari instans tersebut.

  Anda dapat memperoleh alamat DNS publik untuk instans Anda dari konsol Amazon EC2. Periksa kolom IPv4 DNS Publik panel Instans. Jika kolom ini disembunyikan, pilih ikon pengaturan ( ) di sudut kanan atas layar, dan pilih IPv4 DNS Publik. Anda juga dapat menemukan DNS publik di bagian informasi instans pada panel Instans. Saat Anda memilih instans di panel Instans konsol Amazon EC2, informasi tentang instans tersebut akan muncul di bagian bawah halaman. Di bawah tab Detail, cari IPv4DNS Publik.

  Jika mau, Anda dapat menggunakan perintah describe-instance (AWS CLI) atau Get-EC2Instance().AWS Tools for Windows PowerShell

  Jika tidak ada IPv4 DNS Publik yang ditampilkan, verifikasi bahwa status Instans sedang Berjalan, dan Anda belum meluncurkan instance di subnet pribadi. Jika meluncurkan instans menggunakan wizard peluncuran instans, Anda mungkin telah mengedit bidang Tetapkan otomatis IP publik pada Pengaturan jaringan dan mengubah nilainya menjadi Nonaktifkan. Jika Anda menonaktifkan opsi Tetapkan otomatis IP publik, instans tidak diberi alamat IP publik saat diluncurkan.
- (IPv6 hanya contoh) Dapatkan IPv6 alamat instance.

Jika Anda telah menetapkan alamat IPv6 untuk instans Anda, maka Anda dapat secara opsional ter-connect ke instans menggunakan alamat IPv6-nya, bukan alamat IPv4 publik atau nama host DNS IPv4 publik. Komputer lokal Anda harus mempunyai alamat IPv6 dan harus dikonfigurasi untuk menggunakan IPv6. Anda dapat memperoleh alamat IPv6 instans Anda dari konsol Amazon EC2. Periksa IPv6 IPskolom panel Instances. Atau, Anda dapat menemukan IPv6 alamatnya di bagian informasi instance. Saat Anda memilih instans di panel Instans konsol Amazon EC2, informasi tentang instans tersebut akan muncul di bagian bawah halaman. Di bawah tab Detail, cari IPv6alamat.

Jika mau, Anda dapat menggunakan perintah describe-instance (AWS CLI) atau Get-EC2Instance().AWS Tools for Windows PowerShell Untuk informasi lebih lanjut tentang IPv6, lihatIPv6 alamat.

- (Instance Linux) Dapatkan nama pengguna untuk instans Anda.

  Anda dapat terhubung ke instans menggunakan nama pengguna untuk akun pengguna Anda atau nama pengguna default untuk AMI yang Anda gunakan untuk meluncurkan instans Anda.

  - Dapatkan nama pengguna untuk akun pengguna Anda.

    Untuk informasi selengkapnya tentang cara membuat akun pengguna, lihat Kelola pengguna sistem di instans Amazon EC2 Linux Anda.

  - Dapatkan nama pengguna default untuk AMI yang Anda gunakan untuk meluncurkan instans Anda.

    - Amazon Linux - `ec2-user`
    - CentOS — atau `centos` `ec2-user`
    - Debian — `admin`
    - Fedora — atau `fedora` `ec2-user`
    - FreeBSD — `ec2-user`
    - RHEL — `ec2-user` atau `root`
    - SUSE — `ec2-user` atau `root`
    - Ubuntu — `ubuntu`
    - Oracle – `ec2-user`
    - Bitnami — `bitnami`
    - Linux berbatu — `rocky`
    - Lainnya — Periksa dengan penyedia AMI

Temukan kunci pribadi dan atur izin

Anda harus mengetahui lokasi file kunci pribadi Anda untuk membuat koneksi awal ke instance Linux menggunakan SSH atau instance Windows menggunakan RDP. Untuk koneksi SSH, Anda harus mengatur izin file sehingga hanya Anda yang dapat membaca kunci pribadi.

Untuk informasi tentang cara kerja pasangan kunci saat menggunakan Amazon EC2, lihat Pasangan kunci Amazon EC2 dan instans Amazon EC2.

- Temukan kunci pribadi.

  Dapatkan jalur yang memenuhi semua syarat ke lokasi di komputer Anda dari file `.pem` untuk pasangan kunci yang Anda tentukan saat meluncurkan instans. Untuk informasi selengkapnya, lihat the section called “Mengidentifikasi kunci publik yang ditentukan saat peluncuran”.

  Jika Anda tidak dapat menemukan file kunci pribadi Anda, lihat Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance saya?

  (Instance Linux) Jika Anda terhubung ke instans Anda menggunakan PuTTY dan perlu mengonversi file `.pem` `.ppk` ke, lihat. Konversikan kunci pribadi Anda menggunakan Pu TTYgen

- (Instance Linux) Atur izin kunci pribadi Anda sehingga hanya Anda yang dapat membacanya.
  - Hubungkan dari macOS atau Linux

    Jika Anda berencana menggunakan klien SSH pada komputer macOS atau Linux untuk terhubung ke instans Linux, gunakan perintah berikut untuk mengatur izin file kunci privat Anda sehingga hanya Anda yang dapat membacanya.

    ```
    chmod 400 key-pair-name.pem
    ```

    Jika Anda tidak mengatur izin tersebut, Anda tidak akan dapat terhubung ke instans Anda menggunakan pasangan kunci ini. Untuk informasi selengkapnya, lihat Kesalahan: File kunci privat yang tidak dilindungi.

  - Hubungkan dari Windows

    Buka File Explorer dan klik kanan pada `.pem` file tersebut. Pilih Properties > Security tab dan pilih Advanced. Pilih Nonaktifkan warisan. Hapus akses ke semua pengguna kecuali untuk pengguna saat ini.

(Opsional) Dapatkan sidik jari instans

Untuk melindungi diri dari man-in-the-middle serangan, Anda dapat memverifikasi keaslian instance yang akan Anda sambungkan dengan memverifikasi sidik jari yang ditampilkan. Memverifikasi sidik jari berguna jika Anda meluncurkan instans dari AMI publik yang disediakan oleh pihak ketiga.

Gambaran umum tugas

Pertama, dapatkan sidik jari instance dari instance. Kemudian, ketika Anda terhubung ke instance dan diminta untuk memverifikasi sidik jari, bandingkan sidik jari yang Anda peroleh dalam prosedur ini dengan sidik jari yang ditampilkan. Jika sidik jari tidak cocok, seseorang mungkin mencoba menyerang. man-in-the-middle Jika cocok, Anda dapat dengan percaya diri terhubung ke instans Anda.

Prasyarat untuk mendapatkan sidik jari instans

- Instans tidak boleh dalam status `pending`. Sidik jari hanya tersedia setelah boot pertama instans selesai.
- Anda harus menjadi pemilik instans untuk mendapatkan output konsol.
- Ada berbagai cara untuk mendapatkan sidik jari instance. Jika Anda ingin menggunakan AWS CLI, itu harus diinstal pada komputer lokal Anda. Untuk informasi tentang menginstal AWS CLI, lihat Memulai dengan AWS CLI di Panduan AWS Command Line Interface Pengguna.

Untuk mendapatkan sidik jari instans

Pada Langkah 1, Anda mendapatkan output konsol, yang mencakup sidik jari instance. Pada Langkah 2, Anda menemukan sidik jari instance di output konsol.

1. Dapatkan output konsol menggunakan salah satu metode berikut.

   Console

   1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
   2. Dari navigator kiri, pilih Instans.
   3. Pilih instance Anda, lalu pilih Actions, Monitor dan troubleshoot, Dapatkan log sistem.

AWS CLI

Di komputer lokal Anda (bukan pada instance yang Anda sambungkan), gunakan get-console-outputperintah. Jika outputnya besar, Anda dapat menyalurkannya ke file teks, yang mungkin lebih mudah dibaca.

```
aws ec2 get-console-output \
    --instance-id i-1234567890abcdef0 \
    --query Output \
    --output text > temp.txt
```

PowerShell

Di komputer lokal Anda, gunakan Get-EC2ConsoleOutputcmdlet berikut.

```
$encodedOutput = (Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0).Output
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encodedOutput
```

2. Dalam output konsol, temukan sidik jari instance (host), yang terletak di bawah`BEGIN SSH HOST KEY FINGERPRINTS`. Mungkin ada beberapa contoh sidik jari. Ketika Anda terhubung ke instans Anda, itu hanya akan menampilkan salah satu sidik jari.

   Output yang tepat dapat bervariasi menurut sistem operasi, versi AMI, dan apakah AWS dibuat pasangan kunci. Berikut ini adalah output contoh.

```
ec2:#############################################################
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #############################################################
```

> **Note**
>
> Anda akan mereferensikan sidik jari ini saat Anda terhubung ke instance.

Hubungkan ke instans Linux Anda, menggunakan SSH.

Ada beberapa cara untuk terhubung ke instance Linux Anda menggunakan SSH. Beberapa cara tergantung pada sistem operasi komputer lokal yang Anda sambungkan. Metode lain berbasis browser, seperti Instance EC2 Connect atau AWS Systems Manager Session Manager, dan dapat digunakan dari komputer manapun. Anda dapat menggunakan SSH untuk terhubung ke instance Linux Anda dan menjalankan perintah, atau menggunakan SSH untuk mentransfer file antara komputer lokal Anda dan instance Anda.

Sebelum Anda terhubung ke instans Linux Anda menggunakan SSH, lengkapi prasyarat berikut:

- Periksa apakah pesan Anda telah lulus pemeriksaan statusnya. Diperlukan beberapa menit agar sebuah instans siap menerima permintaan koneksi. Untuk informasi selengkapnya, lihat Melihat pemeriksaan status.
- Pastikan grup keamanan yang terkait dengan instans Anda mengizinkan lalu lintas SSH masuk dari alamat IP Anda. Untuk informasi selengkapnya, lihat Aturan-aturan untuk terhubung ke instans dari komputer Anda.
- Dapatkan detail instance yang diperlukan.
- Temukan kunci pribadi dan atur izin.
- (Opsional) Dapatkan sidik jari instans.

Kemudian, pilih salah satu opsi berikut untuk terhubung ke instance Linux Anda menggunakan SSH.

- Connect menggunakan klien SSH
- Connect menggunakan PuTTY
- Transfer file menggunakan SCP

Jika Anda tidak dapat terhubung ke instans dan memerlukan bantuan pemecahan masalah, lihat. Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda

Hubungkan ke instans Linux Anda menggunakan klien SSH

Anda dapat menggunakan Secure Shell (SSH) untuk terhubung ke instance Linux Anda dari komputer lokal Anda. Untuk informasi selengkapnya tentang opsi lain, lihatConnect ke instans EC2.

> **Note**
>
> Jika Anda menerima kesalahan saat mencoba terhubung ke instans Anda, pastikan instans Anda memenuhi semua. Prasyarat koneksi SSH Jika memenuhi semua prasyarat, dan Anda masih tidak dapat terhubung ke instans Linux Anda, lihat Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda.

Daftar Isi

- Prasyarat koneksi SSH
- Hubungkan ke instans Linux Anda menggunakan klien SSH

Prasyarat koneksi SSH

Sebelum Anda dapat terhubung ke instance Linux Anda menggunakan SSH, selesaikan tugas-tugas berikut.

Lengkapi prasyarat umum.

- Periksa apakah pesan Anda telah lulus pemeriksaan statusnya. Diperlukan beberapa menit agar sebuah instans siap menerima permintaan koneksi. Untuk informasi selengkapnya, lihat Melihat pemeriksaan status.
- Dapatkan detail instance yang diperlukan.
- Temukan kunci pribadi dan atur izin.
- (Opsional) Dapatkan sidik jari instans.

Izinkan lalu lintas SSH masuk dari alamat IP Anda.

Pastikan grup keamanan yang terkait dengan instans Anda mengizinkan lalu lintas SSH masuk dari alamat IP Anda. Untuk informasi selengkapnya, lihat Aturan-aturan untuk terhubung ke instans dari komputer Anda.

Instal klien SSH di komputer lokal Anda (jika diperlukan).

Komputer lokal Anda kemungkinan telah menginstal klien SSH secara default. Anda dapat memverifikasi ini dengan memasukkan perintah berikut di jendela terminal. Jika komputer Anda tidak mengenali perintah, Anda harus menginstal klien SSH.

```
ssh
```

Berikut ini adalah beberapa opsi yang memungkinkan untuk Windows. Jika komputer Anda menjalankan sistem operasi yang berbeda, lihat dokumentasi untuk sistem operasi tersebut untuk opsi klien SSH.

Instal OpenSSH di Windows

Setelah Anda menginstal OpenSSH pada Windows, Anda dapat terhubung ke instance Linux Anda dari komputer Windows Anda menggunakan SSH. Sebelum Anda mulai, pastikan Anda memenuhi persyaratan berikut.

Versi Windows

Versi Windows di komputer Anda harus Windows Server 2019 atau yang lebih baru.

Untuk versi Windows yang lebih lama, unduh dan instal Win32-OpenSSH sebagai gantinya.

PowerShell persyaratan

Untuk menginstal OpenSSH di OS Windows Anda PowerShell menggunakan, Anda harus PowerShell menjalankan versi 5.1 atau yang lebih baru, dan akun Anda harus menjadi anggota grup Administrator bawaan. Jalankan `$PSVersionTable.PSVersion` dari PowerShell untuk memeriksa PowerShell versi Anda.

Untuk memeriksa apakah Anda anggota grup Administrator bawaan, jalankan PowerShell perintah berikut:

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Jika Anda adalah anggota grup Administrator bawaan, output-nya adalah `True`.

Untuk menginstal OpenSSH untuk Windows PowerShell menggunakan, jalankan perintah berikut. PowerShell

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Berikut ini adalah output contoh.

```
Path          :
Online        : True
```

```
RestartNeeded : False
```

Untuk menghapus OpenSSH dari Windows PowerShell menggunakan, jalankan perintah berikut. PowerShell

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Berikut ini adalah output contoh.

```
Path          :
Online        : True
RestartNeeded : True
```

Instal Subsistem Windows untuk Linux (WSL)

Setelah Anda menginstal WSL pada Windows, Anda dapat terhubung ke instance Linux Anda dari komputer Windows Anda menggunakan alat baris perintah Linux, seperti klien SSH.

Ikuti petunjuk dalam Instal Windows Subsystem untuk Linux pada instans EC2 Windows Anda. Jika Anda mengikuti petunjuk dalam panduan instalasi Microsoft, mereka menginstal distribusi Ubuntu Linux. Anda dapat menginstal distribusi Linux yang berbeda jika Anda mau.

Di jendela terminal WSL, salin `.pem` file (untuk key pair yang Anda tentukan untuk instance Anda saat peluncuran) dari Windows ke WSL. Perhatikan jalur yang sepenuhnya memenuhi syarat ke file `.pem` di WSL untuk digunakan saat menghubungkan ke instans Anda. Untuk informasi tentang cara menentukan jalur ke hard drive Windows Anda, lihat Bagaimana cara mengakses drive C saya?.

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Untuk informasi tentang membongkar Subsistem Windows untuk Linux, lihat Bagaimana cara membongkar Distribusi WSL?.

Hubungkan ke instans Linux Anda menggunakan klien SSH

Gunakan prosedur berikut untuk terhubung ke instans Linux Anda menggunakan klien SSH.

Untuk terhubung ke instans Anda menggunakan klien SSH

1. Buka jendela terminal di komputer Anda.
2. Gunakan ssh perintah untuk terhubung ke instance. Anda memerlukan detail tentang contoh Anda yang Anda kumpulkan sebagai bagian dari prasyarat. Misalnya, Anda memerlukan lokasi

kunci pribadi (`.pem`file), nama pengguna, dan nama atau IPv6 alamat DNS publik. Berikut ini adalah contoh perintah.

- (DNS Publik) Untuk menggunakan nama DNS publik, masukkan perintah berikut.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Atau, jika instance Anda memiliki IPv6 alamat, masukkan perintah berikut untuk menggunakan IPv6 alamat tersebut.

```
ssh -i /path/key-pair-name.pem instance-user-name@2001:db8::1234:5678:1.2.3.4
```

Berikut ini adalah contoh respons.

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

3. (Opsional) Verifikasi bahwa sidik jari dalam peringatan keamanan cocok dengan sidik jari. Jika sidik jari ini tidak cocok, seseorang mungkin mencoba menyerang. man-in-the-middle Jika cocok, lanjutkan ke langkah berikutnya. Untuk informasi selengkapnya, lihat Mendapatkan sidik jari instance.
4. Masukkan **`yes`**.

   Anda akan melihat tanggapan seperti berikut:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Connect ke instans Linux Anda menggunakan Putty

Anda dapat terhubung ke instance Linux Anda menggunakan PuTTY, klien SSH gratis untuk Windows.

Jika Anda menjalankan Windows Server 2019 atau yang lebih baru, kami sarankan Anda menggunakan OpenSSH, alat konektivitas open source untuk login jarak jauh menggunakan protokol SSH.

> **Note**
>
> Jika Anda menerima kesalahan saat mencoba terhubung ke instans Anda, pastikan instans Anda memenuhi semua. Prasyarat koneksi SSH Jika memenuhi semua prasyarat, dan Anda masih tidak dapat terhubung ke instans Linux Anda, lihat Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda.

Daftar Isi

- Prasyarat
- (Opsional) Konversi kunci pribadi Anda menggunakan Pu TTYgen
- Hubungkan ke instans Linux Anda

Prasyarat

Sebelum Anda terhubung ke instance Linux Anda menggunakan PuTTY, selesaikan tugas-tugas berikut.

Lengkapi prasyarat umum.

- Periksa apakah pesan Anda telah lulus pemeriksaan statusnya. Diperlukan beberapa menit agar sebuah instans siap menerima permintaan koneksi. Untuk informasi selengkapnya, lihat Melihat pemeriksaan status.
- Dapatkan detail instance yang diperlukan.
- Temukan kunci pribadi dan atur izin.
- (Opsional) Dapatkan sidik jari instans.

Izinkan lalu lintas SSH masuk dari alamat IP Anda.

Pastikan grup keamanan yang terkait dengan instans Anda mengizinkan lalu lintas SSH masuk dari alamat IP Anda. Untuk informasi selengkapnya, lihat Aturan-aturan untuk terhubung ke instans dari komputer Anda.

Instal PuTTY di komputer lokal Anda (jika perlu).

Unduh dan pasang PuTTY dari halaman unduhan PuTTY. Jika Anda sudah memiliki versi PuTTY sebelumnya yang terpasang, kami merekomendasikan Anda mengunduh versi terbaru. Pastikan untuk menginstal seluruh rangkaian.

Konversikan kunci pribadi Anda ke format PPK menggunakan PuTTYgen.

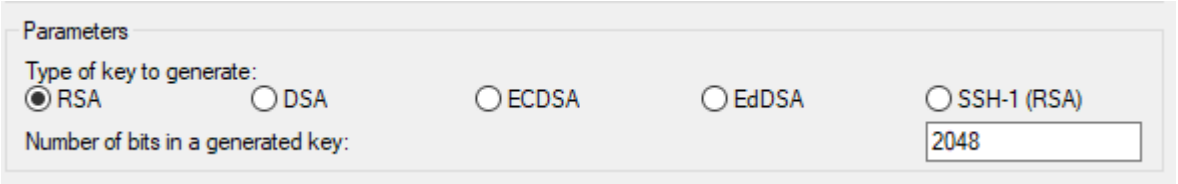
Anda harus menentukan kunci pribadi untuk key pair yang Anda tentukan saat meluncurkan instance. Jika Anda membuat kunci pribadi dalam format.pem, Anda harus mengubahnya menjadi file PPK untuk digunakan dengan PutTY. Temukan kunci pribadi (file.pem), lalu ikuti langkah-langkahnya. Konversikan kunci pribadi Anda menggunakan Pu TTYgen

(Opsional) Konversi kunci pribadi Anda menggunakan Pu TTYgen

PuTTY tidak secara native mendukung format PEM untuk kunci SSH. PuTTY menyediakan alat bernama PuTTYgen, yang mengubah kunci PEM ke format PPK yang diperlukan untuk PutTY. Jika Anda membuat kunci menggunakan format PEM alih-alih format PPK, Anda harus mengonversi kunci pribadi Anda (file.pem) ke dalam format ini (file.ppk) untuk digunakan dengan PuTTY.

Untuk mengonversi kunci pribadi Anda dari format PEM ke PPK

1. Dari menu Start, pilih All Programs, Putty, Pu. TTYgen
2. Di bawah tipe kunci yang akan dibuat, pilih RSA. Jika versi Pu Anda TTYgen tidak menyertakan opsi ini, pilih SSH-2 RSA.



3. Pilih Muat. Secara default, Pu hanya TTYgen menampilkan file dengan ekstensi `.ppk`. Untuk menemukan file `.pem`, pilih opsi untuk menampilkan file dari semua tipe.

4. Pilih file `.pem` Anda untuk pasangan kunci yang Anda tentukan saat Anda meluncurkan instans dan memilih Buka. Pu TTYgen menampilkan pemberitahuan bahwa `.pem` file berhasil diimpor. Pilih OK.
5. Untuk menyimpan kunci dalam format yang dapat digunakan PuTTY, pilih Simpan kunci privat. Pu TTYgen menampilkan peringatan tentang menyimpan kunci tanpa frasa sandi. Pilih Ya.

> **Note**
>
> Frasa sandi pada kunci privat adalah lapisan perlindungan ekstra. Meskipun kunci pribadi Anda ditemukan, kunci tersebut tidak dapat digunakan tanpa frasa sandi. Kelemahan menggunakan frasa sandi adalah membuat otomatisasi lebih sulit karena diperlukan campur tangan manusia untuk masuk ke sebuah instans, atau untuk menyalin file ke sebuah instans.

6. Tentukan nama yang sama untuk kunci yang Anda gunakan untuk pasangan kunci (misalnya, `key-pair-name`) dan pilih Simpan. PuTTY secara otomatis menambahkan ekstensi file `.ppk`.

Kunci privat Anda sekarang dalam format yang benar untuk digunakan dengan PuTTY. Anda sekarang dapat terhubung ke instans Anda menggunakan klien SSH PuTTY.

Hubungkan ke instans Linux Anda

Gunakan prosedur berikut untuk terhubung ke instans Linux Anda menggunakan klien PuTTY. Anda memerlukan file `.ppk` yang Anda buat untuk kunci privat Anda. Untuk informasi selengkapnya, lihat (Opsional) Konversi kunci pribadi Anda menggunakan Pu TTYgen di bagian sebelumnya. Jika Anda menemui kesalahan saat mencoba untuk terhubung ke instans, lihat Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda.

Versi terakhir diuji - Putty .78

Untuk terhubung ke instans Anda menggunakan PuTTY

1. Mulai Putty (dari menu Mulai, cari Putty, kemudian pilih Buka).
2. Di panel Kategori, pilih Sesi dan lengkapi bidang berikut:

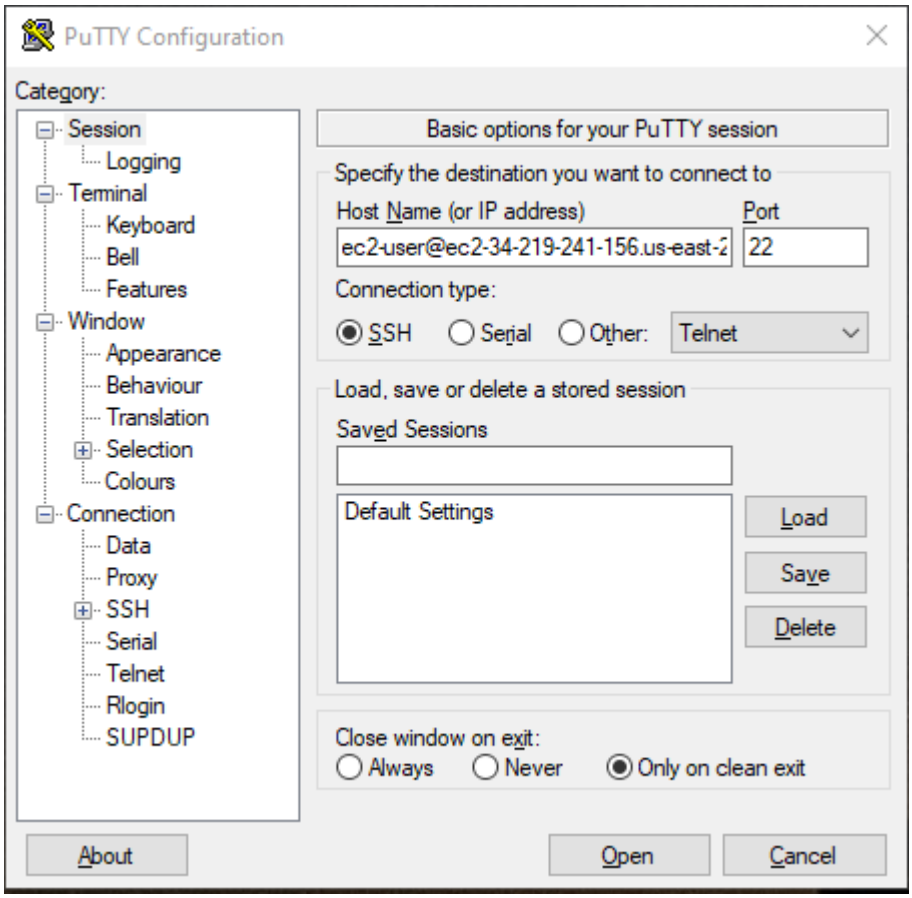
   a. Di kotak Nama Host, lakukan salah satu hal berikut ini:

      - (DNS Publik) Untuk terhubung menggunakan nama DNS publik instans Anda, masukkan *instance-user-name* @. *instance-public-dns-name*
      - (IPv6) Atau, jika instans Anda memiliki IPv6 alamat, untuk terhubung menggunakan IPv6 alamat instans Anda, masukkan *instance-user-name* @*2001:db8::1234:5678:1.2.3.4*.

      Untuk informasi tentang cara mendapatkan nama pengguna untuk instans Anda, dan nama DNS publik atau IPv6 alamat instans Anda, lihatDapatkan detail instance yang diperlukan.

b. Pastikan nilai Port adalah 22.

c. Di bawah Tipe koneksi, pilih SSH.



3. (Opsional) Anda dapat mengonfigurasi PuTTY untuk secara otomatis mengirim data 'keepalive' secara berkala agar sesi tetap aktif. Ini berguna untuk menghindari pemutusan hubungan dari instans Anda karena sesi tidak aktif. Di panel Kategori, pilih Koneksi, lalu masukkan interval yang diperlukan di Detik antara periode tetap aktif. Misalnya, jika sesi Anda terputus setelah 10 menit tidak ada aktivitas, masukkan 180 untuk mengonfigurasi PuTTY untuk mengirim data keepalive setiap 3 menit.
4. Di panel Kategori, perluas Koneksi, SSH, dan Otorisasi Pilih Kredensial.
5. Di samping File kunci pribadi untuk otentikasi, pilih Browse. Dalam kotak dialog Pilih file kunci privat, pilih file `.ppk` yang Anda buat untuk pasangan kunci Anda. Anda dapat mengeklik dua kali pada file atau memilih Buka di kotak dialog Pilih file kunci privat.
6. (Opsional) Jika Anda berencana untuk terhubung ke instans ini lagi setelah sesi ini, Anda dapat menyimpan informasi sesi untuk penggunaan di masa mendatang. Di panel Kategori, pilih Sesi. Masukkan nama untuk sesi di Sesi Tersimpan, lalu pilih Simpan.

7. Untuk terhubung ke instans, pilih Buka.
8. Jika ini adalah pertama kalinya Anda terhubung ke instans ini, PuTTY menampilkan kotak dialog peringatan keamanan yang menanyakan apakah Anda mempercayai host yang Anda sambungkan.

    a. (Opsional) Pastikan sidik jari di kotak dialog peringatan keamanan cocok dengan sidik jari yang Anda peroleh sebelumnya di (Opsional) Dapatkan sidik jari instans. Jika sidik jari ini tidak cocok, seseorang mungkin mencoba serangan “man-in-the-middle”. Jika cocok, lanjutkan ke langkah berikutnya.

    b. Pilih Terima. Sebuah jendela terbuka dan Anda terhubung ke instans Anda.

> **Note**
>
> Jika Anda menentukan frasa sandi saat mengonversi kunci pribadi Anda ke format PuTTY, Anda harus memberikan frasa sandi tersebut saat masuk ke instans.

Jika Anda menemui kesalahan saat mencoba untuk terhubung ke instans, lihat Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda.

Transfer file ke instance Linux menggunakan SCP

Salah satu cara untuk mentransfer file antara komputer lokal dan instans Linux Anda adalah dengan menggunakan protokol salinan aman (SCP). SCP adalah pilihan yang baik untuk operasi sederhana, seperti salinan file satu kali. SCP mengamankan transfer file menggunakan file.pem yang sama yang Anda gunakan untuk terhubung ke instance menggunakan SSH. Jika Anda perlu menyimpan file yang disinkronkan, atau jika file berukuran besar, rsync lebih cepat dan lebih efisien daripada SCP. Untuk keamanan, gunakan rsync melalui SSH, sebagai rsync transfer data menggunakan teks biasa secara default.

Sebelum Anda terhubung ke instans Linux Anda menggunakan SCP, selesaikan tugas-tugas berikut:

- Lengkapi prasyarat umum.
    - Periksa apakah pesan Anda telah lulus pemeriksaan statusnya. Diperlukan beberapa menit agar sebuah instans siap menerima permintaan koneksi. Untuk informasi selengkapnya, lihat Melihat pemeriksaan status.
    - Dapatkan detail instance yang diperlukan.
    - Temukan kunci pribadi dan atur izin.

  - (Opsional) Dapatkan sidik jari instans.
- Izinkan lalu lintas SSH masuk dari alamat IP Anda.

  Pastikan grup keamanan yang terkait dengan instans Anda mengizinkan lalu lintas SSH masuk dari alamat IP Anda. Untuk informasi selengkapnya, lihat Aturan-aturan untuk terhubung ke instans dari komputer Anda.
- Instal klien SCP.

  Kebanyakan komputer Linux, Unix, dan Apple menyertakan klien SCP secara default. Jika milik Anda tidak, proyek OpenSSH menyediakan implementasi gratis dari rangkaian lengkap alat SSH, termasuk klien SCP. Untuk informasi selengkapnya, lihat https://www.openssh.com.

Prosedur berikut akan membantu Anda menggunakan SCP untuk mentransfer file menggunakan nama DNS publik instans, atau IPv6 alamat jika instans Anda memilikinya.

Untuk menggunakan SCP untuk mentransfer file antara komputer Anda dan instans Anda

1. Tentukan lokasi file sumber pada komputer Anda dan jalur tujuan pada instans. Dalam contoh berikut, nama file kunci pribadi adalah`key-pair-name.pem`, file yang akan ditransfer adalah`my-file.txt`, nama pengguna untuk instance adalahec2-user, nama DNS publik dari instance adalah`instance-public-dns-name`, dan IPv6 alamat instance adalah`2001:db8::1234:5678:1.2.3.4`.
   - (DNS Publik) Untuk mentransfer file ke tujuan yang ada di instans, masukkan perintah berikut dari komputer Anda.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```
   - (IPv6) Untuk mentransfer file ke tujuan pada instance jika instance memiliki IPv6 alamat, masukkan perintah berikut dari komputer Anda. IPv6 Alamat harus dilampirkan dalam tanda kurung siku (`[ ]`), yang harus lolos (). `\`

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@
     \[2001:db8::1234:5678:1.2.3.4\]:path/
     ```
2. Jika Anda belum ter-connect ke instans menggunakan SSH, maka Anda akan melihat respons seperti berikut:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

(Opsional) Anda dapat secara opsional memverifikasi bahwa sidik jari di peringatan keamanan cocok dengan sidik jari instans. Untuk informasi selengkapnya, lihat (Opsional) Dapatkan sidik jari instans.

Masukkan **yes**.

3. Jika transfer berhasil, maka responsnya sama dengan berikut ini:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

4. Untuk mentransfer file ke arah lain (dari EC2 instans Amazon Anda ke komputer Anda), balikkan urutan parameter host. Misalnya, Anda dapat mentransfer `my-file.txt` dari EC2 instans Anda ke tujuan di komputer lokal Anda sepertimy`-file2.txt`, seperti yang ditunjukkan dalam contoh berikut.

   - (DNS Publik) Untuk mentransfer file ke tujuan yang ada di instans, masukkan perintah berikut dari komputer Anda.

     ```
     scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-
     file.txt path/my-file2.txt
     ```

   - (IPv6) Untuk mentransfer file ke tujuan di komputer Anda jika instance memiliki IPv6 alamat, masukkan perintah berikut dari komputer Anda. IPv6 Alamat harus dilampirkan dalam tanda kurung siku (`[ ]`), yang harus lolos (). `\`

     ```
     scp -i /path/key-pair-name.pem ec2-user@\[2001:db8::1234:5678:1.2.3.4\]:path/
     my-file.txt path/my-file2.txt
     ```

Kelola pengguna sistem di instans Amazon EC2 Linux Anda

Setiap instans Linux diluncurkan dengan pengguna sistem Linux default. Anda dapat menambahkan pengguna ke instans Anda dan menghapus pengguna.

Untuk pengguna default, nama pengguna default ditentukan oleh AMI yang ditentukan saat Anda meluncurkan instance.

> **Note**
>
> Secara default, autentikasi kata sandi dan login root dinonaktifkan, dan sudo diaktifkan. Untuk masuk ke instans Anda, Anda harus menggunakan pasangan kunci. Untuk informasi selengkapnya tentang logging, lihat Hubungkan ke instans Linux Anda, menggunakan SSH.. Anda dapat mengizinkan autentikasi kata sandi dan login root untuk instans Anda. Untuk informasi selengkapnya tentang bagaimana menonaktifkan driver perangkat, lihat dokumentasi untuk sistem operasi Anda.

> **Note**
>
> Pengguna sistem Linux jangan bingung dengan pengguna (IAM). Untuk informasi selengkapnya, lihat Pengguna IAM di Panduan Pengguna IAM.

Daftar Isi

- Nama pengguna default
- Pertimbangan-pertimbangan
- Buat pengguna
- Menghapus pengguna

Nama pengguna default

Nama pengguna default untuk EC2 instans Anda ditentukan oleh AMI yang ditentukan saat Anda meluncurkan instance.

Nama pengguna default adalah:

- Untuk Amazon Linux AMI, nama penggunanya adalah`ec2-user`.
- Untuk CentOS AMI, nama penggunanya adalah `centos` atau. `ec2-user`
- Untuk AMI Debian, nama penggunanya adalah`admin`.
- Untuk Fedora AMI, nama penggunanya adalah `fedora` atau. `ec2-user`

- Untuk AMI FreeBSD, nama penggunanya adalah. `ec2-user`
- Untuk RHEL AMI, nama penggunanya adalah `ec2-user` atau`root`.
- Untuk SUSE AMI, nama penggunanya adalah `ec2-user` atau`root`.
- Untuk AMI Ubuntu, nama penggunanya adalah`ubuntu`.
- Untuk AMI Oracle, nama penggunanya adalah`ec2-user`.
- Untuk Bitnami AMI, nama penggunanya adalah. `bitnami`

> **Note**
>
> Untuk menemukan nama pengguna default untuk distribusi Linux lainnya, tanyakan kepada penyedia AMI.

Pertimbangan-pertimbangan

Menggunakan pengguna default sudah cukup untuk banyak aplikasi. Namun, Anda dapat memilih untuk menambahkan pengguna sehingga individu dapat memiliki file dan ruang kerja mereka sendiri. Lebih jauh lagi, membuat pengguna untuk pengguna baru jauh lebih aman daripada memberikan beberapa (mungkin tidak berpengalaman) akses pengguna default, karena pengguna default dapat menyebabkan banyak kerusakan pada sistem bila digunakan dengan tidak benar. Untuk informasi selengkapnya, lihat Tips untuk Mengamankan EC2 Instans Anda.

Untuk mengaktifkan akses SSH pengguna ke EC2 instans Anda menggunakan pengguna sistem Linux, Anda harus berbagi kunci SSH dengan pengguna. Atau, Anda dapat menggunakan EC2 Instance Connect untuk menyediakan akses ke pengguna tanpa perlu berbagi dan mengelola kunci SSH. Untuk informasi selengkapnya, lihat Connect ke instans Linux Anda menggunakan alamat IP publik dan EC2 Instance Connect.

Buat pengguna

Pertama buat pengguna, lalu tambahkan kunci publik SSH yang memungkinkan pengguna untuk terhubung dan masuk ke instans.

> **Important**
>
> Pada Langkah 1 dari prosedur ini, Anda membuat key pair baru. Karena key pair berfungsi seperti kata sandi, sangat penting untuk menanganinya dengan aman. Jika Anda membuat key pair untuk pengguna, Anda harus memastikan bahwa kunci pribadi dikirim kepada

mereka dengan aman. Atau, pengguna dapat menyelesaikan Langkah 1 dan 2 dengan membuat key pair mereka sendiri, menjaga kunci pribadi tetap aman di mesin mereka, dan kemudian mengirimkan kunci publik untuk menyelesaikan prosedur dari Langkah 3.

Untuk membuat pengguna

1. Buat pasangan kunci baru. Anda harus menyediakan file `.pem` untuk pengguna yang Anda buat penggunanya. Mereka harus menggunakan file ini untuk terhubung ke instans.
2. Ambil kunci publik dari pasangan kunci yang Anda buat di langkah sebelumnya.

   ```
   $ ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   Perintah tersebut mengembalikan kunci publik, seperti yang ditunjukkan pada contoh berikut.

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
   i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
   +CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. Hubungkan dengan instans.
4. Gunakan perintah adduser untuk membuat pengguna dan menambahkannya ke sistem (dengan entri di file `/etc/passwd`). Perintah tersebut juga membuat grup dan direktori home untuk pengguna. Dalam contoh ini, pengguna dinamai *`newuser`*.

   - AL2023 dan Amazon Linux 2

     Dengan AL2 023 dan Amazon Linux 2, pengguna dibuat dengan otentikasi kata sandi dinonaktifkan secara default.

     ```
     [ec2-user ~]$ sudo adduser newuser
     ```

   - Ubuntu

     Sertakan `--disabled-password` parameter untuk membuat pengguna dengan otentikasi kata sandi dinonaktifkan.

```
[ubuntu ~]$ sudo adduser newuser --disabled-password
```

5. Beralih ke pengguna baru agar direktori dan file yang Anda buat memiliki kepemilikan yang sesuai.

```
[ec2-user ~]$ sudo su - newuser
```

Perintah berubah dari `ec2-user` *`newuser`* ke untuk menunjukkan bahwa Anda telah mengalihkan sesi shell ke pengguna baru.

6. Tambahkan kunci publik SSH ke pengguna. Pertama buat direktori di direktori utama pengguna untuk file kunci SSH, lalu buat file kunci, dan terakhir tempelkan kunci publik ke dalam file kunci, seperti yang dijelaskan di sub-langkah berikut.

   a. Membuat direktori `.ssh` di direktori beranda *`newuser`* dan mengubah izin filenya menjadi `700` (hanya pemilik yang dapat membaca, menulis, atau membuka direktori).

```
[newuser ~]$ mkdir .ssh
```

```
[newuser ~]$ chmod 700 .ssh
```

> **Important**
>
> Tanpa izin file yang tepat ini, pengguna tidak akan bisa masuk.

   b. Membuat file bernama `authorized_keys` di direktori `.ssh` dan mengubah izin filenya menjadi `600` (hanya pemilik yang dapat membaca atau menulis ke file).

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

> **Important**
>
> Tanpa izin file yang tepat ini, pengguna tidak akan bisa masuk.

   c. Buka file `authorized_keys` menggunakan editor teks favorit Anda (seperti vim atau nano).

```
[newuser ~]$ nano .ssh/authorized_keys
```

Tempel kunci publik yang Anda ambil pada Langkah 2 ke dalam file dan simpan perubahannya.

> **Important**
>
> Pastikan Anda menempelkan kunci publik dalam satu baris berkelanjutan. Kunci publik tidak boleh dibagi menjadi beberapa baris.

Pengguna sekarang harus dapat masuk ke *newuser* pengguna di instans Anda, menggunakan kunci privat yang sesuai dengan kunci publik yang Anda tambahkan ke `authorized_keys` file. Untuk informasi selengkapnya tentang berbagai metode untuk menghubungkan ke instans Linux, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..

Menghapus pengguna

Jika pengguna tidak lagi diperlukan, Anda dapat menghapus pengguna tersebut sehingga tidak dapat digunakan lagi.

Gunakan perintah userdel untuk menghapus pengguna dari sistem. Saat Anda menentukan parameter `-r`, direktori beranda pengguna dan spool email akan dihapus. Untuk mempertahankan home directory dan mail spool pengguna, hilangkan parameter `-r`.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Hubungkan ke instans Windows Anda menggunakan RDP

Anda dapat terhubung ke instans Amazon EC2 yang dibuat dari sebagian besar Gambar Mesin Amazon Windows (AMIs) menggunakan Remote Desktop. Desktop Jarak Jauh menggunakan Remote Desktop Protocol (RDP) untuk terhubung ke dan gunakan instans Anda dengan cara yang sama seperti Anda menggunakan komputer yang ada di depan Anda (komputer lokal). Ini tersedia di sebagian besar edisi Windows dan juga tersedia untuk Mac OS.

Lisensi untuk sistem operasi Windows Server memungkinkan dua koneksi jarak jauh secara bersamaan untuk tujuan administratif. Lisensi untuk Windows Server sudah termasuk dalam harga instans Windows Anda. Jika Anda membutuhkan lebih dari dua koneksi jarak jauh secara bersamaan, Anda harus membeli lisensi Remote Desktop Services (RDS). Jika Anda mencoba koneksi ketiga, terjadi kesalahan.

> **Tip**
>
> Jika Anda perlu terhubung ke instans Anda untuk memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya untuk instans yang dibangun di Sistem AWS Nitro, Anda dapat menggunakan. EC2 Serial Console untuk instans

Daftar Isi

- Connect ke instans Windows Anda menggunakan klien RDP
- Hubungkan ke instans Windows Anda menggunakan Fleet Manager
- Transfer file ke instance Windows menggunakan RDP

Connect ke instans Windows Anda menggunakan klien RDP

Anda dapat terhubung ke instance Windows Anda menggunakan klien RDP sebagai berikut.

> **Tip**
>
> Atau, Anda dapat terhubung ke instans Windows menggunakan Systems Manager Fleet Manager atau EC2 Instance Connect Endpoint.

Prasyarat

Anda harus memenuhi prasyarat berikut untuk terhubung ke instance Windows Anda menggunakan klien RDP.

- Lengkapi prasyarat umum.
  - Periksa apakah pesan Anda telah lulus pemeriksaan statusnya. Diperlukan beberapa menit agar sebuah instans siap menerima permintaan koneksi. Untuk informasi selengkapnya, lihat Melihat pemeriksaan status.

  - Dapatkan detail instance yang diperlukan.
  - Temukan kunci pribadi dan atur izin.
  - (Opsional) Dapatkan sidik jari instans.
- Instal klien RDP.
  - (Windows) Windows menyertakan klien RDP secara default. Untuk memverifikasi, ketik mstsc di jendela Command Prompt. Jika komputer Anda tidak mengenali perintah ini, unduh aplikasi Microsoft Remote Desktop dari Microsoft Store.
  - (macOS X) Unduh Aplikasi Windows untuk Mac (sebelumnya bernama Microsoft Remote Desktop dari Mac App Store.
  - (Linux) Gunakan Remmina.
- Izinkan lalu lintas RDP masuk dari alamat IP Anda.

  Pastikan bahwa grup keamanan yang terkait dengan instans Anda memungkinkan lalu lintas RDP masuk dari alamat IP Anda. Untuk informasi selengkapnya, lihat Aturan-aturan untuk terhubung ke instans dari komputer Anda.

Ambil kata sandi administrator

Jika Anda menggabungkan instans Anda ke domain, Anda dapat terhubung ke instans Anda menggunakan kredensi domain dari. Directory Service Pada layar login Remote Desktop, alih-alih menggunakan nama komputer lokal dan kata sandi yang dihasilkan, gunakan nama pengguna yang sepenuhnya memenuhi syarat untuk administrator (misalnya,**`corp.example.com\Admin`**), dan kata sandi untuk akun ini.

Untuk terhubung ke instance Windows menggunakan RDP, Anda harus mengambil kata sandi administrator awal dan kemudian memasukkan kata sandi ini saat Anda terhubung ke instans Anda. Diperlukan beberapa menit setelah peluncuran instans sebelum sandi ini tersedia. Akun Anda harus memiliki izin untuk memanggil GetPasswordDatatindakan tersebut. Untuk informasi selengkapnya, lihat Contoh kebijakan untuk mengontrol akses API Amazon EC2.

Nama pengguna default untuk akun Administrator tergantung pada bahasa sistem operasi (OS) yang terkandung dalam AMI. Untuk menentukan nama pengguna yang benar, identifikasi bahasa OS, lalu pilih nama pengguna yang sesuai. Misalnya, untuk OS bahasa Inggris, nama pengguna adalah`Administrator`, untuk OS Prancis itu`Administrateur`, dan untuk OS Portugis itu`Administrador`. Jika versi bahasa OS tidak memiliki nama pengguna dalam bahasa yang sama,

pilih nama penggunaAdministrator (Other). Untuk informasi selengkapnya, lihat Nama Lokal untuk Akun Administrator di Windows di situs web Microsoft.

Untuk mengambil kata sandi administrator awal

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Hubungkan.
4. Pada halaman Connect to instance, pilih tab klien RDP.
5. Untuk Nama Pengguna, pilih nama pengguna default untuk akun Administrator. Nama pengguna yang Anda pilih harus sesuai dengan bahasa sistem operasi (OS) yang terdapat dalam AMI yang Anda gunakan untuk meluncurkan instance Anda. Jika tidak ada nama pengguna dalam bahasa yang sama dengan OS Anda, pilih Administrator (Lainnya).
6. Pilih Dapatkan kata sandi.
7. Pada halaman Dapatkan kata sandi Windows, lakukan hal berikut:

    a. Pilih Unggah file kunci pribadi dan arahkan ke file kunci pribadi (.pem) yang Anda tentukan saat meluncurkan instance. Pilih file dan pilih Buka untuk menyalin seluruh isi file ke jendela ini.

    b. Pilih Dekripsi kata sandi. Halaman Dapatkan kata sandi Windows ditutup, dan kata sandi administrator default untuk instance muncul di bawah Kata Sandi, menggantikan tautan Dapatkan kata sandi yang ditampilkan sebelumnya.

    c. Salin kata sandi dan simpan di tempat yang aman. Kata sandi ini diperlukan untuk terhubung ke instans.

Hubungkan ke instans Windows Anda

Prosedur berikut menggunakan klien Remote Desktop Connection untuk Windows (MSTSC). Jika Anda menggunakan klien RDP yang berbeda, unduh file RDP dan kemudian lihat dokumentasi untuk klien RDP untuk langkah-langkah untuk membuat koneksi RDP.

Untuk terhubung ke instance Windows menggunakan klien RDP

1. Pada halaman Connect to instance, pilih Download file remote desktop. Setelah pengunduhan file selesai, pilih Batal untuk kembali ke halaman Instans. File RDP diunduh ke folder AndaDownloads.

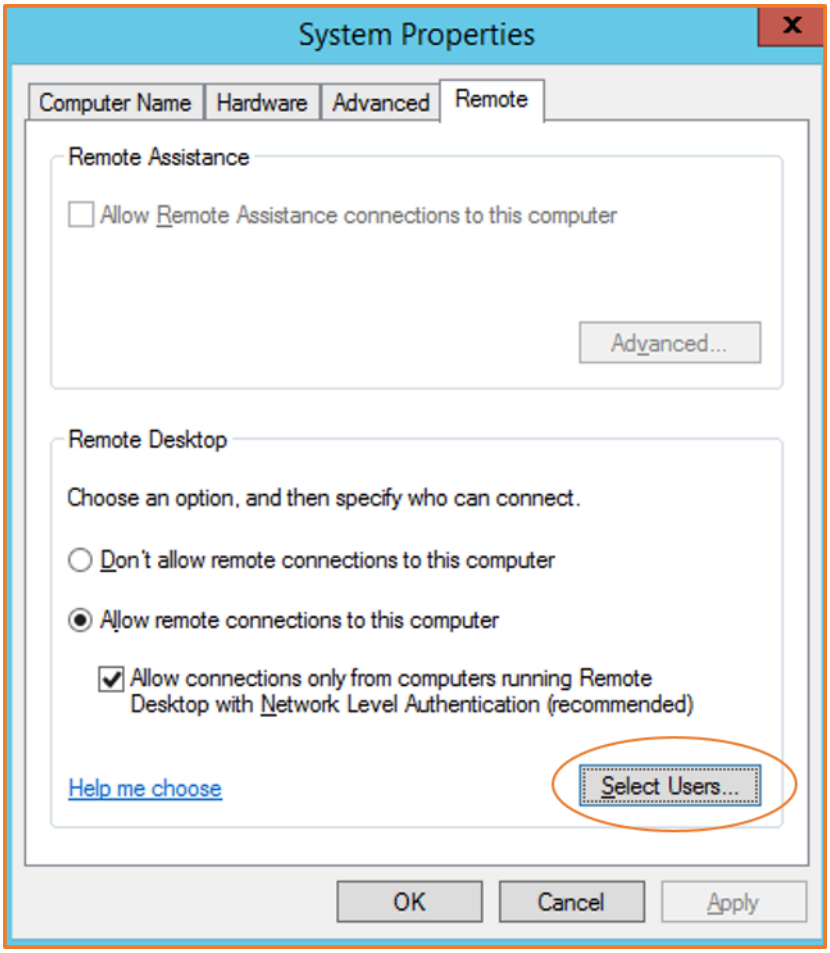
2. Jalankan `mstsc.exe` untuk membuka klien RDP.
3. Perluas opsi Tampilkan, pilih Buka, dan pilih file.rdp dari folder Anda. `Downloads`
4. Secara default, Komputer adalah nama IPv4 DNS publik dari instance dan Nama pengguna adalah akun administrator. Untuk terhubung ke instance menggunakan IPv6 sebagai gantinya, ganti nama IPv4 DNS publik instance dengan IPv6 alamatnya. Tinjau pengaturan default dan ubah sesuai kebutuhan.
5. Pilih Hubungkan. Jika Anda menerima peringatan bahwa penerbit koneksi jarak jauh tidak diketahui, pilih Connect untuk melanjutkan.
6. Masukkan kata sandi yang Anda simpan sebelumnya, lalu pilih OK.
7. Karena sifat dari sertifikat yang ditandatangani sendiri, Anda mungkin mendapatkan peringatan bahwa sertifikat keamanan tidak dapat diautentikasi. Lakukan salah satu tindakan berikut:
   - Jika Anda mempercayai sertifikat, pilih Ya untuk terhubung ke instans Anda.
   - [Windows] Sebelum Anda melanjutkan, bandingkan sidik jari sertifikat dengan nilai dalam log sistem untuk mengkonfirmasi identitas komputer jarak jauh. Pilih Lihat sertifikat dan kemudian pilih Thumbprint dari tab Detail. Bandingkan nilai ini dengan nilai `RDPCERTIFICATE-THUMBPRINT` dalam Tindakan, Pantau dan pemecahan masalah, Dapatkan log sistem.
   - [Mac OS X] Sebelum Anda melanjutkan, bandingkan sidik jari sertifikat dengan nilai dalam log sistem untuk mengonfirmasi identitas komputer jarak jauh. Pilih Tampilkan Sertifikat, perluas Detail, dan pilih SHA1 Sidik Jari. Bandingkan nilai ini dengan nilai `RDPCERTIFICATE-THUMBPRINT` dalam Tindakan, Pantau dan pemecahan masalah, Dapatkan log sistem.
8. Jika koneksi RDP berhasil, klien RDP menampilkan layar login Windows dan kemudian desktop Windows. Jika Anda menerima pesan kesalahan, lihatthe section called “Desktop Jarak Jauh tidak dapat terhubung ke komputer jarak jauh”. Ketika Anda selesai dengan koneksi RDP, Anda dapat menutup klien RDP.

Konfigurasikan akun pengguna

Setelah Anda terhubung ke instans Anda melalui RDP, kami sarankan Anda melakukan tugas-tugas berikut:

- Ubah kata sandi administrator dari nilai default. Anda dapat mengubah kata sandi saat masuk ke instans itu sendiri, seperti yang Anda lakukan di komputer mana pun yang menjalankan Windows Server.

- Buat pengguna lain dengan hak akses administrator di instans tersebut. Ini adalah perlindungan jika Anda lupa kata sandi administrator atau memiliki masalah dengan akun administrator. Pengguna baru harus memiliki izin untuk mengakses instans dari jarak jauh. Buka System Properties dengan mengklik kanan ikon This PC di desktop Windows atau File Explorer dan pilih Properties. Pilih Pengaturan jarak jauh, dan pilih Pilih Pengguna untuk menambahkan pengguna ke grup Pengguna Desktop Jarak Jauh.



Hubungkan ke instans Windows Anda menggunakan Fleet Manager

Anda dapat menggunakan Fleet Manager, kemampuan AWS Systems Manager, untuk terhubung ke instance Windows menggunakan Remote Desktop Protocol (RDP) dan menampilkan hingga empat instance Windows pada halaman yang sama di halaman yang sama. Konsol Manajemen AWS Anda dapat terhubung ke instans pertama di Desktop Jarak Jauh Manajer Armada langsung dari halaman Instans di konsol Amazon EC2. Untuk informasi selengkapnya tentang Fleet Manager, lihat Connect ke instance terkelola menggunakan Remote Desktop di Panduan AWS Systems Manager Pengguna.

Anda tidak perlu secara khusus mengizinkan lalu lintas RDP masuk dari alamat IP Anda jika Anda menggunakan Fleet Manager untuk terhubung. Manajer Armada menangani itu untuk Anda.

Prasyarat

Sebelum mencoba terhubung ke instans menggunakan Fleet Manager, Anda harus mengatur lingkungan Anda. Untuk informasi selengkapnya, lihat Menyiapkan lingkungan Anda di Panduan AWS Systems Manager Pengguna.

Untuk terhubung ke instance Windows menggunakan Fleet Manager

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Hubungkan.
4. Pada tab klien RDP, untuk Jenis Koneksi, pilih Connect menggunakan Fleet Manager.
5. Pilih Desktop Jarak Jauh Manajer Armada. Halaman Desktop Jarak Jauh Fleet Manager akan terbuka di konsol AWS Systems Manager .
6. Masukkan kredensialnya, lalu pilih Connect.
7. Jika koneksi RDP berhasil, Fleet Manager menampilkan desktop Windows. Setelah selesai dengan sesi, pilih Actions, End session.

Untuk informasi selengkapnya, lihat Menyambungkan ke instans terkelola Windows Server menggunakan Remote Desktop di Panduan AWS Systems Manager Pengguna.

Transfer file ke instance Windows menggunakan RDP

Anda dapat bekerja dengan instans Windows Anda dengan cara yang sama seperti Anda bekerja dengan server Windows mana pun. Misalnya, Anda dapat mentransfer file antara instance Windows dan komputer lokal Anda menggunakan fitur berbagi file lokal dari perangkat lunak Microsoft Remote Desktop Connection (RDP). Anda dapat mengakses file lokal di drive hard disk, drive DVD, drive media portabel, dan drive jaringan yang dipetakan.

Untuk mengakses file lokal Anda dari instans Windows, Anda harus mengaktifkan fitur berbagi file lokal dengan memetakan drive sesi jarak jauh ke drive lokal Anda. Langkah-langkahnya sedikit berbeda tergantung pada apakah sistem operasi komputer lokal Anda adalah Windows atau macOS X.

Untuk informasi lebih lanjut tentang prasyarat untuk terhubung menggunakan RDP, lihat. Prasyarat

Windows

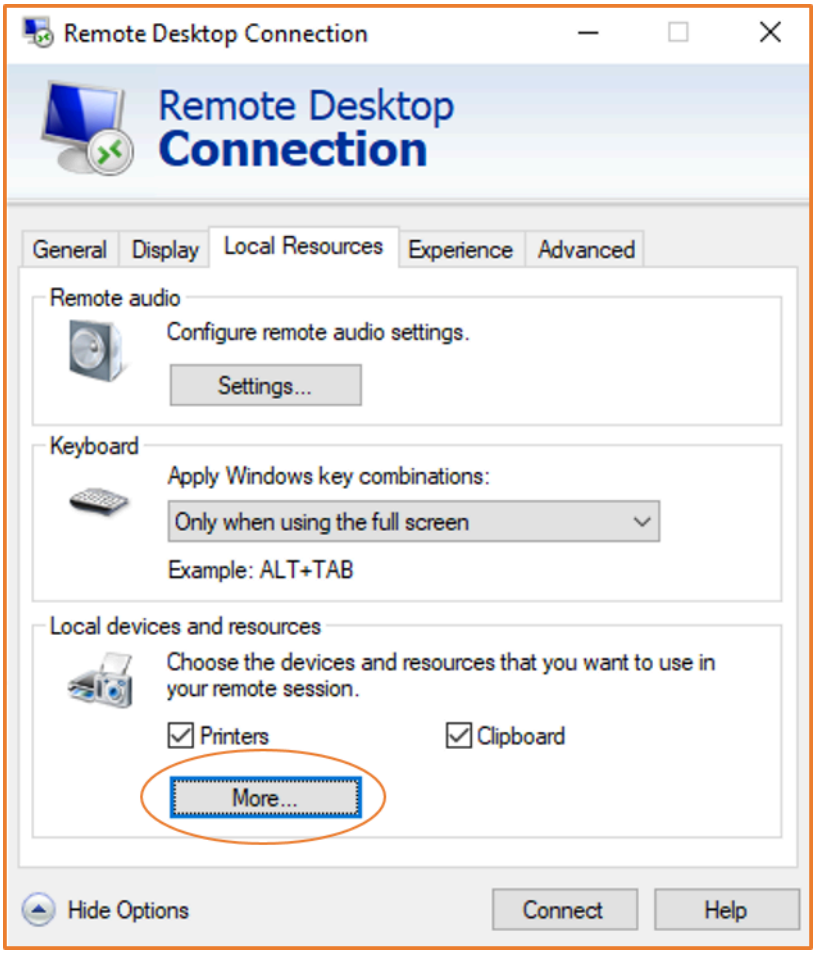
Untuk memetakan drive sesi jarak jauh ke folder lokal Anda di komputer Windows lokal Anda

1. Buka klien Remote Desktop Connection.
2. Pilih Tunjukkan Opsi.
3. Tambahkan nama host instance ke bidang Komputer dan nama pengguna ke bidang Nama pengguna, sebagai berikut:

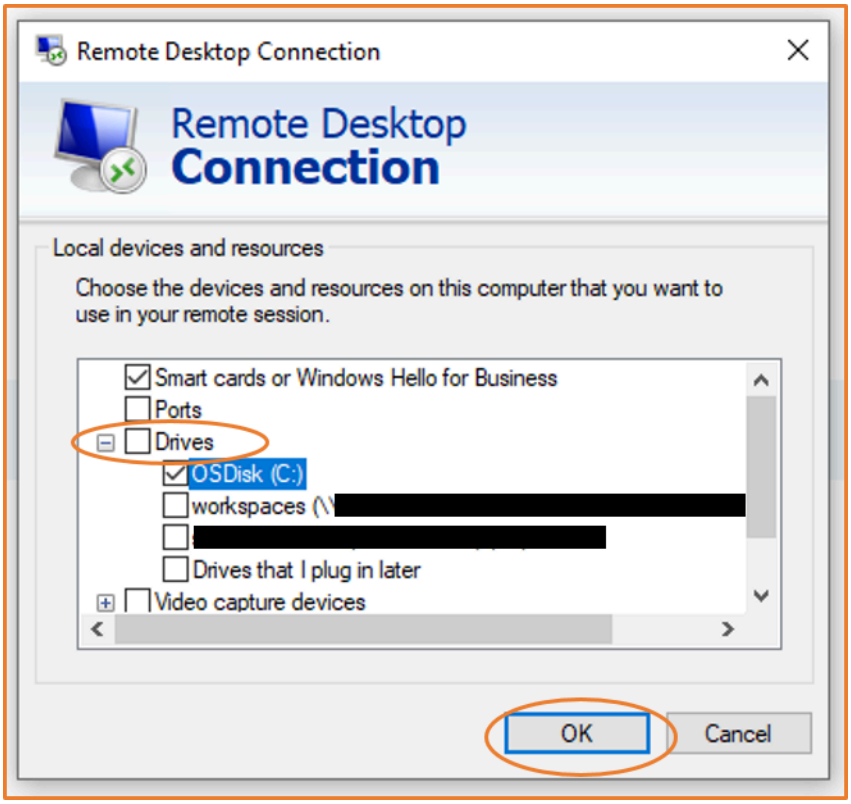
   a. Pada Pengaturan koneksi, pilih Buka... , lalu jelajahi file pintasan RDP yang Anda unduh dari konsol Amazon EC2. File berisi nama host IPv4 DNS Publik, yang mengidentifikasi instance, dan nama pengguna Administrator.

   b. Pilih file dan pilih Buka. Bidang Computer and User name diisi dengan nilai-nilai dari file shortcut RDP.

   c. Pilih Simpan.
4. Pilih tab Sumber Daya Lokal.
5. Di bawah Perangkat lokal dan sumber daya, pilih Selengkapnya...



6. Buka Drive dan pilih drive lokal untuk dipetakan ke instans Windows Anda.
7. Pilih OKE.

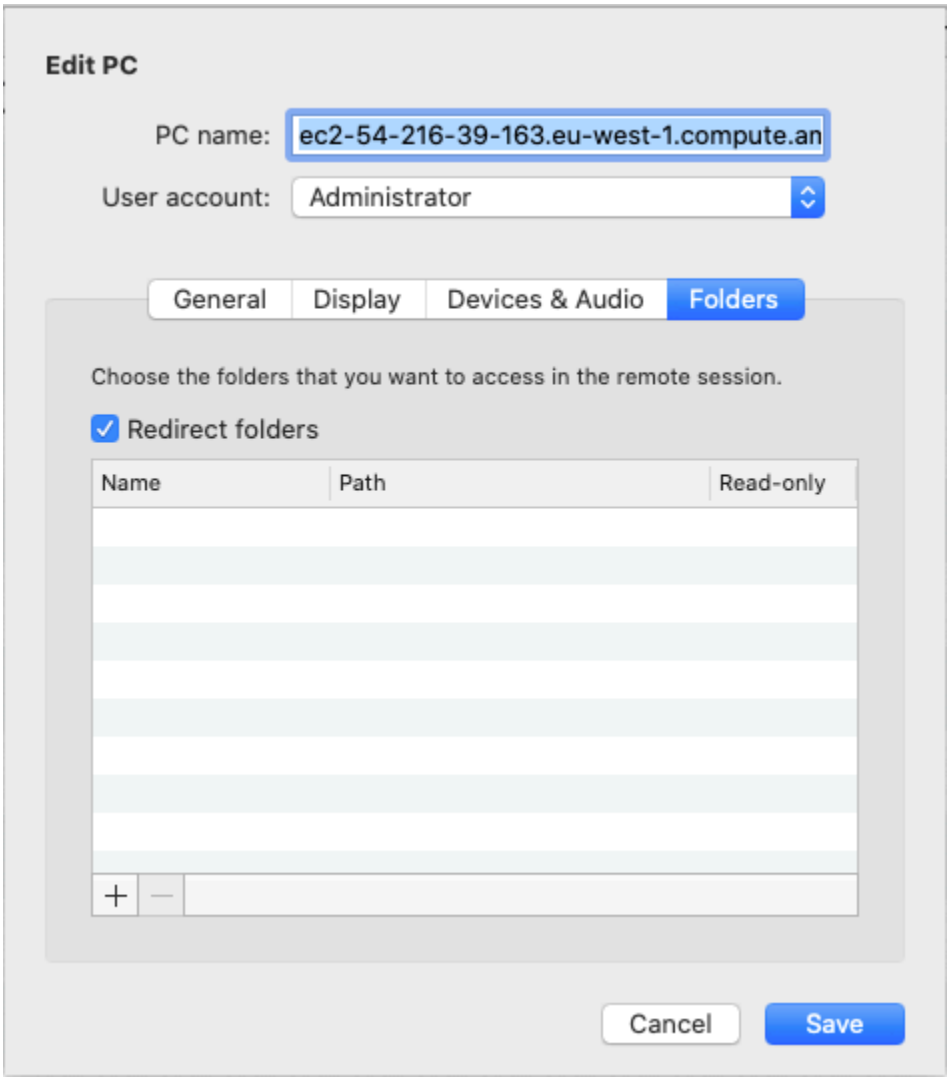


8. Pilih Hubungkan untuk terhubung ke instans Windows Anda.

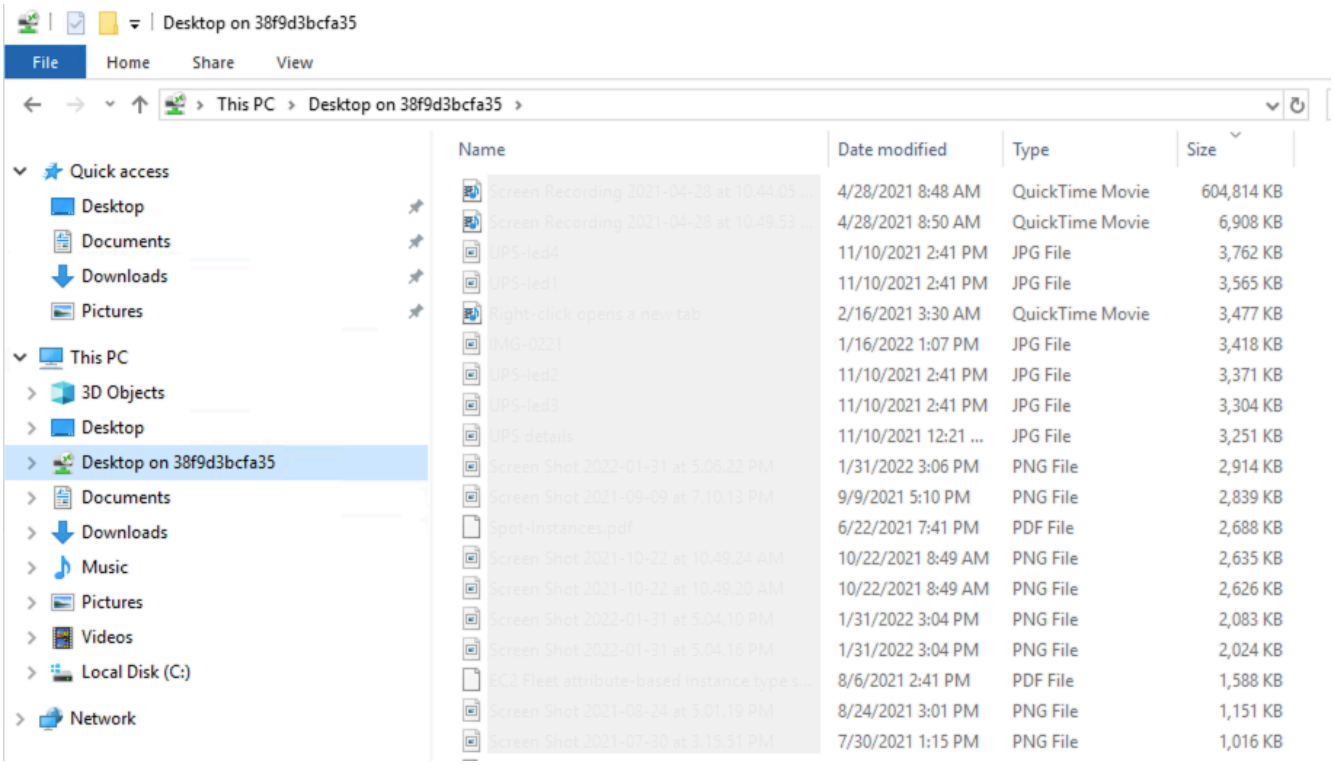
macOS X

Untuk memetakan drive sesi jarak jauh ke folder lokal Anda di komputer macOS X lokal Anda

1. Buka klien Remote Desktop Connection.
2. Jelajahi file RDP yang Anda unduh dari konsol Amazon EC2 (saat awal Anda terhubung ke instans), dan seret file ke klien Remote Desktop Connection.
3. Klik kanan file RDP, dan pilih Edit.
4. Pilih tab Folder, dan pilih kotak centang Redirect folder.



5. Pilih ikon + di kiri bawah, jelajahi ke folder untuk memetakan, dan pilih Buka. Ulangi langkah ini untuk setiap folder untuk dipetakan.
6. Pilih Simpan.
7. Pilih Hubungkan untuk terhubung ke instans Windows Anda. Anda akan dimintai kata sandi.
8. Pada contoh, di File Explorer, perluas PC ini, dan temukan folder bersama tempat Anda dapat mengakses file lokal Anda. Pada tangkapan layar berikut, folder Desktop di komputer lokal dipetakan ke drive sesi jarak jauh pada instans.



Untuk informasi selengkapnya tentang membuat perangkat lokal tersedia untuk sesi jarak jauh di komputer Mac, lihat Memulai dengan klien macOS.

Connect ke EC2 instans Amazon menggunakan Session Manager

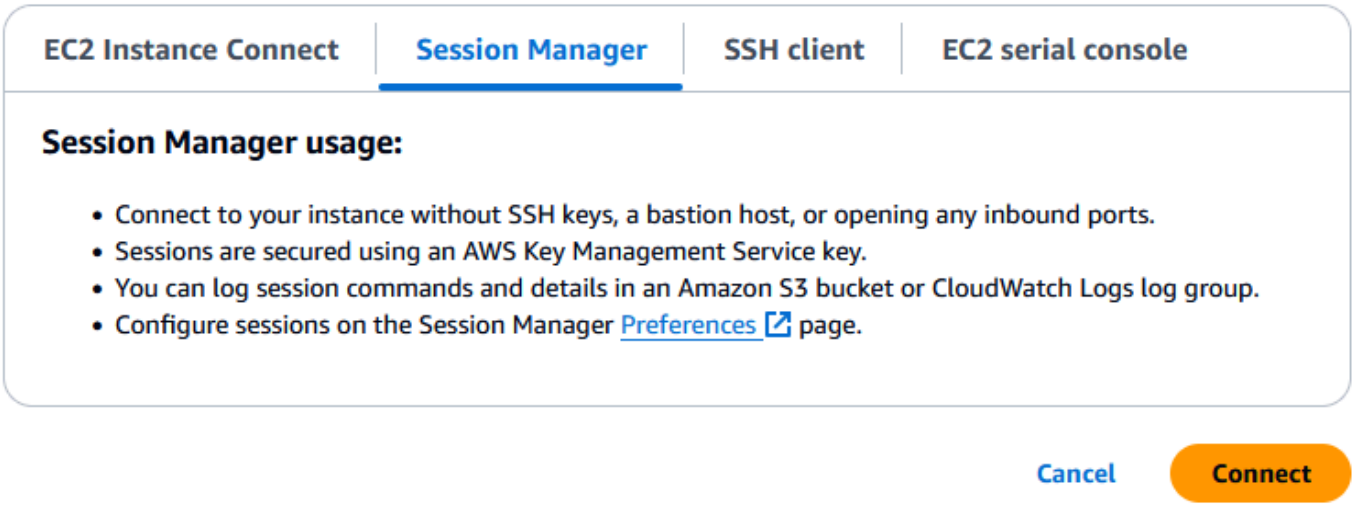
Session Manager adalah AWS Systems Manager kemampuan yang dikelola sepenuhnya untuk mengelola EC2 instans Amazon Anda melalui shell interaktif, satu-klik, berbasis browser, atau melalui file. AWS CLI Anda dapat menggunakan Session Manager untuk memulai sesi dengan sebuah instans di akun Anda. Setelah sesi dimulai, Anda dapat menjalankan perintah interaktif pada instance seperti yang Anda lakukan untuk jenis koneksi lainnya. Untuk informasi lebih lanjut tentang penggunaan Session Manager, lihat AWS Systems Manager Session Manager di Panduan Pengguna AWS Systems Manager .

Prasyarat

Sebelum mencoba menyambung ke instans menggunakan Session Manager, Anda harus menyelesaikan langkah-langkah penyiapan yang diperlukan. Misalnya, instans harus dikelola oleh SSM dan harus memiliki peran IAM terlampir dengan kebijakan Amazon SSMManaged InstanceCore. Untuk informasi selengkapnya, lihat Menyiapkan Session Manager.

Untuk menyambung ke EC2 instans Amazon menggunakan Session Manager di EC2 konsol Amazon

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Hubungkan.
4. Untuk metode koneksi, pilih Session Manager.
5. Pilih Connect untuk memulai sesi.



Pemecahan masalah

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan satu atau beberapa tindakan Systems Manager (`ssm:command-name`), Anda harus memperbarui kebijakan agar Anda dapat memulai sesi dari EC2 konsol Amazon. Untuk informasi dan instruksi lebih lanjut, lihat Kebijakan IAM default Quickstart untuk Session Manager di Panduan Pengguna AWS Systems Manager .

Connect ke instans Linux Anda menggunakan alamat IP publik dan EC2 Instance Connect

Amazon EC2 Instance Connect menyediakan cara aman untuk terhubung ke instans Linux Anda melalui Secure Shell (SSH). Dengan EC2 Instance Connect, Anda menggunakan kebijakan dan prinsipal AWS Identity and Access Management (IAM) untuk mengontrol akses SSH ke instans Anda, menghilangkan kebutuhan untuk berbagi dan mengelola kunci SSH. Semua permintaan koneksi menggunakan EC2 Instance Connect dicatat AWS CloudTrail sehingga Anda dapat mengaudit permintaan koneksi.

Anda dapat menggunakan EC2 Instance Connect untuk menyambung ke instans menggunakan konsol Amazon EC2 atau klien SSH pilihan Anda.

Saat Anda terhubung ke sebuah instans menggunakan EC2 Instance Connect, API EC2 Instance Connect mendorong kunci publik SSH ke metadata instans yang tetap bertahan selama 60 detik. Kebijakan IAM yang dilampirkan ke pengguna mengizinkan pengguna Anda untuk mendorong kunci publik ke metadata instans. Daemon SSH menggunakan `AuthorizedKeysCommand` dan`AuthorizedKeysCommandUser`, yang dikonfigurasi saat EC2 Instance Connect diinstal, untuk mencari kunci publik dari metadata instance untuk otentikasi, dan menghubungkan Anda ke instance.

> **Tip**
>
> EC2 Instance Connect adalah salah satu opsi untuk terhubung ke instans Linux Anda. Untuk opsi lain, lihat Hubungkan ke instans Linux Anda, menggunakan SSH.. Untuk terhubung ke instance Windows, lihatHubungkan ke instans Windows Anda menggunakan RDP.

Harga

EC2 Instance Connect tersedia tanpa biaya tambahan.

Ketersediaan wilayah

EC2 Instance Connect tersedia di semua Wilayah AWS, kecuali Asia Pasifik (Taipei). Hal ini tidak didukung di Local Zones.

Daftar Isi

- Tutorial: Selesaikan konfigurasi yang diperlukan untuk terhubung ke instans Anda menggunakan EC2 Instance Connect
- Prasyarat untuk EC2 Instance Connect
- Berikan izin IAM untuk EC2 instans Connect
- Instal EC2 instans Connect pada instans EC2 Anda
- Connect ke instans Linux menggunakan EC2 Instance Connect
- Hapus instalasi EC2 Instance Connect

Untuk posting blog yang membahas cara meningkatkan keamanan host bastion Anda menggunakan EC2 Instance Connect, lihat Mengamankan host bastion dengan Amazon EC2 Instance Connect.

Tutorial: Selesaikan konfigurasi yang diperlukan untuk terhubung ke instans Anda menggunakan EC2 Instance Connect

Untuk menyambung ke instans menggunakan EC2 Instance Connect di konsol Amazon EC2, pertama-tama Anda harus menyelesaikan konfigurasi prasyarat yang memungkinkan Anda untuk berhasil terhubung ke instans Anda. Tujuan dari tutorial ini adalah untuk memandu Anda melalui tugas-tugas untuk menyelesaikan konfigurasi prasyarat.

Ikhtisar tutorial

Dalam tutorial ini, Anda akan menyelesaikan empat tugas berikut:

- Tugas 1: Berikan izin yang diperlukan untuk menggunakan EC2 Instance Connect

  Pertama, Anda akan membuat kebijakan IAM yang berisi izin IAM yang memungkinkan Anda mendorong kunci publik ke metadata instance. Anda akan melampirkan kebijakan ini ke identitas IAM Anda (pengguna, grup pengguna, atau peran) sehingga identitas IAM Anda mendapatkan izin ini.
- Tugas 2: Izinkan lalu lintas masuk dari layanan EC2 Instance Connect ke instans Anda

  Kemudian Anda akan membuat grup keamanan yang memungkinkan lalu lintas dari layanan EC2 Instance Connect ke instans Anda. Ini diperlukan saat Anda menggunakan EC2 Instance Connect di konsol Amazon EC2 untuk menyambung ke instans Anda.
- Tugas 3: Luncurkan instans Anda

  Anda kemudian akan meluncurkan instans EC2 menggunakan AMI yang sudah diinstal sebelumnya dengan EC2 Instance Connect dan Anda akan menambahkan grup keamanan yang Anda buat pada langkah sebelumnya.
- Tugas 4: Connect ke instans Anda

  Terakhir, Anda akan menggunakan EC2 Instance Connect di konsol Amazon EC2 untuk terhubung ke instans Anda. Jika Anda dapat terhubung, maka Anda dapat yakin bahwa konfigurasi prasyarat yang Anda selesaikan di Tugas 1, 2, dan 3 berhasil.

Tugas 1: Berikan izin yang diperlukan untuk menggunakan EC2 Instance Connect

Saat Anda terhubung ke sebuah instans menggunakan EC2 Instance Connect, API EC2 Instance Connect mendorong kunci publik SSH ke metadata instans yang tetap bertahan selama 60 detik.

Anda memerlukan kebijakan IAM yang dilampirkan pada identitas IAM Anda (pengguna, grup pengguna, atau peran) untuk memberi Anda izin yang diperlukan untuk mendorong kunci publik ke metadata instans.

Tujuan tugas

Anda akan membuat kebijakan IAM yang memberikan izin untuk mendorong kunci publik ke instance. Tindakan spesifik untuk memungkinkan adalah`ec2-instance-connect:SendSSHPublicKey`. Anda juga harus mengizinkan `ec2:DescribeInstances` tindakan sehingga Anda dapat melihat dan memilih instans Anda di konsol Amazon EC2.

Setelah membuat kebijakan, Anda akan melampirkan kebijakan ke identitas IAM Anda (pengguna, grup pengguna, atau peran) sehingga identitas IAM Anda mendapatkan izin.

Anda akan membuat kebijakan yang dikonfigurasi sebagai berikut:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

Important

Kebijakan IAM yang dibuat dalam tutorial ini adalah kebijakan yang sangat permisif; ini memungkinkan Anda untuk terhubung ke instance apa pun menggunakan nama pengguna AMI apa pun. Kami menggunakan kebijakan yang sangat permisif ini untuk menjaga tutorial tetap sederhana dan fokus pada konfigurasi spesifik yang diajarkan tutorial ini. Namun, dalam lingkungan produksi, kami menyarankan agar kebijakan IAM Anda dikonfigurasi untuk

memberikan izin hak istimewa paling sedikit. Untuk contoh kebijakan IAM, lihat Berikan izin IAM untuk EC2 instans Connect.

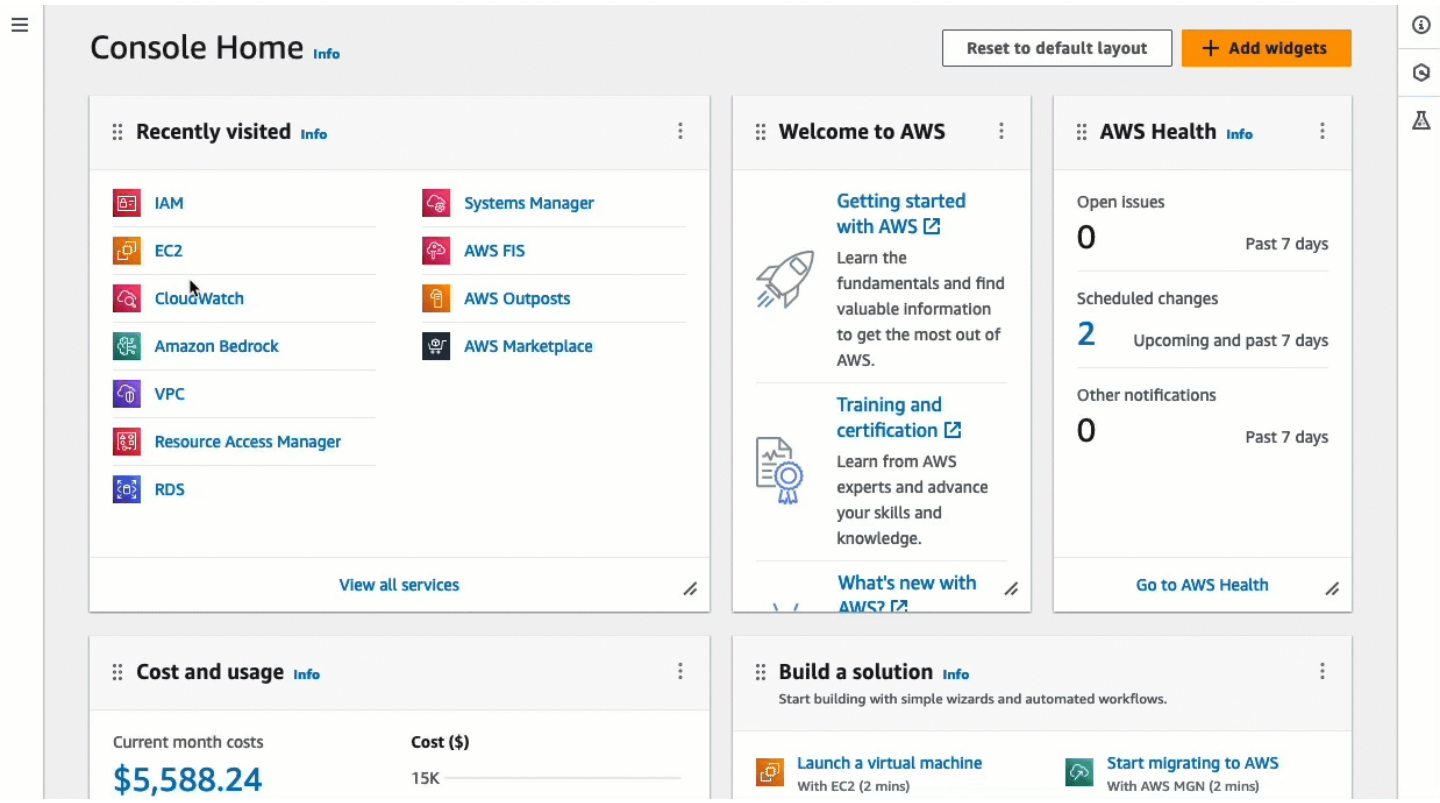
Untuk membuat dan melampirkan kebijakan IAM yang memungkinkan Anda menggunakan EC2 Instance Connect untuk terhubung ke instans

1. Pertama buat kebijakan IAM
   a. Buka konsol IAM di https://console.aws.amazon.com/iam/.
   b. Di panel navigasi, pilih Kebijakan.
   c. Pilih Buat kebijakan.
   d. Pada halaman Tentukan izin, lakukan hal berikut:
      i. Untuk Layanan, pilih EC2 Instance Connect.
      ii. Di bawah Tindakan yang diizinkan, di bidang pencarian mulai mengetik **send** untuk menampilkan tindakan yang relevan, lalu pilih Kirim SSHPublic Kunci.
      iii. Di bawah Sumber Daya, pilih Semua. Untuk lingkungan produksi, kami sarankan untuk menentukan instance dengan ARN-nya, tetapi untuk tutorial ini, Anda mengizinkan semua instance.
      iv. Pilih Tambahkan lebih banyak izin.
      v. Untuk Layanan , pilih EC2.
      vi. Di bawah Tindakan diizinkan, di bidang pencarian mulai mengetik **describein** untuk menampilkan tindakan yang relevan, lalu pilih DescribeInstances.
      vii. Pilih Berikutnya.
   e. Pada halaman Review dan create, lakukan hal berikut:
      i. Untuk Nama kebijakan, masukkan nama untuk kebijakan tersebut.
      ii. Pilih Buat kebijakan.
2. Kemudian lampirkan kebijakan ke identitas Anda
   a. Di konsol IAM, di panel navigasi, pilih Kebijakan.
   b. Dalam daftar kebijakan, pilih tombol opsi di sebelah nama kebijakan yang Anda buat. Anda dapat menggunakan kotak pencarian untuk memfilter daftar kebijakan.
   c. Pilih Tindakan, Lampirkan.

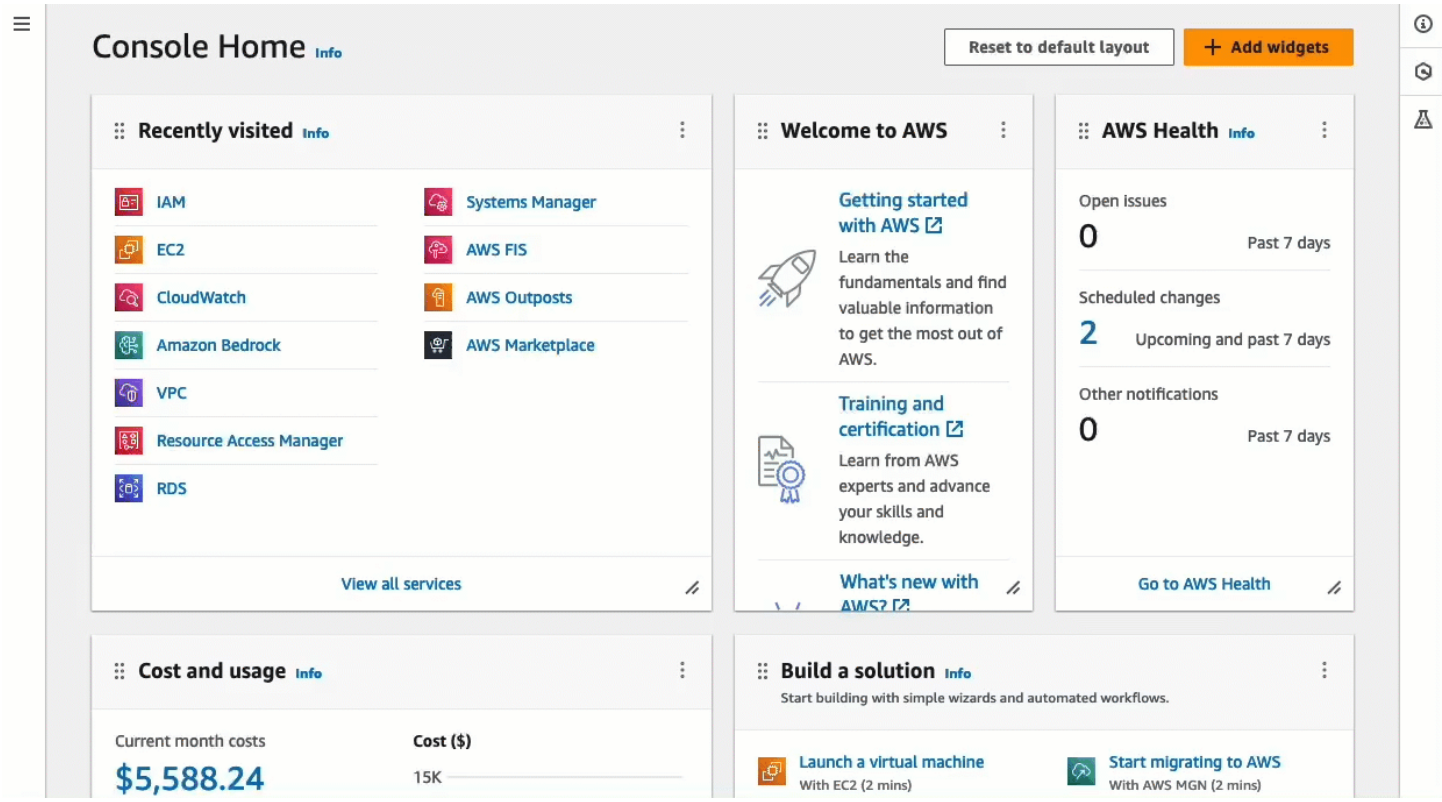
d. Di bawah entitas IAM, pilih kotak centang di samping identitas Anda (pengguna, grup pengguna, atau peran). Anda dapat menggunakan kotak pencarian untuk memfilter daftar entitas.

e. Pilih Lampirkan kebijakan.

Melihat animasi: Buat kebijakan IAM



Melihat animasi: Lampirkan kebijakan IAM



Tugas 2: Izinkan lalu lintas masuk dari layanan EC2 Instance Connect ke instans Anda

Saat Anda menggunakan EC2 Instance Connect di konsol Amazon EC2 untuk menyambung ke instans, lalu lintas yang harus diizinkan untuk mencapai instans adalah lalu lintas dari layanan EC2 Instance Connect. Ini berbeda dengan menghubungkan dari komputer lokal Anda ke sebuah instans; dalam hal ini, Anda harus mengizinkan lalu lintas dari komputer lokal Anda ke instans Anda. Untuk mengizinkan lalu lintas dari layanan EC2 Instance Connect, Anda harus membuat grup keamanan yang memungkinkan lalu lintas SSH masuk dari rentang alamat IP untuk layanan EC2 Instance Connect.

AWS menggunakan daftar awalan untuk mengelola rentang alamat IP. Nama-nama daftar awalan EC2 Instance Connect adalah sebagai berikut, dengan *`region`* diganti dengan kode Region:

- IPv4 nama daftar awalan: `com.amazonaws.`*`region`*`.ec2-instance-connect`
- IPv6 nama daftar awalan: `com.amazonaws.`*`region`*`.ipv6.ec2-instance-connect`

Tujuan tugas

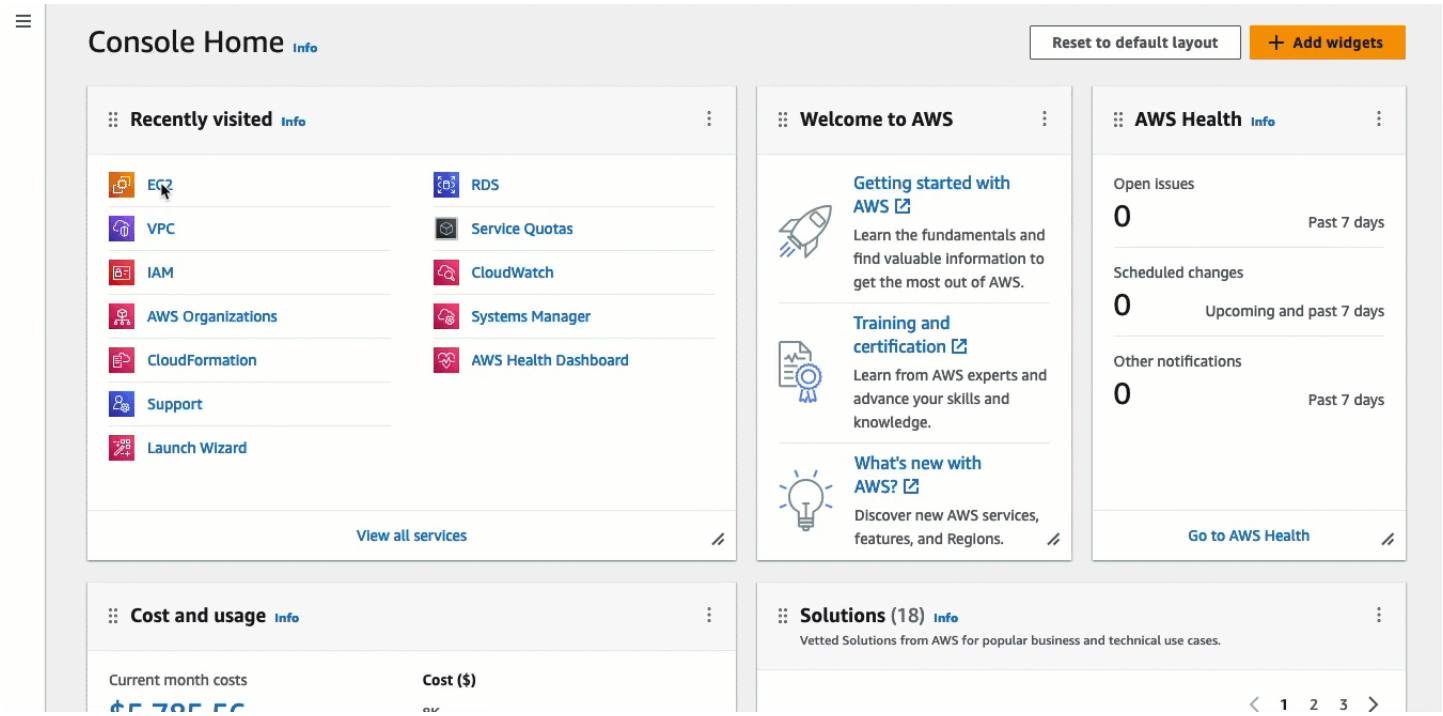
Anda akan membuat grup keamanan yang memungkinkan lalu lintas SSH masuk pada port 22 dari daftar IPv4 awalan di Wilayah tempat instans Anda berada.

Untuk membuat grup keamanan yang memungkinkan lalu lintas masuk dari layanan EC2 Instance Connect ke instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Security Groups (Grup Keamanan).
3. Pilih Buat grup keamanan.
4. Di Detail dasar, lakukan hal berikut:
   a. Untuk nama grup Keamanan, masukkan nama yang berarti untuk grup keamanan Anda.
   b. Untuk Deskripsi, masukkan deskripsi yang bermakna untuk grup keamanan Anda.
5. Di bawah aturan Inbound, lakukan hal berikut:
   a. Pilih Tambahkan aturan.
   b. Untuk Tipe, pilih SSH.
   c. Untuk Sumber, tinggalkan Custom.
   d. Di bidang di sebelah Sumber, pilih daftar awalan untuk EC2 Instance Connect.

      Misalnya, jika instans Anda berada di Wilayah AS Timur (Virginia N.) (**`us-east-1`**) dan pengguna Anda akan terhubung ke IPv4 alamat publiknya, pilih daftar awalan berikut: com.amazonaws.us-east-1.ec2-instance-connect
6. Pilih Buat grup keamanan.

Melihat animasi: Buat grup keamanan



Tugas 3: Luncurkan instans Anda

Saat meluncurkan instance, Anda harus menentukan AMI yang berisi informasi yang diperlukan untuk meluncurkan instance. Anda dapat memilih untuk meluncurkan instans dengan atau tanpa EC2 Instance Connect yang sudah diinstal sebelumnya. Dalam tugas ini, kami menentukan AMI yang sudah diinstal sebelumnya dengan EC2 Instance Connect.

Jika Anda meluncurkan instans tanpa EC2 Instance Connect pra-instal, dan Anda ingin menggunakan EC2 Instance Connect untuk menyambung ke instans Anda, Anda harus melakukan langkah-langkah konfigurasi tambahan. Langkah-langkah ini berada di luar cakupan tutorial ini.

Tujuan tugas

Anda akan meluncurkan instance dengan Amazon Linux 2023 AMI, yang sudah diinstal sebelumnya dengan EC2 Instance Connect. Anda juga akan menentukan grup keamanan yang Anda buat sebelumnya sehingga Anda dapat menggunakan EC2 Instance Connect di konsol Amazon EC2 untuk menyambung ke instans Anda. Karena Anda akan menggunakan EC2 Instance Connect untuk terhubung ke instans Anda, yang mendorong kunci publik ke metadata instans Anda, Anda tidak perlu menentukan kunci SSH saat meluncurkan instance Anda.

Untuk meluncurkan instans yang dapat menggunakan EC2 Instance Connect di konsol Amazon EC2 untuk koneksi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di bilah navigasi di bagian atas layar, AWS Wilayah saat ini ditampilkan (misalnya, Irlandia). Pilih Wilayah untuk meluncurkan instans Anda. Pilihan ini penting karena Anda membuat grup keamanan yang memungkinkan lalu lintas untuk Wilayah tertentu, jadi Anda harus memilih Wilayah yang sama untuk meluncurkan instans Anda.
3. Dari dasbor konsol Amazon EC2, pilih Luncurkan instans.
4. (Opsional) Pada Nama dan tanda, untuk Nama, masukkan nama deskriptif untuk instans Anda.
5. Di bawah Gambar Aplikasi dan OS (Gambar Mesin Amazon), pilih Mulai Cepat. Amazon Linux dipilih secara default. Di bawah Amazon Machine Image (AMI), Amazon Linux 2023 AMI dipilih secara default. Simpan pilihan default untuk tugas ini.
6. Di bawah Jenis Instance, untuk tipe Instance, pertahankan pilihan default, atau pilih jenis instance yang berbeda.
7. Di bawah Key pair (login), untuk nama Key pair, pilih Proceed without a key pair (Tidak disarankan). Saat Anda menggunakan EC2 Instance Connect untuk terhubung ke sebuah instans, EC2 Instance Connect mendorong key pair ke metadata instans, dan key pair inilah yang digunakan untuk koneksi tersebut.
8. Pada Pengaturan jaringan, lakukan hal berikut:

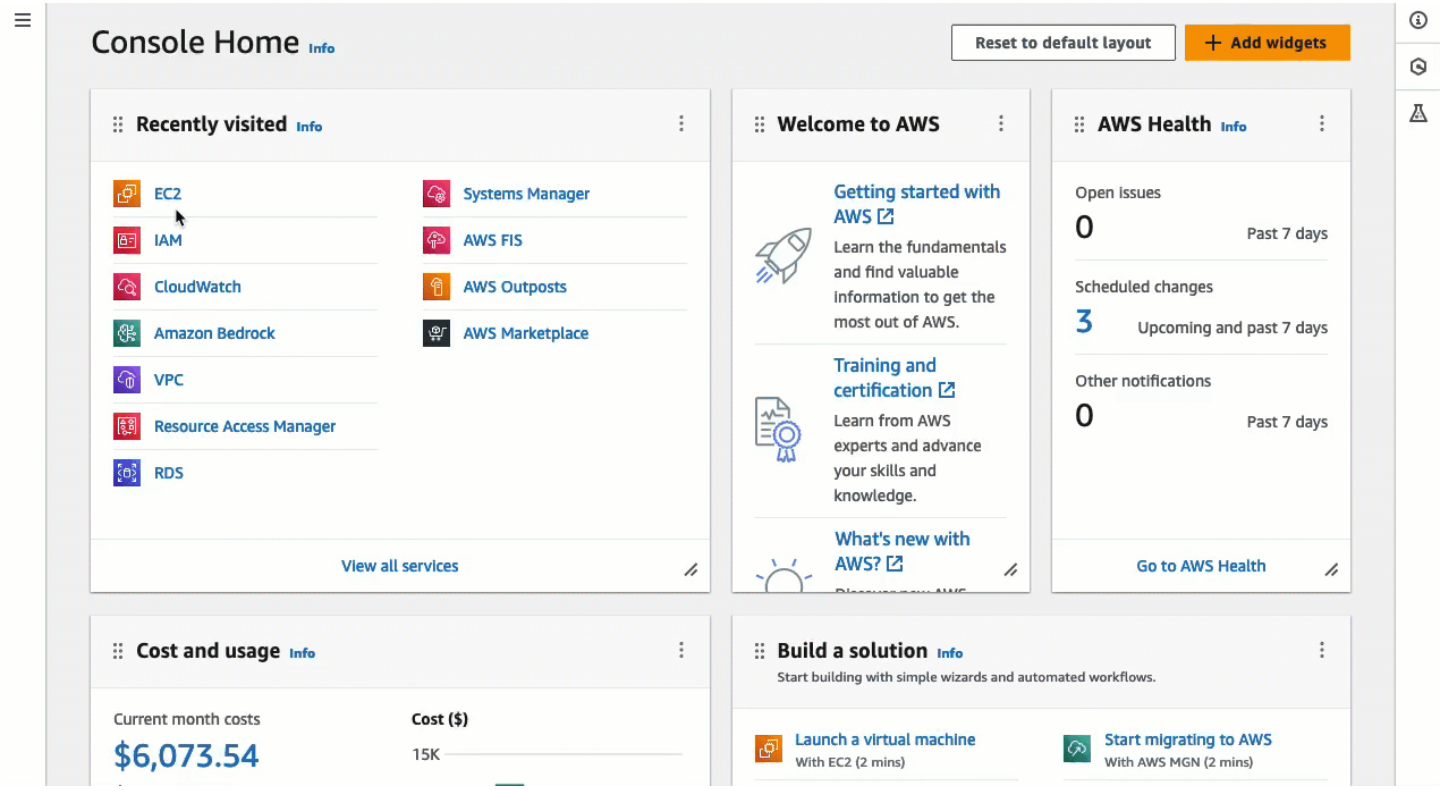
   a. Untuk Auto-tetapkan IP publik, tinggalkan Aktifkan.

   > **Note**
   >
   > Untuk menggunakan EC2 Instance Connect di konsol Amazon EC2 untuk menyambung ke instans, instans harus memiliki IPv4 publik IPv6 atau alamat.

   b. Untuk Firewall (grup keamanan), pilih Pilih grup keamanan yang ada.

   c. Di bawah Grup keamanan umum, pilih grup keamanan yang Anda buat sebelumnya.
9. Di panel Ringkasan, pilih Luncurkan instans.

Melihat animasi: Luncurkan instance Anda



Tugas 4: Connect ke instans Anda

Saat Anda terhubung ke sebuah instans menggunakan EC2 Instance Connect, API EC2 Instance Connect mendorong kunci publik SSH ke metadata instans yang tetap bertahan selama 60 detik. Daemon SSH menggunakan `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser` mencari kunci publik dari metadata instance untuk otentikasi, dan menghubungkan Anda ke instance.

Tujuan tugas

Dalam tugas ini, Anda akan terhubung ke instans menggunakan EC2 Instance Connect di konsol Amazon EC2. Jika Anda menyelesaikan tugas prasyarat 1, 2, dan 3, koneksi harus berhasil.

Langkah-langkah untuk terhubung ke instans Anda

Gunakan langkah-langkah berikut untuk terhubung ke instans Anda. Untuk melihat animasi langkah-langkahnya, lihatMelihat animasi: Connect ke instans Anda.

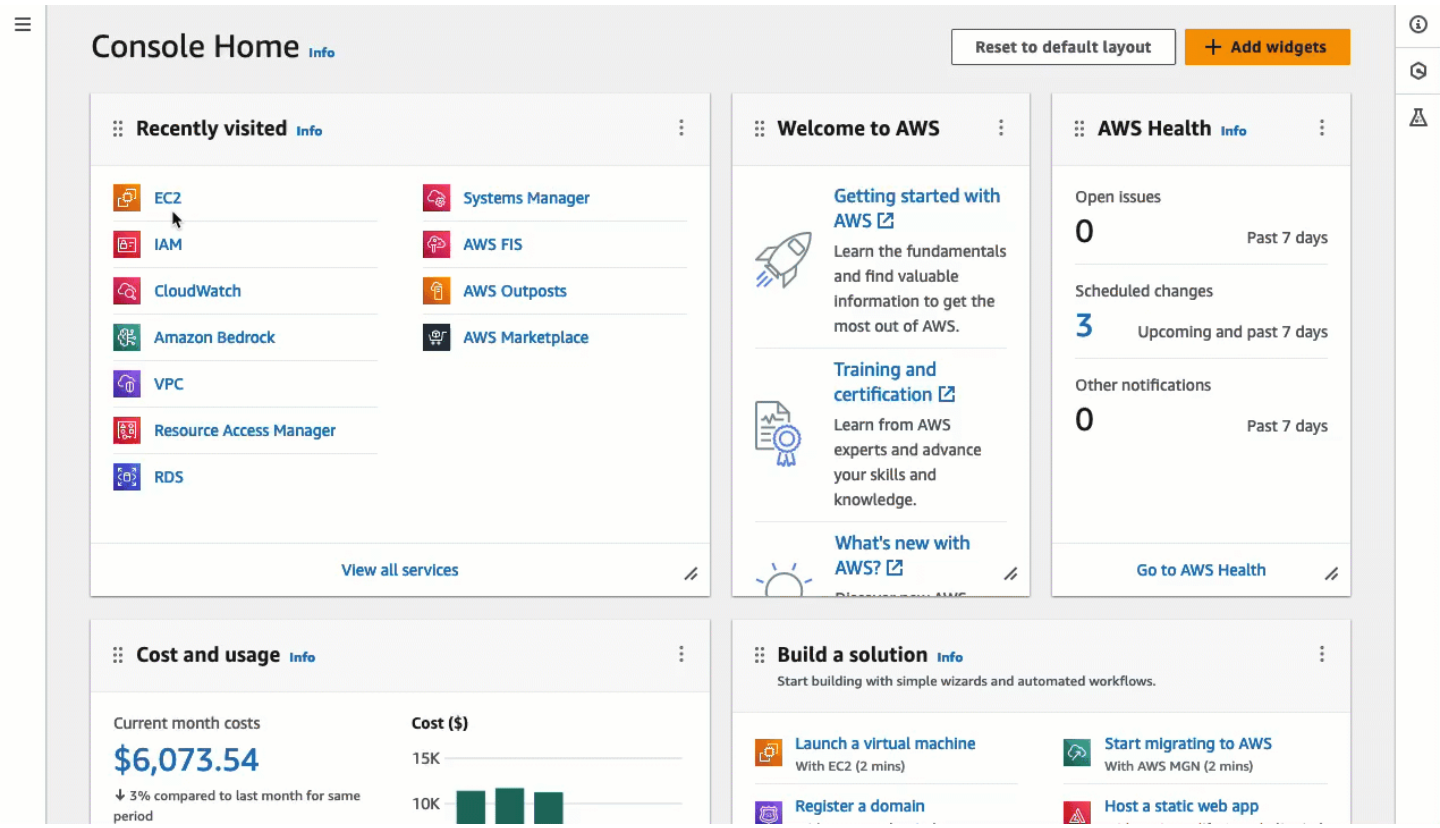
Untuk menghubungkan instans menggunakan EC2 Instance Connect di konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Di bilah navigasi di bagian atas layar, AWS Wilayah saat ini ditampilkan (misalnya, Irlandia). Pilih Wilayah tempat instans Anda berada.
3. Di panel navigasi, pilih Instans.
4. Pilih instans Anda dan pilih Connect.
5. Pilih tab EC2 Instance Connect.
6. Pilih Connect menggunakan IP Publik.
7. Pilih Hubungkan.

   Jendela terminal terbuka di browser, dan Anda terhubung ke instance Anda.

Melihat animasi: Connect ke instans Anda



Prasyarat untuk EC2 Instance Connect

Berikut ini adalah prasyarat untuk menginstal dan menggunakan EC2 Instance Connect:

- Menginstal EC2 Instance Connect
- Pastikan konektivitas jaringan
- Izinkan lalu lintas SSH masuk

- Berikan izin
- Instal klien SSH di komputer lokal Anda
- Memenuhi persyaratan nama pengguna

Menginstal EC2 Instance Connect

Untuk menggunakan EC2 Instance Connect, instans harus menginstal EC2 Instance Connect. Anda dapat meluncurkan instans menggunakan AMI yang sudah diinstal sebelumnya dengan EC2 Instance Connect, atau Anda dapat menginstal EC2 Instance Connect pada instans yang diluncurkan dengan didukung. AMIs Untuk informasi selengkapnya, lihat Instal EC2 instans Connect pada instans EC2 Anda.

Pastikan konektivitas jaringan

Instans dapat dikonfigurasi untuk memungkinkan pengguna terhubung ke instans Anda melalui internet atau melalui alamat IP pribadi instans. Tergantung pada bagaimana pengguna Anda akan terhubung ke instans Anda menggunakan EC2 Instance Connect, Anda harus mengonfigurasi akses jaringan berikut:

- Jika pengguna Anda akan terhubung ke instans Anda melalui internet, maka instans Anda harus memiliki publik IPv4 atau IPv6 alamat dan berada di subnet publik dengan rute ke internet. Jika Anda belum memodifikasi subnet publik default Anda, maka itu berisi rute ke internet IPv4 hanya untuk, dan bukan untuk IPv6. Untuk informasi selengkapnya, lihat Mengaktifkan akses internet VPC menggunakan gateway internet di Panduan Pengguna Amazon VPC.
- Jika pengguna Anda akan terhubung ke instans Anda melalui IPv4 alamat pribadi instans, maka Anda harus membuat konektivitas jaringan pribadi ke VPC Anda, seperti dengan menggunakan AWS Direct Connect, AWS Site-to-Site VPN, atau mengintip VPC, sehingga pengguna Anda dapat mencapai alamat IP pribadi instans.

Jika instans Anda tidak memiliki alamat IPv4 atau IPv6 publik dan Anda memilih untuk tidak mengonfigurasi akses jaringan seperti yang dijelaskan di atas, Anda dapat mempertimbangkan EC2 Instance Connect Endpoint sebagai alternatif dari EC2 Instance Connect. Dengan EC2 Instance Connect Endpoint, Anda dapat terhubung ke instans menggunakan SSH atau RDP meskipun instans tidak memiliki publik atau alamat. IPv4 IPv6 Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda menggunakan konsol Amazon EC2.

Izinkan lalu lintas SSH masuk

Saat menggunakan konsol Amazon EC2 untuk menyambung ke instans

Saat pengguna terhubung ke instans menggunakan konsol Amazon EC2, lalu lintas yang harus diizinkan untuk mencapai instans adalah lalu lintas dari layanan EC2 Instance Connect. Layanan ini diidentifikasi oleh rentang alamat IP tertentu, yang AWS mengelola melalui daftar awalan. Anda harus membuat grup keamanan yang memungkinkan lalu lintas SSH masuk dari layanan EC2 Instance Connect. Untuk mengonfigurasinya, untuk aturan masuk, di bidang di sebelah Sumber, pilih daftar awalan EC2 Instance Connect.

AWS menyediakan daftar awalan terkelola yang berbeda untuk alamat IPv4 dan IPv6 untuk setiap Wilayah. Nama-nama daftar awalan EC2 Instance Connect adalah sebagai berikut, dengan *`region`* diganti dengan kode Region:

- IPv4 nama daftar awalan: `com.amazonaws.`*`region`*`.ec2-instance-connect`
- IPv6 nama daftar awalan: `com.amazonaws.`*`region`*`.ipv6.ec2-instance-connect`

Untuk instruksi untuk membuat grup keamanan, lihatTugas 2: Izinkan lalu lintas masuk dari layanan EC2 Instance Connect ke instans Anda. Untuk informasi selengkapnya, lihat Daftar awalan AWS terkelola yang tersedia di Panduan Pengguna Amazon VPC.

Saat menggunakan CLI atau SSH untuk terhubung ke sebuah instance

Pastikan grup keamanan yang terkait dengan instans Anda mengizinkan lalu lintas SSH masuk pada port 22 dari alamat IP Anda atau dari jaringan Anda. Grup keamanan default untuk VPC tidak mengizinkan lalu lintas SSH masuk secara default. Grup keamanan yang dibuat oleh wizard peluncuran instans memungkinkan lalu lintas SSH masuk secara default. Untuk informasi selengkapnya, lihat Aturan-aturan untuk terhubung ke instans dari komputer Anda.

Berikan izin

Anda harus memberikan izin yang diperlukan untuk setiap pengguna IAM yang akan menggunakan EC2 Instance Connect untuk terhubung ke instans. Untuk informasi selengkapnya, lihat Berikan izin IAM untuk EC2 instans Connect.

Instal klien SSH di komputer lokal Anda

Jika pengguna Anda akan terhubung menggunakan SSH, mereka harus memastikan bahwa komputer lokal mereka memiliki klien SSH.

Komputer lokal milik pengguna kemungkinan besar telah menginstal klien SSH secara default. Mereka dapat memeriksa klien SSH dengan mengetik ssh di baris perintah. Jika komputer lokal mereka tidak mengenali perintah tersebut, mereka dapat menginstal klien SSH. Untuk informasi tentang instalasi klien SSH di Linux atau macOS X, lihat http://www.openssh.com. Untuk informasi tentang instalasi klien SSH di Windows 10, lihat OpenSSH di Windows.

Tidak perlu menginstal klien SSH di komputer lokal jika pengguna Anda hanya menggunakan konsol Amazon EC2 untuk terhubung ke sebuah instans.

Memenuhi persyaratan nama pengguna

Saat menggunakan EC2 Instance Connect untuk menyambung ke instans, nama pengguna harus memenuhi persyaratan berikut:

- Karakter pertama: Harus berupa huruf (`A-Z`,`a-z`), digit (`0-9`), atau garis bawah (`_`)
- Karakter selanjutnya: Dapat berupa huruf (`A-Z`, `a-z`), digit (`0-9`), atau karakter berikut: `@ . _ -`
- Panjang minimum: 1
- Panjang maksimal: 31 karakter

Berikan izin IAM untuk EC2 instans Connect

Untuk terhubung ke instans menggunakan EC2 Instance Connect, Anda harus membuat kebijakan IAM yang memberikan izin kepada pengguna Anda untuk tindakan dan kondisi berikut:

- Tindakan `ec2-instance-connect:SendSSHPublicKey` – Memberikan izin untuk mendorong kunci publik ke sebuah instans.
- Kondisi `ec2:osuser` – Menentukan nama pengguna OS yang dapat mendorong kunci publik ke sebuah instans. Gunakan nama pengguna default untuk AMI yang Anda gunakan untuk meluncurkan instance. Nama pengguna default untuk AL2023 dan Amazon Linux 2 adalah`ec2-user`, dan untuk Ubuntu ituu`buntu`.
- Tindakan `ec2:DescribeInstances` – Wajib saat menggunakan konsol EC2 karena wrapper memanggil tindakan ini. Pengguna mungkin sudah memiliki izin untuk memanggil tindakan ini dari kebijakan lain.
- `ec2:DescribeVpcs`tindakan - Diperlukan saat menghubungkan ke IPv6 alamat.

Pertimbangkan untuk membatasi akses ke instans EC2 tertentu. Jika tidak, semua prinsipal IAM dengan izin untuk `ec2-instance-connect:SendSSHPublicKey` tindakan tersebut dapat

terhubung ke semua instans EC2. Anda dapat membatasi akses dengan menentukan sumber daya ARNs atau dengan menggunakan tag sumber daya sebagai kunci kondisi.

Untuk informasi selengkapnya, lihat Tindakan, sumber daya, dan kunci syarat untuk Amazon EC2 instans Connect.

Untuk informasi tentang pembuatan kebijakan IAM, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Izinkan pengguna untuk terhubung ke instans tertentu

Kebijakan IAM berikut memberikan izin untuk terhubung ke instans tertentu, yang diidentifikasi oleh sumber daya mereka. ARNs

Dalam contoh kebijakan IAM berikut, tindakan dan kondisi berikut ditentukan:

- `ec2-instance-connect:SendSSHPublicKey`Tindakan memberikan izin kepada pengguna untuk terhubung ke dua instance, yang ditentukan oleh sumber daya. ARNs Untuk memberikan izin kepada pengguna untuk terhubung ke semua instans EC2, ganti sumber daya ARNs dengan wildcard. *
- `ec2:osuser`Kondisi memberikan izin untuk terhubung ke instance hanya jika *`ami-username`* ditentukan saat menghubungkan.
- Tindakan `ec2:DescribeInstances` ditentukan untuk memberikan izin kepada pengguna yang akan menggunakan konsol untuk terhubung ke instans Anda. Jika pengguna Anda hanya akan menggunakan klien SSH untuk terhubung ke instans Anda, maka Anda dapat menghapus `ec2:DescribeInstances`. Perhatikan bahwa tindakan API `ec2:Describe*` tidak mendukung izin tingkat sumber daya. Oleh karena itu, wildcard * dibutuhkan dalam `Resource`.
- `ec2:DescribeVpcs`Tindakan ditentukan untuk memberikan izin kepada pengguna yang akan menggunakan konsol untuk terhubung ke instance Anda menggunakan IPv6 alamat. Jika pengguna Anda hanya akan menggunakan IPv4 alamat publik, Anda dapat menghilangkannya`ec2:DescribeVpcs`. Perhatikan bahwa tindakan API `ec2:Describe*` tidak mendukung izin tingkat sumber daya. Oleh karena itu, wildcard * dibutuhkan dalam `Resource`.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": [
                "arn:aws:ec2:us-
east-1:111122223333:instance/i-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:111122223333:instance/i-0598c7d356eba48d7"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Izinkan pengguna untuk terhubung ke instans dengan tanda tertentu

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan tag yang dapat dilampirkan ke pengguna dan sumber daya. AWS Anda dapat menggunakan tanda sumber daya untuk mengontrol akses ke instans. Untuk informasi selengkapnya tentang penggunaan tag untuk mengontrol akses ke AWS sumber daya Anda, lihat Mengontrol akses ke AWS sumber daya di Panduan Pengguna IAM.

Dalam contoh kebijakan IAM berikut, tindakan `ec2-instance-connect:SendSSHPublicKey` memberikan izin kepada pengguna untuk terhubung ke instans apa pun (ditunjukkan oleh wildcard `*` di ARN sumber daya) dengan syarat instans memiliki tanda sumber daya dengan kunci=`tag-key` dan value=`tag-value`.

Tindakan `ec2:DescribeInstances` ditentukan untuk memberikan izin kepada pengguna yang akan menggunakan konsol untuk terhubung ke instans Anda. Jika pengguna Anda hanya akan menggunakan klien SSH untuk terhubung ke instance Anda, Anda dapat menghilangkannya.

`ec2:DescribeInstances` Perhatikan bahwa tindakan API `ec2:Describe*` tidak mendukung izin tingkat sumber daya. Oleh karena itu, wildcard `*` dibutuhkan dalam `Resource`.

`ec2:DescribeVpcs`Tindakan ditentukan untuk memberikan izin kepada pengguna yang akan menggunakan konsol untuk terhubung ke instance Anda menggunakan IPv6 alamat. Jika pengguna Anda hanya akan menggunakan IPv4 alamat publik, Anda dapat menghilangkannya`ec2:DescribeVpcs`. Perhatikan bahwa tindakan API `ec2:Describe*` tidak mendukung izin tingkat sumber daya. Oleh karena itu, wildcard `*` dibutuhkan dalam `Resource`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/tag-key": "tag-value"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Instal EC2 instans Connect pada instans EC2 Anda

Untuk terhubung ke instans Linux menggunakan EC2 Instance Connect, instans harus memiliki EC2 Instance Connect diinstal. Menginstal EC2 Instance Connect akan mengonfigurasi daemon SSH pada instans.

Untuk informasi selengkapnya tentang paket EC2 Instance Connect, lihat aws/aws-ec2 - di situs web. instance-connect-config GitHub

> **Note**
>
> Jika Anda mengonfigurasi pengaturan `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser` untuk autentikasi SSH, instalasi EC2 Instance Connect tidak akan memperbaruinya. Akibatnya, Anda tidak dapat menggunakan EC2 Instance Connect.

Instal prasyarat

Sebelum Anda menginstal EC2 Instance Connect, pastikan Anda memenuhi prasyarat berikut.

- Verifikasi bahwa instance menggunakan salah satu dari yang berikut:
  - Amazon Linux 2 sebelum versi 2.0.20190618*
  - AL2023 AMI minimal atau AMI Amazon ECS yang dioptimalkan
  - CentOS Stream 8 dan 9
  - macOS Sonoma sebelum 14.2.1, Ventura sebelum 13.6.3, dan Monterey sebelum 12.7.2
  - Red Hat Enterprise Linux (RHEL) 8 dan 9
  - Ubuntu 16.04 dan 18.04 *

  > **Tip**
  >
  > * Untuk Amazon Linux 2, macOS, dan Ubuntu: Jika Anda meluncurkan instans menggunakan versi yang lebih baru dari yang tercantum di atas, EC2 Instance Connect sudah diinstal sebelumnya dan tidak diperlukan instalasi manual.

- Verifikasi prasyarat umum untuk EC2 Instance Connect.

  Untuk informasi selengkapnya, lihat Prasyarat untuk EC2 Instance Connect.
- Verifikasi prasyarat untuk menghubungkan ke instans Anda menggunakan klien SSH di mesin lokal Anda.

  Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..
- Dapatkan ID instans.

Anda dapat memperoleh ID instans Anda menggunakan konsol Amazon EC2 (dari kolom ID instans). Jika mau, Anda dapat menggunakan perintah describe-instance (AWS CLI) atau Get-EC2Instance().AWS Tools for Windows PowerShell

Instal EC2 Instance Connect secara manual

> **Note**
>
> Jika Anda meluncurkan instans menggunakan salah satu AMI berikut, EC2 Instance Connect sudah diinstal sebelumnya dan Anda dapat melewati prosedur ini:
>
> - AL2023 standar AMI
> - Amazon Linux 2 2.0.20190618 atau setelahnya
> - macOS Sonoma 14.2.1 atau yang lebih baru
> - macOS Ventura 13.6.3 atau yang lebih baru
> - macOS Monterey 12.7.2 atau yang lebih baru
> - Ubuntu 20.04 atau setelahnya

Gunakan salah satu prosedur berikut untuk menginstal EC2 Instance Connect, tergantung pada sistem operasi instans Anda.

Amazon Linux 2

Untuk menginstal EC2 Instance Connect pada instans yang diluncurkan dengan Amazon Linux 2

1. Hubungkan ke instans Anda menggunakan SSH.

   Ganti contoh nilai dalam perintah berikut dengan nilai Anda. Gunakan key pair SSH yang ditetapkan ke instans Anda saat Anda meluncurkannya dan nama pengguna default AMI yang Anda gunakan untuk meluncurkan instans Anda. Untuk Amazon Linux 2, nama pengguna defaultnya adalah`ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

Untuk informasi selengkapnya tentang menghubungkan ke instans Anda, lihat Hubungkan ke instans Linux Anda menggunakan klien SSH.

2. Instal paket EC2 instans Connect di instans Anda.

```
[ec2-user ~]$ sudo yum install ec2-instance-connect
```

Anda akan melihat tiga skrip baru di folder `/opt/aws/bin/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

3. (Opsional) Memverifikasi bahwa EC2 Instance Connect berhasil diinstal pada instans Anda.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config
```

EC2 Instance Connect berhasil diinstal jika baris `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser` berisi nilai-nilai berikut:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` mengatur skrip `eic_run_authorized_keys` untuk mencari kunci dari metadata instans
- `AuthorizedKeysCommandUser` menetapkan pengguna sistem sebagai `ec2-instance-connect`

> **Note**
>
> Jika sebelumnya Anda mengonfigurasi `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser`, instalasi EC2 Instance Connect tidak akan mengubah nilainya dan Anda tidak akan dapat menggunakan EC2 Instance Connect.

CentOS

Untuk menginstal EC2 Instance Connect pada instans yang diluncurkan dengan CentOS

1. Hubungkan ke instans Anda menggunakan SSH.

   Ganti contoh nilai dalam perintah berikut dengan nilai Anda. Gunakan key pair SSH yang ditetapkan ke instans Anda saat Anda meluncurkannya dan nama pengguna default AMI yang Anda gunakan untuk meluncurkan instans Anda. Untuk CentOS, nama pengguna default adalah `centos` atau. `ec2-user`

   ```
   $ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Untuk informasi selengkapnya tentang terhubung ke instans Anda, lihat Hubungkan ke instans Linux Anda menggunakan klien SSH.

2. Jika Anda menggunakan proksi HTTP atau HTTPS, Anda harus mengatur variabel lingkungan `http_proxy` atau `https_proxy` di sesi shell saat ini.

   Jika Anda tidak menggunakan proksi, Anda dapat melewati langkah ini.

   - Untuk server proksi HTTP, jalankan perintah berikut:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Untuk server proksi HTTPS, jalankan perintah berikut:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Instal paket EC2 Instance Connect di instans Anda dengan menjalankan perintah berikut.

   File konfigurasi EC2 Instance Connect untuk CentOS disediakan dalam paket Red Hat Package Manager (RPM), dengan paket RPM berbeda untuk CentOS 8 dan CentOS 9 dan misalnya jenis yang Intel/AMD berjalan pada (x86_64) atau ARM (). AArch64

   Gunakan blok perintah untuk sistem operasi dan arsitektur CPU Anda.

   - CentOS 8

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
connect-2.0.0-5.rhel8.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

LENGAN (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel8.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- CentOS 9

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
connect-2.0.0-5.rhel9.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
```

```
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

LENGAN (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel9.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Anda akan melihat skrip baru berikut di folder `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opsional) Memverifikasi bahwa EC2 Instance Connect berhasil diinstal pada instans Anda.

   - Untuk CentOS 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/sshd.service.d/ec2-instance-
     connect.conf
     ```

   - Untuk CentOS 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   EC2 Instance Connect berhasil diinstal jika baris `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser` berisi nilai-nilai berikut:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

- `AuthorizedKeysCommand` mengatur skrip `eic_run_authorized_keys` untuk mencari kunci dari metadata instans
- `AuthorizedKeysCommandUser` menetapkan pengguna sistem sebagai `ec2-instance-connect`

> **Note**
>
> Jika sebelumnya Anda mengonfigurasi `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser`, instalasi EC2 Instance Connect tidak akan mengubah nilainya dan Anda tidak akan dapat menggunakan EC2 Instance Connect.

macOS

Untuk menginstal EC2 Instance Connect pada instans yang diluncurkan dengan macOS

1. Hubungkan ke instans Anda menggunakan SSH.

   Ganti contoh nilai dalam perintah berikut dengan nilai Anda. Gunakan key pair SSH yang ditetapkan ke instans Anda saat Anda meluncurkannya dan nama pengguna default AMI yang Anda gunakan untuk meluncurkan instans Anda. Untuk instance macOS, nama pengguna defaultnya adalah. `ec2-user`

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Untuk informasi selengkapnya tentang terhubung ke instans Anda, lihat Hubungkan ke instans Linux Anda menggunakan klien SSH.

2. Perbarui Homebrew menggunakan perintah berikut. Pembaruan akan mencantumkan perangkat lunak yang diketahui Homebrew. Paket EC2 Instance Connect disediakan melalui Homebrew pada instans macOS. Untuk informasi selengkapnya, lihat Perbarui sistem operasi dan perangkat lunak pada instans Amazon EC2 Mac.

   ```
   [ec2-user ~]$ brew update
   ```

3. Instal paket EC2 instans Connect di instans Anda. Ini akan menginstal perangkat lunak dan mengonfigurasi sshd untuk menggunakannya.

```
[ec2-user ~]$ brew install ec2-instance-connect
```

Anda akan melihat skrip baru berikut di folder `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opsional) Memverifikasi bahwa EC2 Instance Connect berhasil diinstal pada instans Anda.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect berhasil diinstal jika baris `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser` berisi nilai-nilai berikut:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` mengatur skrip `eic_run_authorized_keys` untuk mencari kunci dari metadata instans
- `AuthorizedKeysCommandUser` menetapkan pengguna sistem sebagai `ec2-instance-connect`

> **Note**
>
> Jika sebelumnya Anda mengonfigurasi `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser`, instalasi EC2 Instance Connect tidak akan mengubah nilainya dan Anda tidak akan dapat menggunakan EC2 Instance Connect.

RHEL

Untuk menginstal EC2 Instance Connect pada instans yang diluncurkan dengan Red Hat Enterprise Linux (RHEL)

1. Hubungkan ke instans Anda menggunakan SSH.

   Ganti contoh nilai dalam perintah berikut dengan nilai Anda. Gunakan key pair SSH yang ditetapkan ke instans Anda saat Anda meluncurkannya dan nama pengguna default AMI

yang Anda gunakan untuk meluncurkan instans Anda. Untuk RHEL, nama pengguna default adalah `ec2-user` atau`root`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Untuk informasi selengkapnya tentang terhubung ke instans Anda, lihat Hubungkan ke instans Linux Anda menggunakan klien SSH.

2. Jika Anda menggunakan proksi HTTP atau HTTPS, Anda harus mengatur variabel lingkungan `http_proxy` atau `https_proxy` di sesi shell saat ini.

   Jika Anda tidak menggunakan proksi, Anda dapat melewati langkah ini.

   - Untuk server proksi HTTP, jalankan perintah berikut:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Untuk server proksi HTTPS, jalankan perintah berikut:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Instal paket EC2 Instance Connect di instans Anda dengan menjalankan perintah berikut.

   File konfigurasi EC2 Instance Connect untuk RHEL disediakan dalam paket Red Hat Package Manager (RPM), dengan paket RPM berbeda untuk RHEL 8 dan RHEL 9 dan misalnya tipe yang berjalan pada Intel/AMD (x86_64) atau ARM (). AArch64

   Gunakan blok perintah untuk sistem operasi dan arsitektur CPU Anda.

   - RHEL 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
     west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
     connect-2.0.0-5.rhel8.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm
     ```

```
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

LENGAN (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel8.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- RHEL 9

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
connect-2.0.0-5.rhel9.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  LENGAN (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
```

```
connect-2.0.0-5.rhel9.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Anda akan melihat skrip baru berikut di folder `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opsional) Memverifikasi bahwa EC2 Instance Connect berhasil diinstal pada instans Anda.

   - Untuk RHEL 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/sshd.service.d/ec2-instance-
     connect.conf
     ```

   - Untuk RHEL 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   EC2 Instance Connect berhasil diinstal jika baris `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser` berisi nilai-nilai berikut:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

   - `AuthorizedKeysCommand` mengatur skrip `eic_run_authorized_keys` untuk mencari kunci dari metadata instans
   - `AuthorizedKeysCommandUser` menetapkan pengguna sistem sebagai `ec2-instance-connect`

> **Note**
>
> Jika sebelumnya Anda mengonfigurasi `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser`, instalasi EC2 Instance Connect tidak akan mengubah nilainya dan Anda tidak akan dapat menggunakan EC2 Instance Connect.

Ubuntu

Untuk menginstal EC2 Instance Connect pada instans yang diluncurkan dengan Ubuntu 16.04 atau setelahnya

1. Hubungkan ke instans Anda menggunakan SSH.

   Ganti contoh nilai dalam perintah berikut dengan nilai Anda. Gunakan key pair SSH yang ditetapkan ke instans Anda saat Anda meluncurkannya dan gunakan nama pengguna default AMI yang Anda gunakan untuk meluncurkan instans Anda. Untuk AMI Ubuntu, nama penggunanya adalah`ubuntu`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Untuk informasi selengkapnya tentang menghubungkan ke instans Anda, lihat Hubungkan ke instans Linux Anda menggunakan klien SSH.

2. (Opsional) Pastikan instans Anda memiliki AMI Ubuntu terbaru.

   Jalankan perintah berikut untuk memperbarui semua paket pada instans Anda.

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```

3. Instal paket EC2 instans Connect di instans Anda.

   ```
   ubuntu:~$ sudo apt-get install ec2-instance-connect
   ```

   Anda akan melihat tiga skrip baru di folder `/usr/share/ec2-instance-connect/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

4. (Opsional) Memverifikasi bahwa EC2 Instance Connect berhasil diinstal pada instans Anda.

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

EC2 Instance Connect berhasil diinstal jika baris `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser` berisi nilai-nilai berikut:

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` mengatur skrip `eic_run_authorized_keys` untuk mencari kunci dari metadata instans
- `AuthorizedKeysCommandUser` menetapkan pengguna sistem sebagai `ec2-instance-connect`

> **Note**
>
> Jika sebelumnya Anda mengonfigurasi `AuthorizedKeysCommand` dan `AuthorizedKeysCommandUser`, instalasi EC2 Instance Connect tidak akan mengubah nilainya dan Anda tidak akan dapat menggunakan EC2 Instance Connect.

Connect ke instans Linux menggunakan EC2 Instance Connect

Petunjuk berikut menjelaskan cara menyambung ke instans Linux menggunakan EC2 Instance Connect melalui konsol Amazon EC2, klien SSH, AWS CLI atau SSH.

Saat Anda terhubung ke instans menggunakan EC2 Instance Connect melalui konsol atau AWS CLI, EC2 Instance Connect API secara otomatis akan mendorong kunci publik SSH ke metadata instans selama 60 detik. Kebijakan IAM yang dilampirkan pada pengguna Anda mengizinkan tindakan ini. Jika Anda lebih suka menggunakan kunci SSH Anda sendiri, Anda dapat menggunakan klien SSH dan secara eksplisit mendorong kunci SSH Anda ke instans menggunakan EC2 Instance Connect.

Pertimbangan-pertimbangan

Setelah menghubungkan ke instans menggunakan EC2 Instance Connect, koneksi tetap ada hingga sesi SSH dihentikan. Durasi koneksi tidak ditentukan oleh durasi kredenal IAM Anda. Jika kredensil IAM Anda kedaluwarsa, koneksi terus berlanjut. Saat menggunakan pengalaman konsol EC2 Instance Connect, jika kredensyal IAM Anda kedaluwarsa, hentikan koneksi dengan menutup halaman browser. Saat menggunakan klien SSH Anda sendiri dan EC2 Instance Connect untuk menekan kunci Anda, Anda dapat menetapkan nilai batas waktu SSH untuk mengakhiri sesi SSH secara otomatis.

Persyaratan

Sebelum Anda mulai, pastikan untuk meninjau prasyarat.

Opsi koneksi

- Hubungkan menggunakan konsol Amazon EC2
- Connect menggunakan AWS CLI
- Hubungkan menggunakan kunci Anda sendiri dan klien SSH
- Pemecahan Masalah

Hubungkan menggunakan konsol Amazon EC2

Anda dapat menyambung ke instans menggunakan EC2 Instance Connect melalui konsol Amazon EC2.

Persyaratan

Untuk terhubung menggunakan konsol Amazon EC2, instans harus memiliki publik IPv4 atau IPv6 alamat. Jika instans hanya memiliki IPv4 alamat pribadi, Anda dapat menggunakan AWS CLI ec2-instance-connect untuk terhubung.

Untuk menyambung ke instans Anda menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Hubungkan.
4. Pilih tab EC2 Instance Connect.
5. Pilih Connect menggunakan IP Publik.

6. Jika ada pilihan, pilih alamat IP untuk terhubung. Jika tidak, alamat IP dipilih secara otomatis.
7. Untuk Nama Pengguna, verifikasi nama pengguna.
8. Pilih Connect untuk membuat koneksi. Jendela terminal dalam peramban akan terbuka.

Connect menggunakan AWS CLI

Anda dapat menggunakan ec2-instance-connect AWS CLI untuk terhubung ke instans Anda dengan klien SSH. EC2 Instance Connect mencoba membuat koneksi menggunakan alamat IP yang tersedia dalam urutan yang telah ditentukan, berdasarkan jenis koneksi yang ditentukan. Jika alamat IP tidak tersedia, secara otomatis mencoba yang berikutnya dalam urutan.

Tipe koneksi

`auto` (default)

EC2 Instance Connect mencoba menghubungkan menggunakan alamat IP instans dalam urutan berikut dan dengan jenis koneksi yang sesuai:

1. Publik IPv4: `direct`
2. Pribadi IPv4: `eice`
3. IPv6: `direct`

`direct`

EC2 Instance Connect mencoba untuk terhubung menggunakan alamat IP instans dalam urutan sebagai berikut:

1. Publik IPv4
2. IPv6
3. IPv4 pribadi (tidak terhubung melalui EC2 Instance Connect Endpoint)

`eice`

EC2 Instance Connect mencoba untuk terhubung menggunakan IPv4 alamat pribadi instans dan titik akhir EC2 Instance Connect.

> **Note**
>
> Di masa depan, kita mungkin mengubah perilaku jenis `auto` koneksi. Untuk memastikan bahwa jenis koneksi yang Anda inginkan digunakan, kami sarankan Anda secara eksplisit mengatur `--connection-type` ke salah satu atau`direct`. `eice`

Persyaratan

Anda harus menggunakan AWS CLI versi 2. Untuk informasi selengkapnya, lihat Menginstal atau memperbarui ke versi terbaru AWS CLI.

Untuk terhubung ke instans menggunakan ID instans

Jika Anda hanya mengetahui ID instans, dan ingin membiarkan EC2 Instance Connect menentukan jenis koneksi yang akan digunakan saat menghubungkan ke instance Anda, gunakan perintah ec2-instance-connect ssh CLI dengan ID instance.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

Untuk menghubungkan ke instans menggunakan ID instans dan EC2 Instance Connect Endpoint

Jika Anda ingin terhubung ke instans Anda melalui EC2 Instance Connect Endpoint, gunakan perintah sebelumnya dan tentukan juga parameter `--connection-type` dengan nilai `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Untuk terhubung ke instans menggunakan ID instans dan file kunci privat Anda sendiri

Jika Anda ingin terhubung ke instans Anda melalui Titik Akhir Connect instans EC2 menggunakan kunci pribadi Anda sendiri, tentukan ID instans dan jalur ke file kunci pribadi. Jangan sertakan *`file://`* di jalur; contoh berikut akan gagal:*`file:///path/to/key`*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /
path/to/key.pem
```

> **Tip**
>
> Jika Anda mendapatkan kesalahan saat menggunakan perintah ini, pastikan Anda menggunakan AWS CLI versi 2, karena `ssh` perintah hanya tersedia di versi utama ini. Kami

juga merekomendasikan memperbarui secara teratur ke versi minor terbaru dari AWS CLI versi 2 untuk mengakses fitur-fitur terbaru. Untuk informasi selengkapnya, lihat Tentang AWS CLI versi 2 di Panduan AWS Command Line Interface Pengguna.

Hubungkan menggunakan kunci Anda sendiri dan klien SSH

Anda dapat menggunakan kunci SSH Anda sendiri dan terhubung ke instans Anda dari klien SSH pilihan Anda jika menggunakan API EC2 Instance Connect. Hal ini memungkinkan Anda memanfaatkan kemampuan EC2 Instance Connect untuk mendorong kunci publik ke instans. Metode koneksi ini bekerja untuk instans dengan alamat IP privat dan publik.

Persyaratan

- Ketentuan untuk pasangan kunci
  - Jenis yang didukung: RSA (SSH2OpenSSH dan) dan ED25519
  - Panjang yang didukung: 2048 dan 4096.
  - Untuk informasi selengkapnya, lihat Membuat pasangan kunci menggunakan alat pihak ketiga dan mengimpor kunci publik ke Amazon EC2.
- Saat menghubungkan ke instance yang hanya memiliki alamat IP pribadi, komputer lokal tempat Anda memulai sesi SSH harus memiliki konektivitas ke titik akhir layanan EC2 Instance Connect (untuk mendorong kunci publik SSH Anda ke instance) serta konektivitas jaringan ke alamat IP pribadi instans untuk membuat sesi SSH. Endpoint layanan EC2 Instance Connect dapat dijangkau melalui internet atau melalui antarmuka Direct Connect virtual publik. Untuk terhubung ke alamat IP privat instans, Anda dapat memanfaatkan layanan seperti Direct Connect, AWS Site-to-Site VPN, atau VPC peering.

Untuk terhubung ke instans Anda menggunakan kunci Anda sendiri dan klien SSH apa pun

1. (Opsional) Hasilkan kunci privat dan publik SSH baru

   Anda dapat menghasilkan kunci privat dan publik SSH baru, `my_key` dan `my_key.pub`, menggunakan perintah berikut:

   ```
   ssh-keygen -t rsa -f my_key
   ```

2. Dorong kunci publik SSH Anda ke instans

   Gunakan perintah send-ssh-public-key untuk mendorong kunci publik SSH Anda ke instans. Jika Anda meluncurkan instans menggunakan AL2023 atau Amazon Linux 2, nama pengguna default untuk AMI adalah`ec2-user`. Jika Anda meluncurkan instans Anda menggunakan Ubuntu, nama pengguna default untuk AMI adalah`ubuntu`.

   Contoh berikut mendorong kunci publik ke instans yang ditentukan di Zona Ketersediaan yang ditentukan, untuk mengautentikasi `ec2-user`.

   ```
   aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. Hubungkan ke instans menggunakan kunci privat Anda

   Gunakan perintah ssh untuk terhubung ke instans menggunakan kunci privat sebelum kunci publik dihapus dari metadata instans (Anda memiliki waktu 60 detik sebelum kunci dihapus). Tentukan kunci pribadi yang sesuai dengan kunci publik, nama pengguna default untuk AMI yang Anda gunakan untuk meluncurkan instans Anda, dan nama DNS publik instans (jika menghubungkan melalui jaringan pribadi, tentukan nama DNS pribadi atau alamat IP). Tambahkan opsi `IdentitiesOnly=yes` untuk memastikan bahwa hanya file dalam konfigurasi ssh dan kunci tertentu yang digunakan untuk koneksi tersebut.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

   Contoh berikut digunakan `timeout 3600` untuk mengatur sesi SSH Anda untuk mengakhiri setelah 1 jam. Proses yang dimulai selama sesi dapat terus berjalan pada instans Anda setelah sesi berakhir.

   ```
   timeout 3600 ssh -o “IdentitiesOnly=yes” -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

Pemecahan Masalah

Jika Anda menerima kesalahan saat mencoba untuk terhubung ke instans Anda, lihat hal berikut:

- Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda
- Bagaimana cara memecahkan masalah menghubungkan ke instans EC2 saya menggunakan EC2 instans Connect?

Hapus instalasi EC2 Instance Connect

Untuk menonaktifkan EC2 Instance Connect, sambungkan ke instans Linux Anda dan hapus instalan `ec2-instance-connect` paket yang diinstal pada OS. Jika konfigurasi `sshd` cocok dengan pengaturan saat Anda menginstal EC2 Instance Connect, menghapus instalan `ec2-instance-connect` berarti juga menghapus konfigurasi `sshd`. Jika Anda memodifikasi konfigurasi `sshd` setelah menginstal EC2 Instance Connect, Anda harus memperbaruinya secara manual.

Amazon Linux

Anda dapat menghapus instalasi EC2 Instance Connect di AL2023 dan Amazon Linux 2 2.0.20190618 atau setelahnya, tempat EC2 Instance Connect telah dikonfigurasi sebelumnya.

Untuk menghapus instans EC2 Connect pada instans yang diluncurkan menggunakan Amazon Linux

1. Hubungkan ke instans Anda menggunakan SSH. Tentukan key pair SSH yang Anda gunakan untuk instans saat meluncurkannya dan nama pengguna default untuk AL2023 atau Amazon Linux 2 AMI, yaitu`ec2-user`.

   Misalnya, perintah ssh berikut ini terhubung ke instans dengan nama DNS publik `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, menggunakan pasangan kunci `my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Copot instalasi paket `ec2-instance-connect` menggunakan perintah yum.

   ```
   [ec2-user ~]$ sudo yum remove ec2-instance-connect
   ```

Ubuntu

Untuk menghapus instans EC2 Connect pada instans yang diluncurkan menggunakan AMI Ubuntu

1. Hubungkan ke instans Anda menggunakan SSH. Tentukan key pair SSH yang Anda gunakan untuk instans Anda saat Anda meluncurkannya dan nama pengguna default untuk AMI Ubuntu, yaituubuntu.

   Misalnya, perintah ssh berikut ini terhubung ke instans dengan nama DNS publik `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, menggunakan pasangan kunci `my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Copot instalasi paket `ec2-instance-connect` menggunakan perintah apt-get.

   ```
   ubuntu:~$ sudo apt-get remove ec2-instance-connect
   ```

Connect ke instans Anda menggunakan alamat IP pribadi dan EC2 Instance Connect Endpoint

EC2 Instance Connect Endpoint memungkinkan Anda terhubung dengan aman ke instans dari internet, tanpa menggunakan host bastion, atau mengharuskan virtual private cloud (VPC) Anda memiliki konektivitas internet langsung.

Manfaat

- Anda dapat terhubung ke instans Anda tanpa mengharuskan instans memiliki publik IPv4 atau IPv6 alamat. AWS mengenakan biaya untuk semua IPv4 alamat publik, termasuk IPv4 alamat publik yang terkait dengan instans yang sedang berjalan dan alamat IP Elastis. Untuk informasi selengkapnya, lihat tab IPv4 Alamat Publik di halaman harga Amazon VPC.
- Anda dapat terhubung ke instans Anda dari internet tanpa mengharuskan VPC Anda memiliki konektivitas internet langsung melalui gateway internet.
- Anda dapat mengontrol akses ke pembuatan dan penggunaan Titik Akhir Connect Instance EC2 untuk menyambung ke instans menggunakan kebijakan dan izin IAM.

- Semua upaya untuk terhubung ke instans Anda, baik yang berhasil maupun yang tidak berhasil, dicatat. CloudTrail

Harga

Tidak ada biaya tambahan untuk menggunakan EC2 Instance Connect Endpoint. Jika Anda menggunakan Titik Akhir Connect Instance EC2 untuk menyambung ke instans di Availability Zone yang berbeda, akan dikenakan biaya tambahan untuk transfer data di seluruh Availability Zone.

Daftar Isi

- Cara kerjanya
- Pertimbangan-pertimbangan
- Berikan izin untuk menggunakan EC2 Instance Connect Endpoint
- Grup keamanan untuk EC2 Instans Connect Endpoint
- Membuat EC2 Instance Connect Endpoint
- Memodifikasi Titik Akhir Connect Instance EC2
- Menghapus Titik Akhir Connect Instance EC2
- Connect ke instans Amazon EC2 menggunakan EC2 Instance Connect Endpoint
- Koneksi log dibuat melalui EC2 Instance Connect Endpoint
- Peran tertaut layanan untuk EC2 Instance Connect Endpoint
- Kuota untuk EC2 Instance Connect Endpoint

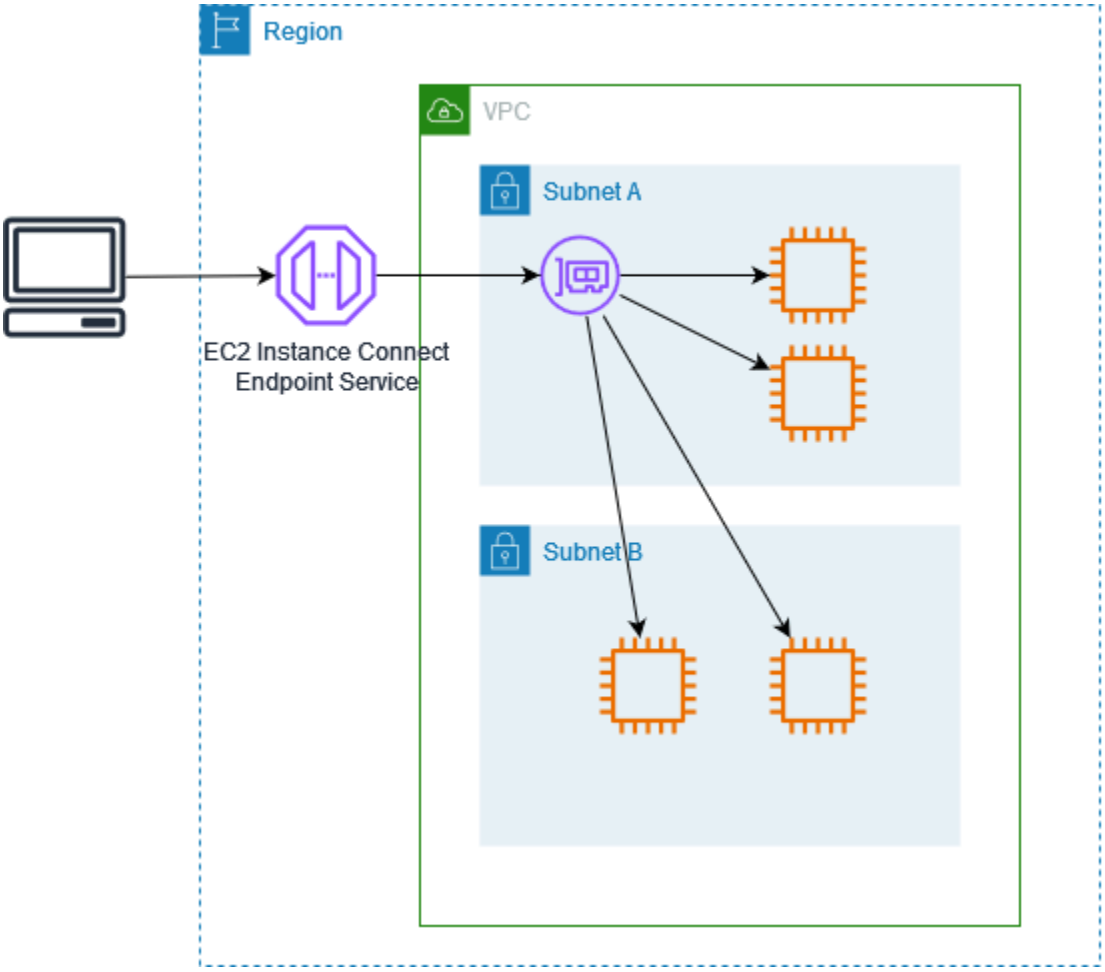
Cara kerjanya

EC2 Instance Connect Endpoint adalah proxy TCP yang sadar identitas. Layanan Endpoint Connect Instance Connect EC2 membuat terowongan pribadi dari komputer Anda ke titik akhir menggunakan kredensil untuk entitas IAM Anda. Lalu lintas diautentikasi dan diotorisasi sebelum mencapai VPC Anda.

Anda dapat mengonfigurasi aturan grup keamanan tambahan untuk membatasi lalu lintas masuk ke instans Anda. Misalnya, Anda dapat menggunakan aturan masuk untuk mengizinkan lalu lintas pada port manajemen hanya dari EC2 Instance Connect Endpoint.

Anda dapat mengonfigurasi aturan tabel rute untuk memungkinkan titik akhir terhubung ke instance apa pun di subnet VPC mana pun.

Diagram berikut menunjukkan bagaimana pengguna dapat terhubung ke instans mereka dari internet menggunakan EC2 Instance Connect Endpoint. Pertama, buat EC2 Instance Connect Endpoint di subnet A. Kami membuat antarmuka jaringan untuk endpoint di subnet, yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan untuk instans Anda di VPC. Jika tabel rute untuk subnet B memungkinkan lalu lintas dari subnet A, maka Anda dapat menggunakan titik akhir untuk mencapai instance di subnet B.



Pertimbangan-pertimbangan

Sebelum Anda mulai, pertimbangkan hal berikut.

- EC2 Instance Connect Endpoint ditujukan khusus untuk kasus penggunaan lalu lintas manajemen, bukan untuk transfer data volume tinggi. Data volume tinggi transfer dibatasi.
- Anda dapat membuat EC2 Instance Connect Endpoint untuk mendukung lalu lintas ke instans yang memiliki IPv4 alamat atau IPv6 alamat pribadi. Jenis alamat IP dari titik akhir harus sesuai dengan alamat IP instance. Anda dapat membuat endpoint yang mendukung semua jenis alamat IP.

- (Instance Linux) Jika Anda menggunakan key pair Anda sendiri, Anda dapat menggunakan AMI Linux apa pun. Jika tidak, instans Anda harus menginstal EC2 Instance Connect. Untuk informasi tentang AMI mana yang menyertakan EC2 Instance Connect dan cara menginstalnya pada AMI lain yang didukung AMIs, lihatMenginstal EC2 Instance Connect.
- Anda dapat menetapkan grup keamanan ke EC2 Instance Connect Endpoint. Jika tidak, kami menggunakan grup keamanan default untuk VPC. Grup keamanan untuk Titik Akhir Connect Instans EC2 harus mengizinkan lalu lintas keluar ke instans tujuan. Untuk informasi selengkapnya, lihat Grup keamanan untuk EC2 Instans Connect Endpoint.
- Anda dapat mengonfigurasi EC2 Instance Connect Endpoint untuk mempertahankan alamat IP sumber klien saat merutekan permintaan ke instans. Jika tidak, alamat IP antarmuka jaringan menjadi alamat IP klien untuk semua lalu lintas yang masuk.
  - Jika Anda mengaktifkan pelestarian IP klien, grup keamanan untuk instance harus mengizinkan lalu lintas dari klien. Selain itu, instans harus berada dalam VPC yang sama dengan EC2 Instance Connect Endpoint.
  - Jika Anda mematikan pelestarian IP klien, grup keamanan untuk instance harus mengizinkan lalu lintas dari VPC. Ini adalah opsi default.
  - Pelestarian IP klien hanya didukung pada IPv4 EC2 Instance Connect Endpoints. Untuk menggunakan pelestarian IP klien, jenis alamat IP dari EC2 Instance Connect Endpoint harus. IPv4 Pelestarian IP klien tidak didukung ketika jenis alamat IP adalah dual-stack atau. IPv6
  - Jenis contoh berikut tidak mendukung pelestarian IP klien: C1, CG1, CG2, G1, HI1, M1, M2, M3, dan T1. Jika Anda mengaktifkan pelestarian IP klien dan mencoba menyambung ke instans dengan salah satu jenis instans ini menggunakan EC2 Instance Connect Endpoint, koneksi akan gagal.
  - Pelestarian IP klien tidak didukung saat lalu lintas dirutekan melalui gateway transit.
- Saat Anda membuat Titik Akhir Connect Instance EC2, peran yang ditautkan layanan akan dibuat secara otomatis untuk layanan Amazon EC2 di (IAM). AWS Identity and Access Management Amazon EC2 menggunakan peran tertaut layanan untuk menyediakan antarmuka jaringan di akun Anda, yang diperlukan saat membuat EC2 Instance Connect Endpoints. Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk EC2 Instance Connect Endpoint.
- Anda hanya dapat membuat 1 EC2 Instance Connect Endpoint per VPC dan per subnet. Untuk informasi selengkapnya, lihat Kuota untuk EC2 Instance Connect Endpoint. Jika Anda perlu membuat Endpoint Connect Instance EC2 lain di Availability Zone yang berbeda dalam VPC yang sama, Anda harus terlebih dahulu menghapus Titik Akhir Instance Connect EC2 yang ada. Jika tidak, Anda akan menerima kesalahan kuota.

- Setiap EC2 Instance Connect Endpoint dapat mendukung hingga 20 koneksi bersamaan.
- Durasi maksimum untuk koneksi TCP yang ditetapkan adalah 1 jam (3.600 detik). Anda dapat menentukan durasi maksimum yang diizinkan dalam kebijakan IAM, yang dapat mencapai 3.600 detik. Untuk informasi selengkapnya, lihat Izin untuk menggunakan EC2 Instance Connect Endpoint untuk menyambung ke instans.

  Durasi koneksi tidak ditentukan oleh durasi kredenal IAM Anda. Jika kredensil IAM Anda kedaluwarsa, koneksi terus berlanjut hingga durasi maksimum yang ditentukan tercapai. Saat Anda terhubung ke instans menggunakan pengalaman konsol EC2 Instance Connect Endpoint, setel durasi terowongan Maks (detik) ke nilai yang kurang dari durasi kredenal IAM Anda. Jika kredensil IAM Anda kedaluwarsa lebih awal, hentikan koneksi ke instans Anda dengan menutup halaman browser.

Berikan izin untuk menggunakan EC2 Instance Connect Endpoint

Secara default, entitas IAM tidak memiliki izin untuk membuat, mendeskripsikan, atau memodifikasi Titik Akhir Connect Instance EC2. Administrator IAM dapat membuat kebijakan IAM yang memberikan izin yang diperlukan untuk melakukan tindakan tertentu pada sumber daya yang mereka butuhkan.

Untuk informasi tentang pembuatan kebijakan IAM, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Contoh kebijakan berikut menunjukkan bagaimana Anda dapat mengontrol izin yang dimiliki pengguna untuk EC2 Instance Connect Endpoint.

Contoh

- Izin untuk membuat, mendeskripsikan, memodifikasi, dan menghapus EC2 Instance Connect Endpoint
- Izin untuk menggunakan EC2 Instance Connect Endpoint untuk menyambung ke instans
- Izin untuk terhubung hanya dari rentang alamat IP tertentu

Izin untuk membuat, mendeskripsikan, memodifikasi, dan menghapus EC2 Instance Connect Endpoint

Untuk membuat dan memodifikasi Titik Akhir Connect Instance EC2, pengguna memerlukan izin untuk tindakan berikut:

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `ec2:ModifyInstanceConnectEndpoint`
- `iam:CreateServiceLinkedRole`

Untuk mendeskripsikan dan menghapus EC2 Instance Connect Endpoint, pengguna memerlukan izin untuk tindakan berikut:

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

Anda dapat membuat kebijakan yang memberikan izin untuk membuat, mendeskripsikan, memodifikasi, dan menghapus EC2 Instance Connect Endpoint di semua subnet. Atau, Anda dapat membatasi tindakan untuk subnet tertentu hanya dengan menentukan subnet ARNs sebagai diizinkan `Resource` atau dengan menggunakan kunci kondisi. `ec2:SubnetID` Anda juga dapat menggunakan kunci syarat `aws:ResourceTag` untuk secara eksplisit mengizinkan atau menolak pembuatan titik akhir dengan tanda tertentu. Untuk informasi selengkapnya, lihat Kebijakan dan izin di IAM pada Panduan Pengguna IAM.

Contoh kebijakan IAM

Dalam contoh berikut kebijakan IAM, `Resource` bagian memberikan izin untuk membuat, memodifikasi, dan menghapus titik akhir di semua subnet, yang ditentukan oleh tanda bintang (). * Tindakan API `ec2:Describe*` tidak mendukung izin tingkat sumber daya. Oleh karena itu, wildcard * dibutuhkan dalam `Resource`.

Izin untuk menggunakan EC2 Instance Connect Endpoint untuk menyambung ke instans

Tindakan `ec2-instance-connect:OpenTunnel` tersebut memberikan izin untuk membuat koneksi TCP ke instans untuk terhubung melalui EC2 Instance Connect Endpoint. Anda dapat menentukan EC2 Instance Connect Endpoint untuk digunakan. Atau, `Resource` dengan tanda bintang (*) memungkinkan pengguna untuk menggunakan semua EC2 Instance Connect Endpoint yang tersedia. Anda juga dapat membatasi akses ke instans berdasarkan ada atau tidak adanya tanda sumber daya sebagai kunci syarat.

Kondisi

- `ec2-instance-connect:remotePort`— Port pada instance yang dapat digunakan untuk membuat koneksi TCP. Ketika kunci syarat ini digunakan, percobaan untuk terhubung ke instans pada port lain selain port yang ditentukan dalam kebijakan akan mengakibatkan kegagalan.
- `ec2-instance-connect:privateIpAddress`— Alamat IP pribadi tujuan yang terkait dengan instance yang ingin Anda buat koneksi TCP. Anda dapat menentukan satu alamat IP, seperti`10.0.0.1/32`, atau rentang IPs melalui CIDRs, seperti`10.0.1.0/28`. Ketika kunci syarat ini digunakan, percobaan untuk terhubung ke sebuah instans dengan alamat IP privat yang berbeda atau di luar rentang CIDR akan mengakibatkan kegagalan.
- `ec2-instance-connect:maxTunnelDuration`— Durasi maksimum untuk koneksi TCP yang ditetapkan. Satuannya adalah detik dan durasinya berkisar dari minimal 1 detik hingga maksimum 3.600 detik (1 jam). Jika kondisi tidak ditentukan, durasi default diatur ke 3.600 detik (1 jam). Mencoba terhubung ke instans lebih lama dari durasi yang ditentukan dalam kebijakan IAM atau lebih lama dari maksimum default akan menghasilkan kegagalan. Koneksi terputus setelah durasi yang ditentukan.

  Jika `maxTunnelDuration` ditentukan dalam kebijakan IAM dan nilai yang ditentukan kurang dari 3.600 detik (default), maka Anda harus menentukan `--max-tunnel-duration` dalam perintah saat menghubungkan ke sebuah instans. Untuk informasi selengkapnya tentang terhubung ke instans Anda, lihat Connect ke instans Amazon EC2 menggunakan EC2 Instance Connect Endpoint.

Anda juga dapat memberikan akses pengguna untuk membuat koneksi ke instans berdasarkan keberadaan tag sumber daya pada Titik Akhir Connect Instance EC2. Untuk informasi selengkapnya, lihat Kebijakan dan izin di IAM dalam Panduan Pengguna IAM.

Untuk instance Linux, `ec2-instance-connect:SendSSHPublicKey` tindakan memberikan izin untuk mendorong kunci publik ke sebuah instance. Kondisi `ec2:osuser` menentukan nama pengguna OS (sistem operasi) yang dapat mendorong kunci publik ke sebuah instans. Gunakan nama pengguna default untuk AMI yang Anda gunakan untuk meluncurkan instance. Untuk informasi selengkapnya, lihat Berikan izin IAM untuk EC2 instans Connect.

Contoh kebijakan IAM

Contoh berikut kebijakan IAM mengizinkan prinsipal IAM untuk terhubung ke instance hanya menggunakan Titik Akhir Connect Instance EC2 yang ditentukan, yang diidentifikasi oleh ID titik

akhir yang ditentukan. `eice-123456789abcdef` Koneksi berhasil dibuat hanya jika semua kondisi terpenuhi.

> **Note**
>
> Tindakan API `ec2:Describe*` tidak mendukung izin tingkat sumber daya. Oleh karena itu, wildcard `*` dibutuhkan dalam `Resource`.

Linux

Contoh ini mengevaluasi jika koneksi ke instance dibuat pada —port 22 (SSH), jika alamat IP pribadi instance berada dalam kisaran `10.0.1.0/31` (antara `10.0.1.0` dan`10.0.1.1`), dan kurang dari atau sama dengan detik. `maxTunnelDuration` `3600` Koneksi terputus setelah `3600` detik (1 jam).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
```

```
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Windows

Contoh ini mengevaluasi jika koneksi ke instance dibuat pada port 3389 (RDP), jika alamat IP pribadi dari instance terletak dalam kisaran `10.0.1.0/31` (antara `10.0.1.0` dan`10.0.1.1`), dan kurang dari atau sama `maxTunnelDuration` dengan detik. `3600` Koneksi terputus setelah `3600` detik (1 jam).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
```

```
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Izin untuk terhubung hanya dari rentang alamat IP tertentu

Contoh kebijakan IAM berikut memungkinkan pengguna utama IAM untuk terhubung ke instans dengan syarat instans tersebut terhubung dari alamat IP dalam rentang alamat IP yang ditentukan dalam kebijakan. Jika panggilan utama IAM `OpenTunnel` dari alamat IP yang tidak berada di dalam `192.0.2.0/24` (contoh rentang alamat IP dalam kebijakan ini), responsnya adalah`Access Denied`. Untuk informasi selengkapnya, lihat `aws:SourceIp` dalam Panduan Pengguna IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                },
```

```
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Grup keamanan untuk EC2 Instans Connect Endpoint

Grup keamanan mengontrol lalu lintas yang diizinkan untuk mencapai dan meninggalkan sumber daya yang terkait dengannya. Misalnya, kami menolak lalu lintas ke dan dari instans Amazon EC2 kecuali diizinkan secara khusus oleh grup keamanan yang terkait dengan instans tersebut.

Contoh berikut menunjukkan cara mengonfigurasi aturan grup keamanan untuk Titik Akhir Connect Instance Connect EC2 dan instance target.

Contoh

- Aturan grup keamanan EC2 Instance Connect Endpoint
- Aturan grup keamanan instans target

Aturan grup keamanan EC2 Instance Connect Endpoint

Aturan grup keamanan untuk Titik Akhir Connect Instans EC2 harus mengizinkan lalu lintas keluar yang ditujukan untuk instans target untuk meninggalkan titik akhir. Anda dapat menentukan grup keamanan instans IPv4 atau rentang IPv6 alamat VPC sebagai tujuan.

Lalu lintas ke titik akhir berasal dari Layanan Titik Akhir Connect Instance Connect EC2, dan itu diizinkan terlepas dari aturan masuk untuk grup keamanan titik akhir. Untuk mengontrol siapa yang dapat menggunakan EC2 Instance Connect Endpoint untuk menyambung ke instans, gunakan kebijakan IAM. Untuk informasi selengkapnya, lihat Izin untuk menggunakan EC2 Instance Connect Endpoint untuk menyambung ke instans.

Contoh aturan keluar: Referensi grup keamanan

Contoh berikut menggunakan referensi grup keamanan, yang berarti bahwa tujuan adalah grup keamanan yang terkait dengan instance target. Aturan ini memungkinkan lalu lintas keluar dari titik akhir ke semua instance yang menggunakan grup keamanan ini.

Protokol	Tujuan	Rentang port	Komentar
TCP	*ID of instance security group*	22	Mengizinkan lalu lintas SSH keluar ke semua instance yang terkait dengan grup keamanan instance

Contoh aturan keluar: rentang IPv4 alamat

Contoh berikut memungkinkan lalu lintas keluar ke rentang IPv4 alamat yang ditentukan. IPv4 Alamat instance ditetapkan dari subnetnya, sehingga Anda dapat menggunakan rentang IPv4 alamat VPC.

Protokol	Tujuan	Rentang port	Komentar
TCP	*VPC IPv4 CIDR*	22	Memungkinkan lalu lintas SSH keluar ke VPC

Contoh aturan keluar: rentang IPv6 alamat

Contoh berikut memungkinkan lalu lintas keluar ke rentang IPv6 alamat yang ditentukan. IPv6 Alamat instance ditetapkan dari subnetnya, sehingga Anda dapat menggunakan rentang IPv6 alamat VPC.

Protokol	Tujuan	Rentang port	Komentar
TCP	*VPC IPv6 CIDR*	22	Memungkinkan lalu lintas SSH keluar ke VPC

Aturan grup keamanan instans target

Aturan grup keamanan untuk instans target harus mengizinkan lalu lintas masuk dari Titik Akhir Connect Instans EC2. Anda dapat menentukan grup keamanan titik akhir atau rentang IPv6 alamat sebagai sumbernya. IPv4 Jika Anda menentukan rentang IPv4 alamat, sumbernya tergantung pada apakah pelestarian IP klien tidak aktif atau aktif. Untuk informasi selengkapnya, lihat Pertimbangan-pertimbangan.

Karena grup keamanan stateful, lalu lintas respons diizinkan untuk meninggalkan VPC terlepas dari aturan keluar untuk grup keamanan instance.

Contoh aturan masuk: Referensi grup keamanan

Contoh berikut menggunakan referensi grup keamanan, yang berarti bahwa sumbernya adalah grup keamanan yang terkait dengan titik akhir. Aturan ini memungkinkan lalu lintas SSH masuk dari titik akhir ke semua instance yang menggunakan grup keamanan ini, baik pelestarian IP klien aktif atau tidak aktif. Jika tidak ada aturan grup keamanan masuk lainnya untuk SSH, maka instance menerima lalu lintas SSH hanya dari titik akhir.

Protokol	Sumber	Rentang port	Komentar
TCP	*ID of endpoint security group*	22	Mengizinkan lalu lintas SSH masuk dari sumber daya yang terkait dengan grup keamanan titik akhir

Contoh aturan masuk: Pelestarian IP klien mati

Contoh berikut memungkinkan lalu lintas SSH masuk dari rentang IPv4 alamat yang ditentukan. Karena pelestarian IP klien tidak aktif, IPv4 alamat sumber adalah alamat antarmuka jaringan

titik akhir. Alamat antarmuka jaringan endpoint ditetapkan dari subnetnya, sehingga Anda dapat menggunakan rentang IPv4 alamat VPC untuk memungkinkan koneksi ke semua instance di VPC.

Protokol	Sumber	Rentang port	Komentar
TCP	*VPC IPv4 CIDR*	22	Memungkinkan lalu lintas SSH masuk dari VPC

Contoh aturan masuk: Pelestarian IP klien aktif

Contoh berikut memungkinkan lalu lintas SSH masuk dari rentang IPv4 alamat yang ditentukan. Karena pelestarian IP klien aktif, IPv4 alamat sumber adalah alamat klien.

Protokol	Sumber	Rentang port	Komentar
TCP	*Public IPv4 address range*	22	Mengizinkan lalu lintas masuk dari rentang IPv4 alamat klien yang ditentukan

Membuat EC2 Instance Connect Endpoint

Anda dapat membuat Instance Connect Endpoint EC2 untuk memungkinkan koneksi aman ke instans Anda.

Pertimbangan-pertimbangan

- Subnet bersama - Anda dapat membuat Titik Akhir Connect Instance EC2 di subnet yang dibagikan dengan Anda. Namun, Anda tidak dapat menggunakan EC2 Instance Connect Endpoint yang dibuat oleh pemilik VPC di subnet yang dibagikan dengan Anda.
- Jenis alamat IP — EC2 Instance Connect Endpoint mendukung jenis alamat berikut, yang harus kompatibel dengan subnet Anda:
  - `ipv4`— Connect hanya ke instans EC2 dengan alamat pribadi IPv4 .
  - `dualstack`— Connect ke instans EC2 dengan IPv4 alamat atau IPv6 alamat pribadi.
  - `ipv6`— Connect hanya ke instans EC2 dengan IPv6 alamat.

Prasyarat

Anda harus memiliki izin IAM yang diperlukan untuk membuat EC2 Instance Connect Endpoint. Untuk informasi selengkapnya, lihat Izin untuk membuat, mendeskripsikan, memodifikasi, dan menghapus EC2 Instance Connect Endpoint.

Console

Untuk membuat EC2 Instance Connect Endpoint

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi kiri, pilih Titik Akhir.
3. Pilih Buat titik akhir, lalu tentukan pengaturan titik akhir sebagai berikut:
   a. (Opsional) Untuk Tanda nama, masukkan nama untuk titik akhir.
   b. Untuk Type, pilih EC2 Instance Connect Endpoint.
   c. Di bawah Pengaturan jaringan, untuk VPC, pilih VPC yang memiliki instance target.
   d. (Opsional) Untuk mempertahankan alamat IP klien, perluas Pengaturan tambahan dan pilih kotak centang Pertahankan IP Klien. Jika tidak, defaultnya adalah menggunakan antarmuka jaringan endpoint sebagai alamat IP klien.

      > **Note**
      >
      > Opsi ini hanya tersedia ketika jenis alamat IP titik akhir dikonfigurasi sebagai IPv4.

   e. (Opsional) Untuk Grup keamanan, pilih grup keamanan untuk dikaitkan dengan titik akhir. Jika tidak, defaultnya adalah menggunakan grup keamanan default untuk VPC. Untuk informasi selengkapnya, lihat Grup keamanan untuk EC2 Instans Connect Endpoint.
   f. Untuk Subnet, pilih subnet untuk membuat titik akhir.
   g. Untuk jenis alamat IP, pilih jenis alamat IP untuk titik akhir. Pilih Dualstack jika Anda perlu mendukung keduanya IPv4 dan IPv6 koneksi ke instans Anda. Pilih IPv4apakah Anda perlu mendukung pelestarian IP klien.
   h. (Opsional) Untuk menambahkan tanda, pilih Tambahkan tanda baru dan masukkan kunci dan nilai tanda.
4. Tinjau pengaturan Anda dan kemudian pilih Buat titik akhir.

Status awal endpoint adalah Pending. Sebelum Anda dapat terhubung ke sebuah instance menggunakan endpoint ini, Anda harus menunggu hingga status endpoint tersedia. Hal ini dapat menghabiskan waktu beberapa menit.

5. Untuk terhubung ke instans menggunakan titik akhir Anda, lihatSambungkan ke instans.

AWS CLI

Untuk membuat EC2 Instance Connect Endpoint

Gunakan perintah create-instance-connect-endpoint.

```
aws ec2 create-instance-connect-endpoint \
    --subnet-id subnet-0123456789example
```

Untuk menentukan jenis lalu lintas yang didukung endpoint, sertakan `--ip-address-type` parameternya. Nilai yang valid adalah `ipv4`, `dualstack`, atau `ipv6`. Subnet harus mendukung jenis alamat IP yang Anda tentukan. Ketika `--ip-address-type` parameter dihilangkan, nilai default ditentukan oleh jenis alamat IP yang didukung oleh subnet.

```
aws ec2 create-instance-connect-endpoint \
    --subnet-id subnet-0123456789example \
    --ip-address-type ipv4
```

Berikut ini adalah output contoh.

```
{
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "NetworkInterfaceIds": [
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
```

```
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az4",
        "CreatedAt": "2023-04-07T15:43:53.000Z",
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
            "sg-0123abcd"
        ],
        "Tags": [],
        "IpAddressType": "ipv4"
}
```

Untuk memantau status pembuatan

Nilai awal untuk bidang `State` adalah `create-in-progress`. Sebelum Anda dapat terhubung ke instans menggunakan titik akhir ini, tunggu sampai statusnya `create-complete`. Gunakan describe-instance-connect-endpointsperintah untuk memantau status EC2 Instance Connect Endpoint. `--query`Parameter menyaring hasil ke `State` lapangan.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

Berikut ini adalah output contoh.

```
create-complete
```

PowerShell

Untuk membuat Instance Connect Endpoint EC2

Gunakan New-EC2InstanceConnectEndpointcmdlet.

```
New-EC2InstanceConnectEndpoint -SubnetId subnet-0123456789example
```

Untuk menentukan jenis lalu lintas yang didukung endpoint, sertakan `-IpAddressType` parameternya. Nilai yang valid adalah `ipv4`, `dualstack`, atau `ipv6`. Subnet harus mendukung jenis alamat IP yang Anda tentukan. Ketika `-IpAddressType` parameter dihilangkan, nilai default ditentukan oleh jenis alamat IP yang didukung oleh subnet.

```
New-EC2InstanceConnectEndpoint -SubnetId subnet-0123456789example -
IpAddressType ipv4
```

Berikut ini adalah output contoh.

```
OwnerId                    : 111111111111
InstanceConnectEndpointId  : eice-0123456789example
InstanceConnectEndpointArn : arn:aws:ec2:us-east-1:111111111111:instance-connect-
endpoint/eice-0123456789example
State                      : create-complete
StateMessage               :
DnsName                    : eice-0123456789example.0123abcd.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com
FipsDnsName                : eice-0123456789example.0123abcd.fips.ec2-instance-
connect-endpoint.us-east-1.amazonaws.com
NetworkInterfaceIds        : {eni-0123abcd}
VpcId                      : vpc-0123abcd
AvailabilityZone           : us-east-1a
AvailabilityZoneId         : use1-az4
CreatedAt                  : 4/7/2023 3:43:53 PM
SubnetId                   : subnet-0123abcd
PreserveClientIp           : False
SecurityGroupIds           : {sg-0123abcd}
Tags                       : {}
IpAddressType              : ipv4
```

Untuk memantau status pembuatan

Nilai awal untuk bidang `State` adalah `create-in-progress`. Sebelum Anda dapat terhubung ke instans menggunakan titik akhir ini, tunggu sampai statusnya `create-complete`. Gunakan Get-EC2InstanceConnectEndpointcmdlet untuk memantau status EC2 Instance Connect Endpoint. `.State.Value`memfilter hasil ke `State` lapangan.

```
(Get-EC2InstanceConnectEndpoint -InstanceConnectEndpointId
 "eice-0123456789example").State.Value
```

Berikut ini adalah output contoh.

```
create-complete
```

Memodifikasi Titik Akhir Connect Instance EC2

Anda dapat memodifikasi Titik Akhir Connect Instance EC2 yang ada menggunakan AWS CLI atau SDK. Konsol Amazon EC2 tidak mendukung modifikasi titik akhir.

Sebelum memulai, Anda harus memiliki izin IAM yang diperlukan. Untuk informasi selengkapnya, lihat Izin untuk membuat, mendeskripsikan, memodifikasi, dan menghapus EC2 Instance Connect Endpoint.

Parameter yang dapat Anda modifikasi

Anda dapat memodifikasi parameter EC2 Instance Connect Endpoint berikut:

Grup keamanan

Anda dapat menentukan grup keamanan baru untuk EC2 Instance Connect Endpoint. Grup keamanan baru menggantikan grup keamanan saat ini.

Saat memodifikasi grup keamanan, Anda harus menentukan:

- Setidaknya satu grup keamanan, bahkan jika itu hanya grup keamanan default di VPC.
- Kelompok keamanan, bukan nama-nama. IDs

Jenis alamat IP

Anda dapat menentukan jenis alamat IP baru untuk EC2 Instance Connect Endpoint.

Nilai yang valid: `ipv4` | `dualstack` | `ipv6`

Pertahankan pengaturan IP klien

Anda dapat menentukan apakah akan mempertahankan alamat IP klien sebagai sumbernya.

> **Note**
>
> Melestarikan IP klien hanya didukung pada IPv4 EC2 Instance Connect Endpoints. Saat mengaktifkan`PreserveClientIp`, jenis alamat IP titik akhir yang ada harus`ipv4`, atau jika memodifikasi jenis alamat IP dalam permintaan yang sama, nilai baru harus. `ipv4`

AWS CLI

Untuk memodifikasi Instance Connect Endpoint EC2

Gunakan modify-instance-connect-endpointperintah dan tentukan EC2 Instance Connect Endpoint dan parameter yang akan dimodifikasi. Contoh berikut memodifikasi semua parameter dalam satu permintaan.

```
aws ec2 modify-instance-connect-endpoint \
```

```
    --instance-connect-endpoint-id eice-0123456789example \
    --security-group-ids sg-0123456789example \
    --ip-address-type dualstack \
    --no-preserve-client-ip
```

Berikut ini adalah output contoh.

```
{
    "Return": true
}
```

Untuk memantau status pembaruan

Selama modifikasi, status Titik Akhir Instance Connect EC2 berubah menjadi. `update-in-progress` Proses pembaruan berjalan secara asinkron dan dilengkapi dengan status atau. `update-complete` `update-failed` Titik akhir menggunakan konfigurasi lamanya hingga status berubah menjadi`update-complete`.

Gunakan describe-instance-connect-endpointsperintah untuk memantau status pembaruan. `--query`Parameter menyaring hasil ke `State` lapangan.

```
aws ec2 describe-instance-connect-endpoints \
    --instance-connect-endpoint-ids eice-0123456789example \
    --query InstanceConnectEndpoints[*].State --output text
```

Berikut ini adalah output contoh.

```
update-complete
```

PowerShell

Untuk memodifikasi Instance Connect Endpoint EC2

Gunakan Edit-EC2InstanceConnectEndpointcmdlet dan tentukan EC2 Instance Connect Endpoint dan parameter yang akan dimodifikasi. Contoh berikut memodifikasi semua parameter dalam satu permintaan.

```
Edit-EC2InstanceConnectEndpoint `
    -InstanceConnectEndpointId eice-0123456789example `
    -SecurityGroupIds sg-0123456789example `
    -IpAddressType dualstack `
```

```
    -PreserveClientIp $false
```

Berikut ini adalah output contoh.

```
True
```

Untuk memantau status pembaruan

Selama modifikasi, status Titik Akhir Instance Connect EC2 berubah menjadi. `update-in-progress` Proses pembaruan berjalan secara asinkron dan dilengkapi dengan status atau. `update-complete` `update-failed` Titik akhir menggunakan konfigurasi lamanya hingga status berubah menjadi`update-complete`.

Gunakan Get-EC2InstanceConnectEndpointperintah untuk memantau status pembaruan. `.State.Value`memfilter hasil ke `State` lapangan.

```
(Get-EC2InstanceConnectEndpoint -InstanceConnectEndpointId
 "eice-0123456789example").State.Value
```

Berikut ini adalah output contoh.

```
update-complete
```

Menghapus Titik Akhir Connect Instance EC2

Setelah selesai menggunakan EC2 Instance Connect Endpoint, Anda dapat menghapusnya.

Anda harus memiliki izin IAM yang diperlukan untuk membuat EC2 Instance Connect Endpoint. Untuk informasi selengkapnya, lihat Izin untuk membuat, mendeskripsikan, memodifikasi, dan menghapus EC2 Instance Connect Endpoint.

Saat Anda menghapus Instance Connect Endpoint EC2 menggunakan konsol, maka akan masuk ke status Menghapus. Jika penghapusan berhasil, titik akhir yang dihapus tidak lagi muncul. Jika penghapusan gagal, status menghapus-gagal dan pesan Status memberikan alasan kegagalan.

Saat Anda menghapus Instance Connect Endpoint EC2 menggunakan AWS CLI, titik tersebut akan memasuki status. `delete-in-progress` Jika penghapusan berhasil, ia memasuki negara bagian. `delete-complete` Jika penghapusan gagal, negara adalah `delete-failed` dan `StateMessage` memberikan alasan kegagalan.

Console

Untuk menghapus EC2 Instance Connect Endpoint

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Pada panel navigasi kiri, pilih Titik Akhir.
3. Pilih titik akhir.
4. Pilih Tindakan, Hapus titik akhir VPC.
5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

AWS CLI

Untuk menghapus EC2 Instance Connect Endpoint

Gunakan delete-instance-connect-endpointperintah dan tentukan ID dari EC2 Instance Connect Endpoint untuk dihapus.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

Berikut ini adalah output contoh.

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "AvailabilityZoneId": "use1-az2",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
    }
}
```

PowerShell

Untuk menghapus EC2 Instance Connect Endpoint

Gunakan Remove-EC2InstanceConnectEndpointcmdlet dan tentukan ID dari EC2 Instance Connect Endpoint untuk dihapus.

```
Remove-EC2InstanceConnectEndpoint -InstanceConnectEndpointId eice-03f5e49b83924bbc7
```

Berikut ini adalah output contoh.

```
@{
    InstanceConnectEndpoint = @{
        OwnerId = "111111111111"
        InstanceConnectEndpointId = "eice-0123456789example"
        InstanceConnectEndpointArn = "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example"
        State = "delete-in-progress"
        StateMessage = ""
        NetworkInterfaceIds = @()
        VpcId = "vpc-0123abcd"
        AvailabilityZone = "us-east-1d"
        AvailabilityZoneId = "use1-az2"
        CreatedAt = "2023-02-07T12:05:37+00:00"
        SubnetId = "subnet-0123abcd"
    }
}
```

Connect ke instans Amazon EC2 menggunakan EC2 Instance Connect Endpoint

Anda dapat menggunakan EC2 Instance Connect Endpoint untuk menyambung ke instans Amazon EC2 yang mendukung SSH atau RDP.

Prasyarat

- Anda harus memiliki izin IAM yang diperlukan untuk terhubung ke EC2 Instance Connect Endpoint. Untuk informasi selengkapnya, lihat Izin untuk menggunakan EC2 Instance Connect Endpoint untuk menyambung ke instans.
- Titik Akhir Instans Connect EC2 harus berada dalam salah satu status berikut:
  - buat-lengkap untuk titik akhir baru

- update-in-progress, update-complete, atau update-failed untuk endpoint yang ada yang sedang dimodifikasi. Saat memodifikasi titik akhir, ia terus menggunakan konfigurasi aslinya hingga status berubah menjadi pembaruan-selesai.

  Jika VPC Anda tidak memiliki EC2 Instance Connect Endpoint, Anda dapat membuatnya. Untuk informasi selengkapnya, lihat Membuat EC2 Instance Connect Endpoint.

- Jenis alamat IP EC2 Instance Connect Endpoint harus kompatibel dengan jenis alamat IP instans. Jika jenis alamat IP endpoint Anda adalah dual-stack, maka itu dapat bekerja untuk keduanya IPv4 dan alamat. IPv6
- (Instans Linux) Untuk menggunakan konsol Amazon EC2 untuk menyambung ke instans Anda, atau menggunakan CLI untuk menghubungkan dan meminta EC2 Instance Connect menangani kunci sementara, instans Anda harus menginstal EC2 Instance Connect. Untuk informasi selengkapnya, lihat Menginstal EC2 Instance Connect.
- Pastikan grup keamanan instans mengizinkan lalu lintas SSH masuk dari Titik Akhir Connect Instance Connect EC2. Untuk informasi selengkapnya, lihat Aturan grup keamanan instans target.

Opsi koneksi

- Hubungkan ke instans Linux Anda menggunakan konsol Amazon EC2
- Hubungkan ke instans Linux Anda, menggunakan SSH.
- Connect ke instans Linux Anda dengan ID instance-nya menggunakan AWS CLI
- Hubungkan ke instans Windows Anda menggunakan RDP
- Pemecahan Masalah

Hubungkan ke instans Linux Anda menggunakan konsol Amazon EC2

Anda dapat terhubung ke instans menggunakan konsol Amazon EC2 (klien berbasis browser) sebagai berikut.

Untuk menyambung ke instans Anda menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance, lalu pilih Connect.
4. Pilih tab EC2 Instance Connect.

5. Untuk jenis Koneksi, pilih Connect menggunakan IP Pribadi.
6. Pilih IPv4 alamat pribadi atau IPv6alamat. Opsi tersedia berdasarkan alamat IP yang ditetapkan untuk instans Anda. Jika opsi berwarna abu-abu, instance Anda tidak memiliki alamat IP dari jenis yang ditetapkan padanya.
7. Untuk EC2 Instance Connect Endpoint, pilih ID dari EC2 Instance Connect Endpoint.

   > **Note**
   >
   > EC2 Instance Connect Endpoint harus kompatibel dengan alamat IP yang Anda pilih pada langkah sebelumnya. Jika jenis alamat IP endpoint Anda adalah dual-stack, maka itu dapat bekerja untuk keduanya IPv4 dan alamat. IPv6 Untuk informasi selengkapnya, lihat Membuat EC2 Instance Connect Endpoint.

8. Untuk Nama Pengguna, jika AMI yang Anda gunakan untuk meluncurkan instance menggunakan nama pengguna selain`ec2-user`, masukkan nama pengguna yang benar.
9. Untuk durasi terowongan Max (detik), masukkan durasi maksimum yang diizinkan untuk koneksi SSH.

   Durasi harus sesuai dengan `maxTunnelDuration` kondisi apa pun yang ditentukan dalam kebijakan IAM. Jika Anda tidak memiliki akses ke kebijakan IAM, hubungi administrator Anda.
10. Pilih Hubungkan. Ini membuka jendela terminal untuk instance Anda.

Hubungkan ke instans Linux Anda, menggunakan SSH.

Anda dapat menggunakan SSH untuk terhubung ke instans Linux Anda, dan menggunakan perintah `open-tunnel` untuk membuat terowongan privat. Anda dapat menggunakan `open-tunnel` dalam mode koneksi tunggal atau multikoneksi. Anda dapat menentukan ID instans Anda, IPv4 alamat pribadi, atau IPv6 alamat.

Untuk informasi tentang menggunakan AWS CLI to connect ke instans Anda menggunakan SSH, lihatConnect menggunakan AWS CLI.

Contoh berikut menggunakan OpenSSH. Anda dapat menggunakan klien SSH lain yang mendukung mode proxy.

Koneksi tunggal

Untuk mengizinkan hanya satu koneksi ke instans menggunakan SSH dan perintah **`open-tunnel`**

Gunakan `ssh` dan open-tunnel AWS CLI perintah sebagai berikut. Perintah `-o` proxy menyertakan `open-tunnel` perintah yang membuat terowongan pribadi ke instans.

```
ssh -i my-key-pair.pem ec2-user@i-1234567890abcdef0 \
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-1234567890abcdef0'
```

Untuk:

- `-i` – Menentukan pasangan kunci yang digunakan untuk meluncurkan instans.
- *ec2-user*`@`*i-1234567890abcdef0* – Menentukan nama pengguna AMI yang digunakan untuk meluncurkan instans dan ID instans. Untuk contoh dengan IPv6 alamat, Anda harus menentukan IPv6 alamat alih-alih ID instance.
- `--instance-id` – Menentukan ID instans yang akan dihubungkan. Atau, tentukan `%h`, yang mengekstrak ID instans dari pengguna. Untuk contoh dengan IPv6 alamat, ganti `--instance-id` *i-1234567890abcdef0* dengan`--private-ip-address` *2001:db8::1234:5678:1.2.3.4*.

Multi-koneksi

Untuk mengizinkan beberapa koneksi ke sebuah instance, pertama-tama jalankan open-tunnel AWS CLI perintah untuk mulai mendengarkan koneksi TCP baru, dan kemudian gunakan `ssh` untuk membuat koneksi TCP baru dan terowongan pribadi ke instans Anda.

Untuk memungkinkan beberapa koneksi ke instans Anda menggunakan SSH dan perintah **`open-tunnel`**

1. Jalankan perintah berikut untuk mulai mendengarkan koneksi TCP baru pada port yang ditentukan pada komputer lokal Anda.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-1234567890abcdef0 \
       --local-port 8888
   ```

   Keluaran yang diharapkan

   ```
   Listening for connections on port 8888.
   ```

2. Di jendela terminal baru, jalankan perintah `ssh` berikut untuk membuat koneksi TCP baru dan terowongan pribadi ke instans Anda.

```
ssh -i my-key-pair.pem ec2-user@localhost -p 8888
```

Output yang diharapkan — Di jendela terminal pertama, Anda akan melihat hal-hal berikut:

```
[1] Accepted new tcp connection, opening websocket tunnel.
```

Anda mungkin juga melihat yang berikut ini:

```
[1] Closing tcp connection.
```

Connect ke instans Linux Anda dengan ID instance-nya menggunakan AWS CLI

Jika Anda hanya mengetahui ID instans Anda, Anda dapat menggunakan AWS CLI perintah ec2-instance-connect ssh untuk terhubung ke instance Anda menggunakan klien SSH. Untuk informasi selengkapnya, lihat Connect menggunakan AWS CLI.

Prasyarat

- Instal AWS CLI versi 2 dan konfigurasikan menggunakan kredensional Anda. Untuk informasi selengkapnya, lihat Menginstal atau memperbarui ke versi terbaru AWS CLI dan Mengkonfigurasi AWS CLI dalam Panduan AWS Command Line Interface Pengguna.
- Atau, buka AWS CloudShell dan jalankan AWS CLI perintah di shell yang telah diautentikasi sebelumnya.

Untuk menghubungkan ke instans menggunakan ID instans dan EC2 Instance Connect Endpoint

Jika Anda hanya mengetahui ID instance, gunakan perintah ec2-instance-connect ssh CLI, dan tentukan `ssh` perintah, ID instance, dan parameter dengan `eice` nilai untuk menggunakan EC2 Instance Connect Endpoint. `--connection-type` Jika instance hanya memiliki IPv6 alamat, Anda juga harus menyertakan `--instance-ip` parameter dengan IPv6 alamat.

- Jika instance memiliki IPv4 alamat pribadi (juga dapat memiliki IPv6 alamat) gunakan perintah dan parameter berikut:

```
aws ec2-instance-connect ssh \
```

```
    --instance-id i-1234567890example \
    --os-user ec2-user \
    --connection-type eice
```

- Jika instance hanya memiliki IPv6 alamat, sertakan `--instance-ip` parameter dengan IPv6 alamat:

```
aws ec2-instance-connect ssh \
    --instance-id i-1234567890example \
    --instance-ip 2001:db8::1234:5678:1.2.3.4 \
    --os-user ec2-user \
    --connection-type eice
```

> **Tip**
>
> Jika Anda mendapatkan kesalahan, pastikan Anda menggunakan AWS CLI versi 2. `ssh`Parameter ini hanya tersedia di AWS CLI versi 2. Untuk informasi selengkapnya, lihat Tentang AWS CLI versi 2 di Panduan AWS Command Line Interface Pengguna.

Hubungkan ke instans Windows Anda menggunakan RDP

Anda dapat menggunakan Remote Desktop Protocol (RDP) melalui EC2 Instance Connect Endpoint untuk terhubung ke instance Windows tanpa IPv4 alamat publik atau nama DNS publik.

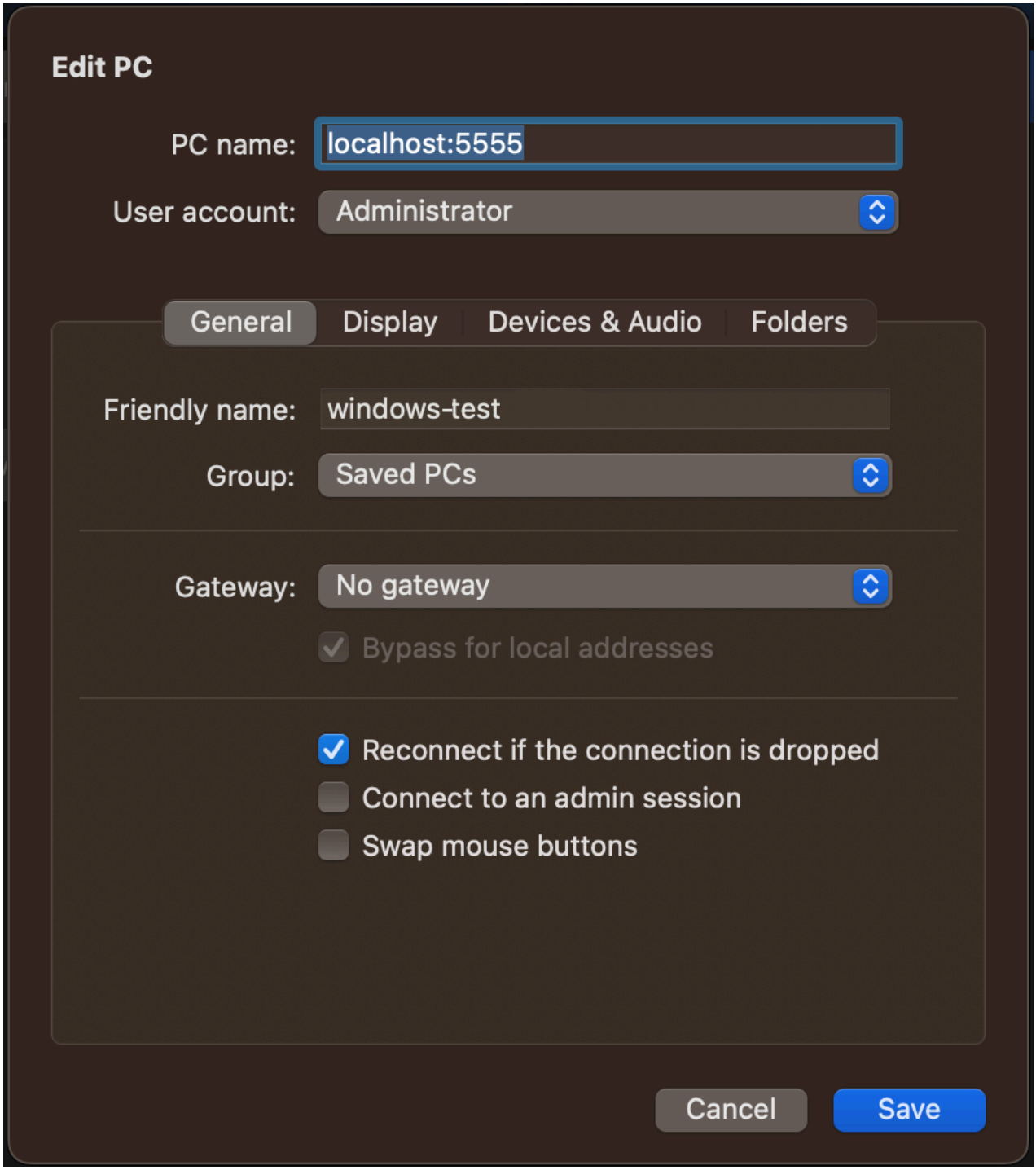
Untuk terhubung ke instans Windows menggunakan klien RDP

1. Selesaikan Langkah 1 - 8 di Connect to instance Windows Anda menggunakan RDP. Setelah mengunduh file desktop RDP pada Langkah 8, Anda akan mendapatkan pesan Unable to connect, yang diharapkan karena instans Anda tidak memiliki alamat IP publik.
2. Jalankan perintah berikut untuk membuat terowongan privat ke VPC di mana instans berada. `--remote-port` harus `3389` karena RDP menggunakan port 3389 secara default.

```
aws ec2-instance-connect open-tunnel \
    --instance-id i-1234567890abcdef0 \
    --remote-port 3389 \
    --local-port any-port
```

3. Di folder Unduhan Anda, temukan file desktop RDP yang Anda unduh, dan seret ke jendela klien RDP.
4. Klik kanan file desktop RDP dan pilih Edit.
5. Di jendela Edit PC, untuk nama PC (instance untuk terhubung), masukkan`localhost:`*`local-port`*, di mana *`local-port`* menggunakan nilai yang sama seperti yang Anda tentukan di Langkah 2, lalu pilih Simpan.

   Perhatikan bahwa tangkapan layar berikut dari jendela Edit PC berasal dari Microsoft Remote Desktop di Mac. Jika Anda menggunakan klien Windows, jendelanya mungkin berbeda.



6. Di klien RDP, klik kanan PC (yang baru saja Anda konfigurasikan) dan pilih Connect untuk terhubung ke instans Anda.
7. Pada saat diminta, masukkan kata sandi terdekripsi untuk akun administrator.

Pemecahan Masalah

Gunakan informasi berikut untuk membantu mendiagnosis dan memperbaiki masalah yang mungkin Anda temukan saat menggunakan EC2 instans Connect Endpoint untuk menghubungkan sebuah instans.

Tidak dapat terhubung ke instans Anda

Berikut ini adalah alasan umum mengapa Anda mungkin tidak dapat terhubung ke instans Anda.

- Grup keamanan — Periksa grup keamanan yang ditetapkan ke EC2 Instance Connect Endpoint dan instans Anda. Untuk informasi selengkapnya tentang aturan grup keamanan yang diperlukan, lihat Grup keamanan untuk EC2 Instans Connect Endpoint.
- Status instans - Verifikasi apakah instans Anda ada dalam `running` status.
- Pasangan kunci - Jika perintah yang Anda gunakan untuk menghubungkan memerlukan kunci pribadi, verifikasi bahwa instans Anda memiliki kunci publik dan Anda memiliki kunci pribadi yang sesuai.
- Izin IAM - Verifikasi apakah Anda memiliki izin IAM yang diperlukan. Untuk informasi selengkapnya, lihat Berikan izin untuk menggunakan EC2 Instance Connect Endpoint.

Untuk tips pemecahan masalah lainnya untuk instance Linux, lihat. Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda Untuk tips pemecahan masalah untuk instance Windows, lihat. the section called “Masalah RDP contoh Windows”

ErrorCode: AccessDeniedException

Jika Anda menerima `AccessDeniedException` kesalahan, dan `maxTunnelDuration` kondisinya ditentukan dalam kebijakan IAM, pastikan untuk menentukan `--max-tunnel-duration` parameter saat menghubungkan ke sebuah instans. Untuk informasi selengkapnya tentang parameter ini, lihat open-tunnel di Referensi Perintah AWS CLI .

Koneksi log dibuat melalui EC2 Instance Connect Endpoint

Anda dapat mencatat operasi sumber daya dan mengaudit koneksi yang dibuat melalui Titik Akhir Connect Instans EC2 dengan AWS CloudTrail log.

Untuk informasi selengkapnya tentang penggunaan AWS CloudTrail dengan Amazon EC2, lihat. Log panggilan EC2 API Amazon menggunakan AWS CloudTrail

Log panggilan EC2 Instance Connect Endpoint API dengan AWS CloudTrail

Operasi sumber daya Endpoint Instance Connect EC2 dicatat CloudTrail sebagai peristiwa manajemen. Saat panggilan API berikut dibuat, aktivitas dicatat sebagai CloudTrail peristiwa dalam riwayat Acara:

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat CloudTrail peristiwa dengan riwayat peristiwa di Panduan AWS CloudTrail Pengguna.

Gunakan AWS CloudTrail untuk mengaudit pengguna yang terhubung ke instans menggunakan EC2 Instance Connect Endpoint

Upaya koneksi ke instans melalui EC2 Instance Connect Endpoint dicatat CloudTrail dalam riwayat peristiwa. Ketika koneksi ke instans dimulai melalui Titik Akhir Connect Instance EC2, koneksi dicatat sebagai peristiwa CloudTrail manajemen dengan dari. `eventName` `OpenTunnel`

Anda dapat membuat EventBridge aturan Amazon yang merutekan CloudTrail acara ke target. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Berikut ini adalah contoh peristiwa `OpenTunnel` manajemen yang masuk CloudTrail.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name"
    },
    "eventTime": "2023-04-11T23:50:40Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "OpenTunnel",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
        "maxTunnelDuration": "3600",
        "remotePort": "22",
        "privateIpAddress": "10.0.1.1"
    },
    "responseElements": null,
    "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
    "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::EC2::InstanceConnectEndpoint",
        "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Peran tertaut layanan untuk EC2 Instance Connect Endpoint

Amazon EC2 menggunakan peran terkait layanan AWS Identity and Access Management (IAM). Peran tertaut layanan adalah tipe peran IAM unik yang tertaut langsung ke Amazon EC2. Peran terkait layanan telah ditentukan sebelumnya oleh Amazon EC2 dan menyertakan semua izin yang diperlukan Amazon EC2 untuk memanggil orang lain atas nama Anda. Layanan AWS Untuk informasi selengkapnya, lihat Peran terkait layanan di Panduan Pengguna IAM.

Izin peran terkait layanan untuk EC2 Instance Connect Endpoint

Amazon EC2 digunakan AWSServiceRoleForEC2InstanceConnectuntuk membuat dan mengelola antarmuka jaringan di akun Anda yang diperlukan oleh EC2 Instance Connect Endpoint.

Peran terkait layanan AWSServiceRoleForEC2InstanceConnect memercayai layanan berikut untuk mengambil peran tersebut:

- `ec2-instance-connect.amazonaws.com`

AWSServiceRoleForEC2InstanceConnectPeran terkait layanan menggunakan kebijakan terkelola berikut:

- EC2 InstanceConnectEndpoint

Untuk melihat izin untuk kebijakan terkelola, lihat Ec2 InstanceConnectEndpoint di Referensi Kebijakan AWS Terkelola.

Membuat peran terkait layanan untuk EC2 Instance Connect Endpoint

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda membuat Titik Akhir Connect Instance EC2, Amazon EC2 akan membuat peran terkait layanan untuk Anda.

Mengedit peran terkait layanan untuk EC2 Instance Connect Endpoint

Titik Akhir Instance Connect EC2 tidak memungkinkan Anda mengedit peran terkait AWSServiceRoleForEC2InstanceConnectlayanan.

Menghapus peran terkait layanan untuk EC2 Instance Connect Endpoint

Jika Anda tidak perlu lagi menggunakan EC2 Instance Connect Endpoint, sebaiknya hapus peran yang ditautkan AWSServiceRoleForEC2InstanceConnectlayanan.

Anda harus menghapus semua sumber daya Titik Akhir Instance Connect EC2 sebelum dapat menghapus peran terkait layanan.

Untuk menghapus peran terkait layanan, lihat Menghapus peran terkait layanan di Panduan Pengguna IAM.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan dalam Panduan Pengguna IAM.

Kuota untuk EC2 Instance Connect Endpoint

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah.

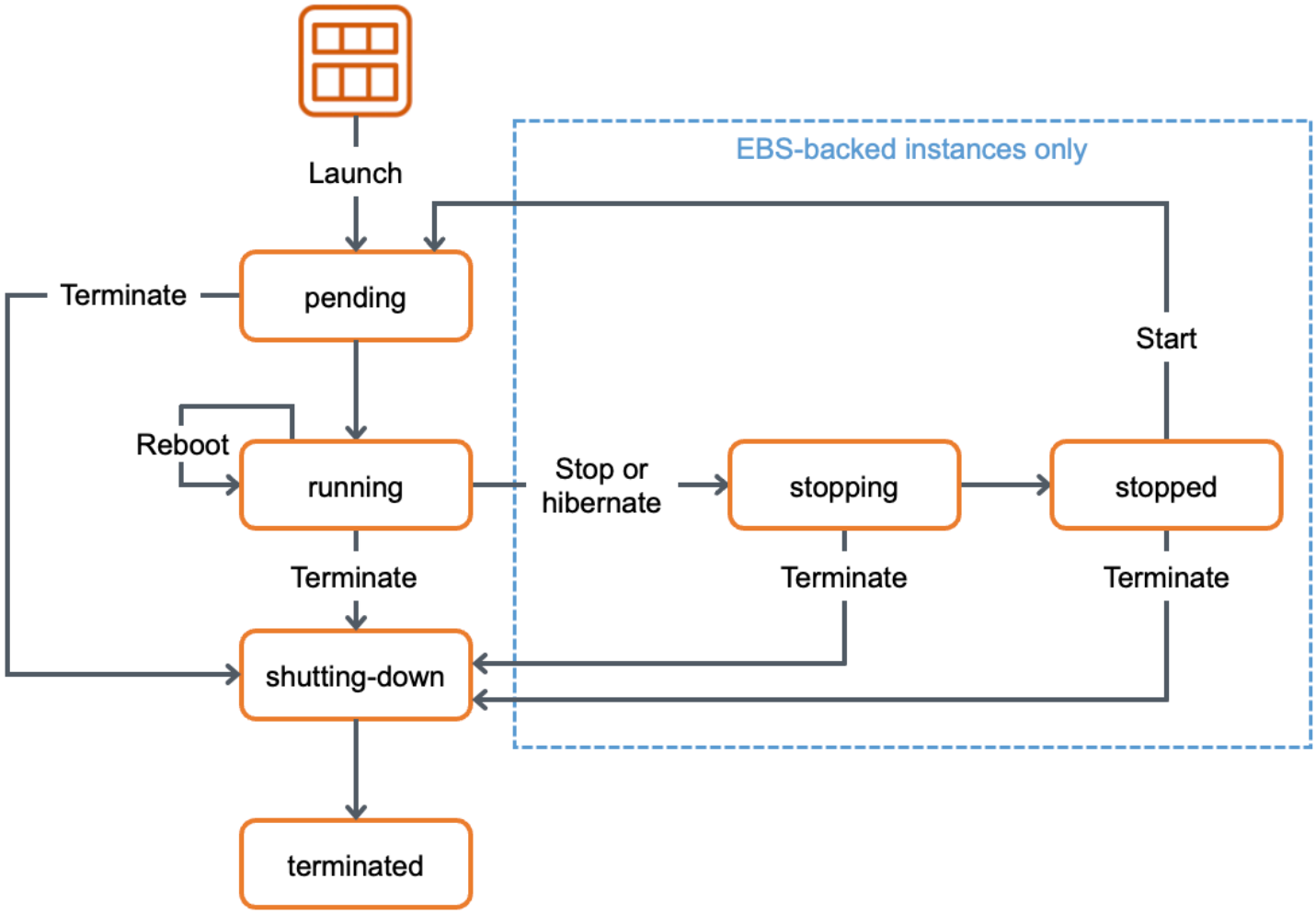
Anda Akun AWS memiliki kuota berikut yang terkait dengan EC2 Instance Connect Endpoint.

Nama	Default	Dapat disesuaikan
Jumlah maksimum EC2 Instance Connect Endpoint per per Akun AWS AWS Region	5	Tidak
Jumlah Maksimum EC2 instans Connect per VPC	1	Tidak
Jumlah maksimum EC2 instans Connect Endpoint per subnet	1	Tidak
Jumlah maksimum koneksi bersamaan per EC2 Instance Connect Endpoint	20	Tidak

Perubahan status EC2 instans Amazon

EC2 Instans Amazon bertransisi melalui status yang berbeda dari saat Anda meluncurkannya hingga penghentiannya.

Ilustrasi berikut menunjukkan transisi di antara status instans.



Anda dapat menerima notifikasi saat instans Anda mengubah status. Untuk informasi selengkapnya, lihat the section called “Peristiwa perubahan status”.

Penagihan berdasarkan status instans

Tabel berikut memberikan deskripsi singkat dari setiap status instance dan menunjukkan apakah penggunaan instance ditagih. Beberapa AWS sumber daya, seperti volume Amazon EBS dan alamat IP Elastis, dikenakan biaya terlepas dari status instans. Untuk informasi selengkapnya, lihat Menghindari Biaya Tidak Terduga dalam AWS Billing Panduan Pengguna .

Status instans	Deskripsi	Penagihan penggunaan instans
`pendinc`	Instans sedang bersiap untuk memasuki status	Tidak ditagih

Status instans	Deskripsi	Penagihan penggunaan instans
	`running`. Sebuah instans memasuki status `pending` saat diluncurkan atau ketika dimulai setelah berada dalam status `stopped`.	
`running`	Instans ini sedang berjalan dan siap digunakan.	Dikenakan biaya
`stopping`	Instans sedang bersiap untuk dihentikan.	Tidak ditagih **Note** Jika Anda hibernasi instance, Anda ditagih saat instance berada dalam status. `stopping`
`stopped`	Instans ini dimatikan dan tidak dapat digunakan. Instans ini dapat dimulai kapan saja.	Tidak ditagih
`shutting-down`	Instans sedang bersiap untuk diakhiri.	Tidak ditagih
`terminated`	Instans ini telah dihapus secara permanen dan tidak dapat dimulai.	Tidak ditagih **Note** Instans Terpesan yang diterapkan ke instans yang diakhiri akan ditagih hingga akhir jangka waktunya sesuai dengan opsi pembayaran mereka. Untuk informasi selengkapnya, lihat Instans Cadangan untuk ikhtisar Amazon EC2

Contoh yang tertunda

Saat Anda meluncurkan sebuah instans, instans akan memasuki ststua `pending`. Tipe instans yang Anda tentukan saat peluncuran menentukan perangkat keras komputer host untuk instans Anda. Kami menggunakan Amazon Machine Image (AMI) yang Anda tentukan saat peluncuran untuk booting instans. Setelah instans siap untuk Anda, instans memasuki status `running`. Anda dapat terhubung ke instans yang sedang berjalan dan menggunakannya seperti Anda menggunakan komputer yang ada di depan Anda.

Segera setelah instans Anda bertransisi ke status `running`, Anda akan dikenai biaya untuk setiap detik Anda menjalankan instans, dengan minimum satu menit, meskipun instans tetap idle dan Anda tidak terhubung dengannya.

Contoh yang dihentikan

Jika instans Anda gagal dalam pemeriksaan status atau tidak menjalankan aplikasi Anda seperti yang diharapkan, dan jika volume root instans Anda adalah volume Amazon EBS, Anda dapat menghentikan dan memulai instans Anda untuk mencoba memperbaiki masalah.

Saat Anda menghentikan sebuah instans, instans tersebut akan memasuki status `stopping`, lalu status `stopped`. Anda tidak dikenakan biaya untuk penggunaan atau biaya transfer data untuk instans Anda yang sedang `stopped`. Biaya dikenakan untuk penyimpanan volume Amazon EBS apa pun. Saat instans Anda ada dalam status `stopped`, Anda dapat memodifikasi atribut tertentu dari instans, termasuk tipe instans.

Saat Anda memulai instans Anda, instans memasuki status `pending`, dan instans akan dipindahkan ke komputer host baru (meskipun dalam beberapa kasus, instant tetap di host saat ini). Saat Anda menghentikan dan memulai instans, Anda kehilangan data apa pun di volume penyimpanan instans yang dilampirkan ke komputer host sebelumnya.

Instans Anda mempertahankan IPv4 alamat pribadinya, yang berarti bahwa alamat IP Elastis yang terkait dengan IPv4 alamat pribadi atau antarmuka jaringan tetap terkait dengan instans Anda. Jika instans Anda memiliki IPv6 alamat, itu mempertahankan IPv6 alamatnya.

Setiap kali Anda melakukan transisi atas sebuah instans dari `stopped` ke `running`, Anda akan dikenai biaya per detik ketika instans sedang berjalan, dengan minimal satu menit setiap kali instans dimulai.

Untuk detail selengkapnya tentang penghentian dan pemulaian sebuah instans, lihat Hentikan dan mulai instans Amazon EC2.

Contoh hibernasi

Saat Anda melakukan hibernasi instance, kami memberi sinyal pada sistem operasi untuk melakukan hibernasi (suspend-to-disk), yang menyimpan konten dari memori instans (RAM) ke volume root Amazon EBS Anda. Kami mempertahankan volume root Amazon EBS instans dan semua volume data Amazon EBS yang terlampir. Saat Anda memulai instans, volume root Amazon EBS dipulihkan ke keadaan sebelumnya dan konten RAM dimuat ulang. Volume data terlampir sebelumnya akan dilampirkan kembali dan instans akan mempertahankan ID instansnya.

Saat Anda menghentikan sebuah instans, instans tersebut akan memasuki status `stopping`, lalu status `stopped`. Kami tidak mengenakan biaya penggunaan untuk instans yang dihibernasi saat berada dalam status `stopped`, tetapi kami mengenakan biaya saat berada dalam status `stopping`, tidak seperti saat Anda menghentikan instans tanpa menghibernasinya. Kami tidak mengenakan biaya penggunaan untuk biaya transfer data, tetapi kami mengenakan biaya volume Amazon EBS, termasuk penyimpanan untuk data RAM.

Saat Anda memulai instans hibernasi, instans memasuki status `pending`, dan kami memindahkan instans ke komputer host baru (meskipun dalam beberapa kasus, instans tetap di host saat ini).

Instans Anda mempertahankan IPv4 alamat pribadinya, yang berarti bahwa alamat IP Elastis yang terkait dengan IPv4 alamat pribadi atau antarmuka jaringan masih terkait dengan instans Anda. Jika instans Anda memiliki IPv6 alamat, itu mempertahankan IPv6 alamatnya.

Untuk informasi selengkapnya, lihat Hibernasi instans Amazon EC2 Anda.

Mem-boot ulang instance

Anda dapat me-reboot instance Anda menggunakan EC2 konsol Amazon, alat baris perintah, dan Amazon EC2 API. Kami menyarankan Anda menggunakan Amazon EC2 untuk me-reboot instance Anda alih-alih menjalankan perintah reboot sistem operasi dari instans Anda.

Mem-boot ulang sebuah instans sama dengan mem-boot ulang sistem operasi. Instans tetap berada di komputer host yang sama dan mempertahankan nama DNS publiknya, alamat IP privat, dan data apa pun pada volume penyimpanan instansnya. Biasanya diperlukan waktu beberapa menit untuk menyelesaikan booting ulang, tetapi waktu yang diperlukan untuk memulai ulang bergantung pada konfigurasi instans.

Mem-boot ulang sebuah instans tidak memulai periode penagihan instans baru; penagihan per detik berlanjut tanpa biaya minimum satu menit lebih lanjut.

Untuk informasi selengkapnya, lihat Nyalakan ulang EC2 instans Amazon Anda.

Instance yang dihentikan

Jika Anda telah memutuskan bahwa Anda tidak lagi membutuhkan sebuah instans, Anda dapat mengakhirinya. Segera setelah status instans berubah menjadi `shutting-down` atau `terminated`, Anda akan berhenti dikenai biaya untuk instans tersebut.

Jika Anda mengaktifkan perlindungan pengakhiran, Anda tidak dapat mengakhiri instans menggunakan konsol, CLI, atau API.

Setelah Anda mengakhiri sebuah instans, instans akan tetap terlihat di konsol untuk beberapa saat, kemudian entri tersebut akan dihapus secara otomatis. Anda juga dapat mendeskripsikan instans yang diakhiri menggunakan CLI dan API. Sumber daya (seperti tanda) secara bertahap dipisahkan dari instans yang diakhiri, oleh karena itu mungkin tidak lagi terlihat pada instans yang diakhiri setelah beberapa saat. Anda tidak dapat terhubung ke atau memulihkan instans yang diakhiri.

Setiap instans yang didukung Amazon EBS mendukung `InstanceInitiatedShutdownBehavior` atribut, yang mengontrol apakah instance berhenti atau berakhir saat Anda memulai shutdown dari dalam instance itu sendiri (misalnya, dengan menggunakan perintah di shutdown Linux). Perilaku defaultnya adalah menghentikan instans. Anda dapat memodifikasi pengaturan atribut ini saat instans sedang berjalan atau berhenti.

Setiap volume Amazon EBS mendukung atribut `DeleteOnTermination`, yang mengontrol apakah volume dihapus atau dipertahankan saat Anda menghentikan instans tempatnya dilampirkan. Defaultnya adalah menghapus volume root dan mempertahankan volume EBS lainnya.

Untuk informasi selengkapnya, lihat Mengakhiri instans Amazon EC2.

Perbedaan antara status instance

Tabel berikut merangkum perbedaan utama antara me-reboot, menghentikan, hibernasi, dan menghentikan instans Anda.

Karakteristik	Mulai ulang	Hentikan/mulai (hanya instans yang didukung Amazon EBS)	Hibernasi (hanya instans yang didukung dengan Amazon EBS)	Mengakhiri
Komputer host	Instance tetap berada di komputer host yang sama.	Kami memindahkan instans ke komputer host baru (meskipun dalam beberapa kasus, instans tetap di host saat ini).	Kami memindahkan instans ke komputer host baru (meskipun dalam beberapa kasus, instans tetap di host saat ini).	Tidak ada
IPv4 Alamat pribadi	Instance menyimpan IPv4 alamat pribadinya.	Instance menyimpan IPv4 alamat pribadinya.	Instance menyimpan IPv4 alamat pribadinya.	Tidak ada
IPv4 Alamat publik	Instance menyimpan IPv4 alamat publiknya.	Instance mendapatkan IPv4 alamat publik baru, kecuali jika memiliki antarmuka jaringan sekunder atau IPv4 alamat pribadi sekunder yang dikaitkan dengan alamat IP Elastis.	Instance mendapatkan IPv4 alamat publik baru, kecuali jika memiliki antarmuka jaringan sekunder atau IPv4 alamat pribadi sekunder yang dikaitkan dengan alamat IP Elastis.	Tidak ada
Alamat IP elastis (IPv4)	Alamat IP Elastis tetap terkait dengan instans	Alamat IP Elastis tetap terkait dengan instans	Alamat IP Elastis tetap terkait dengan instans	Alamat IP Elastis dipisahkan dari instans
IPv6 alamat	Instance menyimpan IPv6 alamatnya	Instance menyimpan IPv6 alamatnya	Instance menyimpan IPv6 alamatnya	Tidak ada

Karakteristik	Mulai ulang	Hentikan/mulai (hanya instans yang didukung Amazon EBS)	Hibernasi (hanya instans yang didukung dengan Amazon EBS)	Mengakhiri
Volume toko instan	Data disimpan	Datanya dihapus	Datanya dihapus	Datanya dihapus
Volume root	Volume dipertahankan	Volume dipertahankan	Volume dipertahankan	Volume dihapus secara default
RAM (isi memori)	RAM dihapus	RAM dihapus	RAM disimpan ke file di volume root	RAM dihapus
Penagihan	Jam penagihan instans tidak berubah	Anda tidak lagi dikenai biaya instans segera setelah statusnya berubah menjadi `stopping`. Setiap kali sebuah instans bertransisi dari `stopped` ke `running`, kami memulai periode tagihan instans baru, yang menagih minimum satu menit setiap kali Anda memulai instans Anda.	Anda dikenai biaya saat instans berada dalam status `stopping`, tetapi tidak lagi dikenai biaya saat instans ada dalam status `stopped`. Setiap kali sebuah instans bertransisi dari `stopped` ke `running`, kami memulai periode tagihan instans baru, yang menagih minimum satu menit setiap kali Anda memulai instans Anda.	Anda berhenti menimbulkan biaya untuk suatu instans segera setelah statusnya berubah menjadi `shutting-down`

Perintah shutdown sistem operasi selalu mengakhiri instance dengan volume root penyimpanan instance. Anda dapat mengontrol apakah perintah shutdown sistem operasi menghentikan atau

menghentikan instance dengan volume root EBS. Lihat informasi yang lebih lengkap di Ubah perilaku shutdown yang dimulai instance.

Hentikan dan mulai instans Amazon EC2

Anda dapat menghentikan dan memulai instans Anda jika memiliki volume Amazon EBS sebagai volume akarnya. Ketika Anda menghentikan sebuah instance, itu mati. Ketika Anda memulai sebuah instance, biasanya dimigrasikan ke komputer host baru yang mendasarinya dan diberi IPv4 alamat publik baru.

Penghentian instans dapat dimulai oleh pengguna (di mana Anda menghentikan instance secara manual) atau dimulai oleh AWS (sebagai respons terhadap peristiwa penghentian terjadwal saat AWS mendeteksi kegagalan host yang mendasari yang tidak dapat diperbaiki untuk instance Anda).

Untuk penghentian yang dimulai pengguna, sebaiknya gunakan konsol Amazon EC2, CLI, atau API alih-alih menjalankan perintah berhenti sistem operasi dari instans Anda. Saat menggunakan Amazon EC2, jika instans tidak dimatikan dengan bersih dalam beberapa menit, Amazon EC2 melakukan hard shutdown. Selanjutnya, AWS CloudTrail buat catatan API kapan instance Anda dihentikan.

Topik ini menjelaskan cara melakukan penghentian yang diprakarsai pengguna. Untuk informasi tentang pemberhentian yang dilakukan oleh AWS, lihatMengelola instans Amazon EC2 yang dijadwalkan untuk berhenti atau pensiun.

Saat Anda menghentikan sebuah instans, instans tersebut tidak dihapus. Jika Anda memutuskan bahwa Anda tidak lagi membutuhkan sebuah instans, Anda dapat mengakhirinya. Untuk informasi selengkapnya, lihat Mengakhiri instans Amazon EC2. Jika Anda ingin menghibernasi instans untuk menyimpan konten dari memori instans (RAM), lihat Hibernasi instans Amazon EC2 Anda. Untuk perbedaan antara tindakan siklus hidup instans, lihat Perbedaan antara status instance.

Daftar Isi

- Bagaimana instans EC2 berhenti dan mulai bekerja
- Metode untuk menghentikan sebuah instance
- Hentikan dan mulai instans Anda secara manual
- Menghentikan dan memulai instans Anda secara otomatis
- Temukan semua instans yang berjalan dan berhenti
- Temukan waktu peluncuran awal dan terbaru

- Aktifkan perlindungan berhenti untuk instans EC2 Anda

Bagaimana instans EC2 berhenti dan mulai bekerja

Saat Anda menghentikan instans Amazon EC2, perubahan akan didaftarkan pada tingkat sistem operasi (OS) instans, beberapa sumber daya hilang, dan beberapa sumber daya tetap ada. Saat Anda memulai sebuah instans, perubahan terdaftar di tingkat instans.

Topik

- Apa yang terjadi jika Anda menghentikan sebuah instans
- Apa yang terjadi jika Anda memulai sebuah instans
- Uji respons aplikasi untuk berhenti dan mulai
- Biaya yang terkait dengan instans stop and start

Apa yang terjadi jika Anda menghentikan sebuah instans

Berikut ini menjelaskan apa yang biasanya terjadi ketika Anda menghentikan sebuah instance menggunakan metode stop default. Perhatikan bahwa beberapa aspek mungkin bervariasi tergantung pada metode stop yang Anda gunakan.

Perubahan terdaftar di tingkat OS

- Permintaan API akan mengirimkan peristiwa penekanan tombol kepada tamu.
- Berbagai layanan sistem dihentikan sebagai akibat dari peristiwa penekanan tombol. Shutdown OS yang anggun dipicu oleh acara tekan tombol shutdown ACPI dari hypervisor.
- Pematian ACPI dimulai.
- Instance dimatikan saat proses shutdown OS yang anggun keluar. Tidak ada waktu pematian OS yang dapat dikonfigurasi.
- Jika OS instans tidak dimatikan dengan bersih dalam beberapa menit, pematian keras dilakukan.
- Instans tersebut berhenti berjalan.
- Status instance berubah menjadi `stopping` dan kemudian`stopped`.
- [Auto Scaling] Jika instans Anda berada dalam grup Auto Scaling, saat instans berada dalam status Amazon EC2 `running` selain, atau jika statusnya untuk pemeriksaan status menjadi, Amazon `impaired` EC2 Auto Scaling menganggap instans tersebut tidak sehat dan

menggantikannya. Untuk informasi selengkapnya, lihat Health memeriksa instans di grup Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling.

- [Instans Windows] Saat Anda menghentikan dan memulai instance Windows, agen peluncuran melakukan tugas pada instance, seperti mengubah huruf drive untuk volume Amazon EBS yang terlampir. Untuk informasi lebih lanjut tentang default ini dan bagaimana Anda dapat mengubahnya, lihat. the section called “EC2Luncurkan v2”

Sumber daya hilang

- Data disimpan pada RAM.
- Data disimpan di volume penyimpanan instans.
- Alamat IPv4 publik yang secara otomatis ditetapkan Amazon EC2 ke instans saat diluncurkan atau dimulai. Untuk mempertahankan IPv4 alamat publik yang tidak pernah berubah, Anda dapat mengaitkan alamat IP Elastis dengan instans Anda.

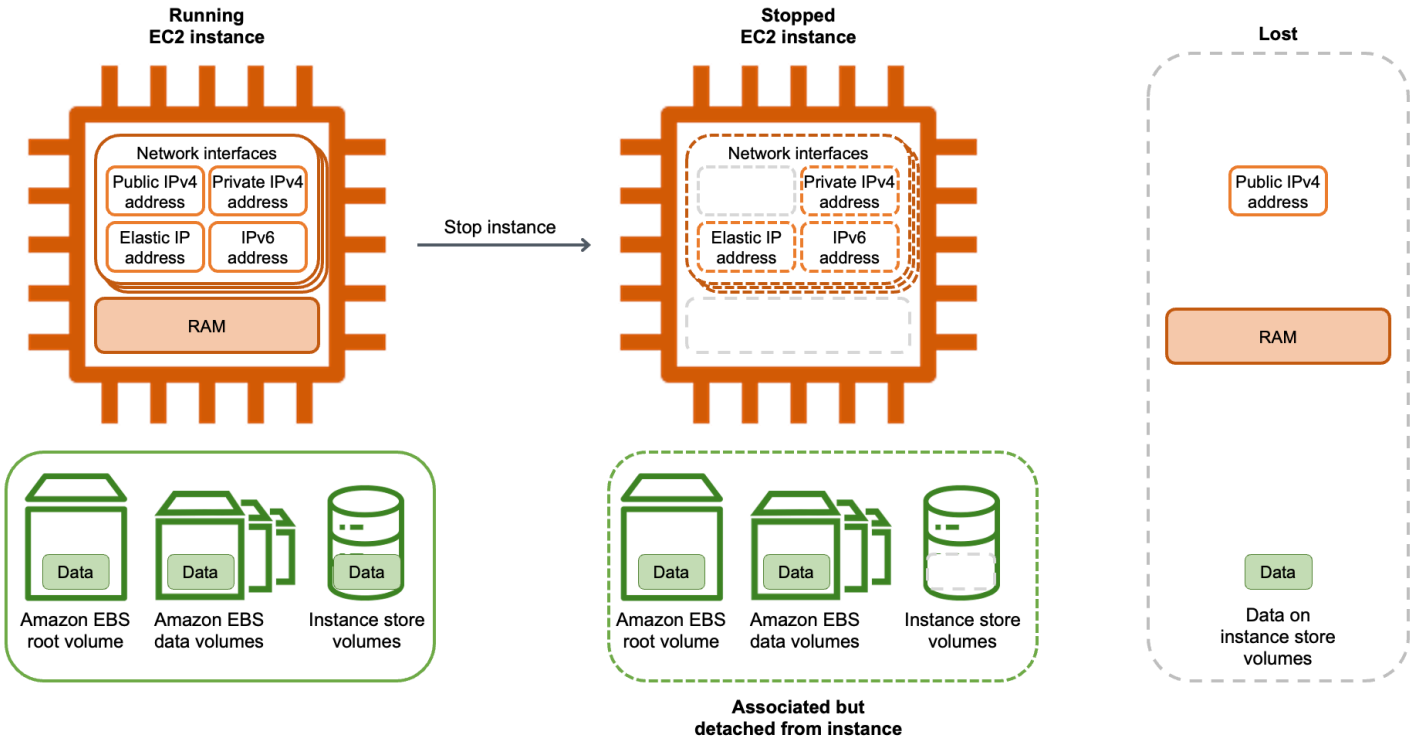
Sumber daya yang bertahan

- Setiap volume root dan data Amazon EBS terlampir.
- Data disimpan di volume Amazon EBS.
- Setiap antarmuka jaringan yang terpasang.

  Antarmuka jaringan mencakup sumber daya berikut, yang juga bertahan:

  - IPv4 Alamat pribadi.
  - IPv6 alamat.
  - Alamat IP Elastis terkait dengan instans. Perhatikan bahwa ketika instans dihentikan, Anda akan dikenakan biaya untuk alamat IP Elastis terkait.

Diagram berikut menggambarkan apa yang bertahan dan apa yang hilang ketika instans EC2 dihentikan. Diagram dibagi menjadi tiga bagian: bagian pertama, berlabel Running EC2 instance, menunjukkan instance dalam `running` keadaan dengan sumber dayanya. Bagian kedua, berlabel Instans EC2 Berhenti, menunjukkan instance dalam `stopped` status dengan sumber daya yang bertahan. Bagian ketiga, berlabel Lost, menunjukkan sumber daya yang hilang ketika instance dihentikan.



Untuk informasi tentang apa yang terjadi ketika Anda menghentikan instance Mac, lihatMenghentikan atau menghentikan instans Amazon EC2 Mac Anda.

Apa yang terjadi jika Anda memulai sebuah instans

- Dalam kebanyakan kasus, instans dimigrasikan ke komputer host dasar yang baru (meskipun dalam beberapa kasus instans tetap di host saat ini, seperti ketika sebuah instans dialokasikan ke host dalam konfigurasi Host Khusus).
- Volume EBS terkait dan antarmuka jaringan disambungkan kembali ke instance.
- Amazon EC2 memberikan IPv4 alamat publik baru ke instans jika instans dikonfigurasi untuk menerima IPv4 alamat publik, kecuali jika memiliki antarmuka jaringan sekunder atau IPv4 alamat pribadi sekunder yang dikaitkan dengan alamat IP Elastis.
- Jika Anda menghentikan satu instans dalam grup penempatan dan kemudian memulainya lagi, ini masih berjalan dalam grup penempatan. Namun demikian, momen mulai gagal jika tidak cukup kapasitas untuk instans. Jika Anda menerima kesalahan kapasitas saat memulai instance dalam grup penempatan yang sudah menjalankan instance, hentikan semua instance di grup penempatan dan mulai semuanya lagi. Memulai instans dapat memigrasikannya ke perangkat keras yang memiliki kapasitas untuk semua proses yang diminta.

Uji respons aplikasi untuk berhenti dan mulai

Anda dapat menggunakan AWS Fault Injection Service untuk menguji bagaimana aplikasi Anda merespons ketika instance Anda dihentikan dan dimulai. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Fault Injection Service.

Biaya yang terkait dengan instans stop and start

Biaya berikut dikaitkan dengan menghentikan dan memulai sebuah instans.

Berhenti — Segera setelah status instance berubah menjadi `shutting-down` atau`terminated`, biaya tidak lagi dikeluarkan untuk instance tersebut. Anda tidak dikenakan biaya untuk penggunaan atau biaya transfer data untuk instans yang dihentikan. Biaya dikenakan untuk menyimpan volume penyimpanan Amazon EBS.

Mulai — Setiap kali Anda memulai instans berhenti, Anda dikenakan biaya minimal satu menit penggunaan. Setelah satu menit, Anda dikenai biaya hanya untuk detik yang digunakan. Misalnya, jika Anda menjalankan instans selama 20 detik, lalu menghentikannya, Anda akan dikenai biaya satu menit penggunaan. Jika Anda menjalankan instans selama 3 menit 40 detik, Anda dikenai biaya 3 menit dan 40 detik penggunaan.

Metode untuk menghentikan sebuah instance

Ada empat cara untuk melakukan stop yang dimulai pengguna: stop default, stop with skip OS shutdown, force stop, dan force stop dengan skip OS shutdown. Tabel berikut membandingkan perbedaan utama antara metode berhenti:

Metode berhenti	Tujuan utama	Kasus penggunaan	Perintah CLI
Berhenti default	Penonaktifan instance normal dengan upaya shutdown OS yang anggun.	Contoh khas berhenti.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0`
Berhenti dengan skip	Melewati shutdown OS yang anggun saat menghentikan sebuah instance.	Saat melewati shutdown OS yang anggun diperlukan.	`aws ec2 stop-instances \ --instance-id i-1234567`

Metode berhenti	Tujuan utama	Kasus penggunaan	Perintah CLI
OS shutdowr			890abcdef0 \ --skip-os-shutdown
Paksa berhenti	Menangani instance yang macet. Mencoba penghenti an default terlebih dahulu; jika instance gagal berhenti, maka secara paksa menghentikan instance.	Ketika instance macet dalam `stopping` keadaan.	aws ec2 stop-instances \ --instance-id i-1234567 890abcdef0 \ --force
Paksa berhenti dengan lewati shutdowr OS	Paksa berhenti dan melewati shutdown OS yang anggun saat menghentikan instance.	Saat memaksa berhenti dan melewati shutdown OS yang anggun diperlukan.	aws ec2 stop-instances \ --instance-id i-1234567 890abcdef0 \ --force \ --skip-os-shutdown

Untuk petunjuk tentang cara menggunakan setiap metode, lihat berikut ini:

- Hentikan instance dengan shutdown OS yang anggun
- Hentikan instance dan lewati shutdown OS yang anggun
- Paksa menghentikan sebuah instance

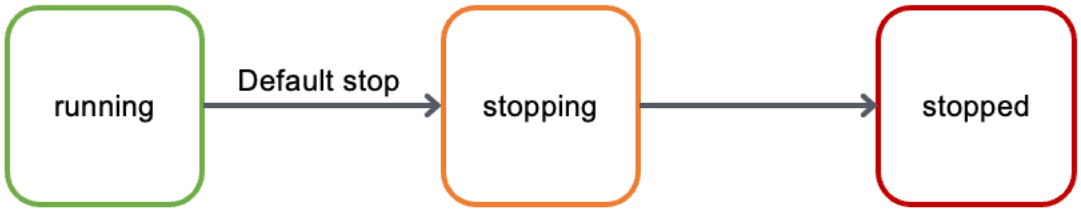
Hentikan metode:

- Berhenti default
- Berhenti dengan skip OS shutdown
- Paksa berhenti
- Paksa berhenti dengan lewati shutdown OS

Bagian berikut memberikan informasi lebih rinci tentang empat metode berhenti yang dimulai pengguna yang berbeda.

Berhenti default

Metode stop default adalah cara standar untuk menghentikan sebuah instance. Saat Anda mengeluarkan StopInstances perintah, instance bertransisi dari `running` status, ke, dan akhirnya ke `stoppingstopped`, seperti yang diilustrasikan oleh diagram berikut:



Tujuan: Penonaktifan instans normal dengan upaya shutdown OS yang anggun.

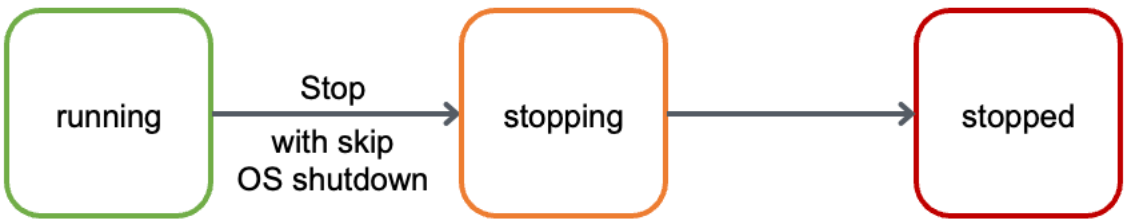
Dampak data: Mempertahankan data pada volume root EBS dan volume data. Kehilangan data pada volume penyimpanan instance.

Kapan menggunakan: Upaya berhenti pertama untuk pemberhentian biasa.

> **Note**
>
> Jika Anda sudah mencoba berhenti dengan skip OS shutdown, upaya berhenti default berikutnya selama sesi transisi status yang sama tidak akan melakukan shutdown OS anggun. Melewati shutdown OS yang anggun tidak dapat diubah untuk sesi instans saat ini.

Berhenti dengan skip OS shutdown

Saat melewati shutdown OS yang anggun diperlukan, metode stop with skip OS shutdown dapat digunakan untuk menghentikan instance dan melewati shutdown OS yang anggun, seperti yang diilustrasikan oleh diagram berikut:



> **Warning**
>
> Melewati shutdown OS yang anggun dapat mengakibatkan kehilangan atau kerusakan data (misalnya, konten memori tidak dibuang ke disk atau hilangnya dalam penerbangan IOs) atau skrip shutdown yang dilewati.

Tujuan: Lewati shutdown OS yang anggun saat menghentikan instance.

Dampak data: Dapat mengakibatkan hilangnya data atau korupsi. Isi memori mungkin tidak dibuang ke disk dan dalam penerbangan IOs mungkin hilang. Mungkin melewatkan skrip shutdown.

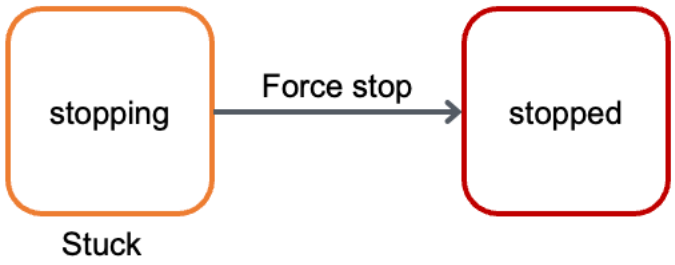
Kapan menggunakan: Saat melewati shutdown OS yang anggun diperlukan. Jika digunakan saat penghentian default dengan shutdown OS yang anggun sedang berlangsung, shutdown OS yang anggun akan dilewati.

> **Note**
>
> Melewati shutdown OS yang anggun tidak dapat diubah untuk sesi transisi status instans saat ini. Upaya berhenti default berikutnya selama sesi ini tidak akan mencoba shutdown OS yang anggun.

Paksa berhenti

Metode force stop digunakan untuk menangani instance yang macet dalam `stopping` keadaan. Sebuah instance biasanya macet karena masalah perangkat keras yang mendasarinya (ditunjukkan oleh pemeriksaan status sistem yang gagal).

Metode force stop pertama kali mencoba stop default. Jika instance tetap terjebak dalam `stopping` status, `force` parameter secara paksa mematikan instance dan mentransisikan instance ke `stopped` status, seperti yang ditunjukkan oleh diagram berikut:



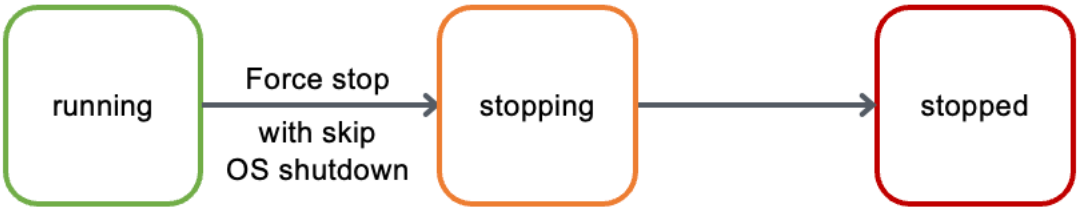
Tujuan: Menangani instance yang macet di `stopping` negara bagian. Mencoba berhenti default terlebih dahulu. Jika instance gagal berhenti, maka secara paksa mematikan instance.

Dampak data: Mencoba penghentian default terlebih dahulu, tetapi jika penghentian paksa terus berlanjut, maka dapat menyebabkan kehilangan data atau korupsi. Dalam kasus yang jarang terjadi, menghasilkan penulisan pasca-berhenti ke volume EBS atau sumber daya bersama lainnya.

Kapan menggunakan: Upaya berhenti kedua ketika sebuah instance tetap macet setelah penghentian default. Untuk informasi selengkapnya, lihat Memecahkan masalah penghentian EC2 instans Amazon.

Paksa berhenti dengan lewati shutdown OS

Ketika penghentian paksa dan melewati shutdown OS yang anggun diperlukan, force stop dengan metode skip OS shutdown dapat digunakan untuk membawa instance ke `stopped` status, seperti yang diilustrasikan dalam diagram berikut:



Tujuan: Menggabungkan force stop dengan melewati shutdown OS yang anggun saat menghentikan instance.

Dampak data: Lewati shutdown OS dapat mengakibatkan kehilangan data atau korupsi. Isi memori mungkin tidak dibuang ke disk dan dalam penerbangan IOs mungkin hilang. Mungkin melewatkan skrip shutdown. Jika force stop terus berlanjut, maka dapat menyebabkan kehilangan data tambahan atau korupsi. Dalam kasus yang jarang terjadi, hasil penulisan post-stop ke volume EBS atau sumber daya bersama lainnya.

Kapan menggunakan: Ketika Anda ingin memastikan bahwa instans Anda akan berhenti dan Anda ingin melewati shutdown OS anggun. Jika digunakan saat penghentian default dengan shutdown OS yang anggun sedang berlangsung, shutdown OS yang anggun akan dilewati.

Hentikan dan mulai instans Anda secara manual

Anda dapat menghentikan dan memulai instans yang didukung Amazon EBS (instans dengan volume root EBS). Anda tidak dapat menghentikan dan memulai instance dengan volume root penyimpanan instance.

Saat menggunakan metode default untuk menghentikan instance, shutdown sistem operasi (OS) anggun dicoba. Anda dapat melewati shutdown OS yang anggun; namun, ini mungkin berisiko integritas data.

> **Warning**
>
> Ketika Anda menghentikan instans, data pada setiap volume penyimpanan instans akan dihapus. Sebelum menghentikan instans, verifikasi bahwa Anda telah menyalin data apa pun yang Anda perlukan dari volume penyimpanan instans ke penyimpanan persisten, seperti Amazon EBS atau Amazon S3.

[Instance Linux] Menggunakan halt perintah OS dari sebuah instance tidak memulai shutdown. Jika Anda menggunakan perintah halt, instans tidak berakhir; tetapi, instans akan menempatkan CPU ke `HLT`, yang menangguhkan operasi CPU. Instans tetap berjalan.

Anda dapat memulai shutdown menggunakan OS shutdown atau poweroff perintah. Saat Anda menggunakan perintah OS, instans berhenti secara default. Anda dapat mengubah perilaku ini. Untuk informasi selengkapnya, lihat Ubah perilaku shutdown yang dimulai instance.

> **Note**
>
> Jika Anda menghentikan instans yang didukung Amazon EBS dan instans tersebut tampak "macet" di status `stopping`, Anda dapat menghentikannya secara paksa. Untuk informasi selengkapnya, lihat Memecahkan masalah penghentian EC2 instans Amazon.

Berhenti dan mulai metode

- Hentikan instance dengan shutdown OS yang anggun
- Hentikan instance dan lewati shutdown OS yang anggun
- Memulai instans

Hentikan instance dengan shutdown OS yang anggun

Anda dapat menghentikan instance menggunakan metode stop default, yang mencakup upaya shutdown OS yang anggun. Untuk informasi selengkapnya, lihat Berhenti default.

Console

Untuk menghentikan instance menggunakan metode stop default

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans, lalu pilih instance.
3. Pilih Status instans, Hentikan instans. Jika opsi ini dinonaktifkan, instance sudah dihentikan atau volume rootnya adalah volume penyimpanan instance.
4. Ketika diminta konfirmasi, pilih Berhenti. Hal ini dapat memerlukan waktu beberapa menit sampai instans berhenti.

AWS CLI

Untuk menghentikan instance menggunakan metode stop default

Gunakan perintah stop-instance.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk menghentikan instance menggunakan metode stop default

Gunakan Stop-EC2Instancecmdlet

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

Hentikan instance dan lewati shutdown OS yang anggun

Anda dapat melewati shutdown OS yang anggun saat menghentikan sebuah instance. Untuk informasi selengkapnya, lihat Berhenti dengan skip OS shutdown.

> **Warning**
>
> Melewati shutdown OS yang anggun dapat mengakibatkan kehilangan atau kerusakan data (misalnya, konten memori tidak dibuang ke disk atau hilangnya dalam penerbangan IOs) atau skrip shutdown yang dilewati.

Console

Untuk menghentikan instance dan melewati shutdown OS yang anggun

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih instans.
3. Pilih Keadaan nyata, Hentikan contoh.
4. Di bawah Lewati shutdown OS, pilih kotak centang Lewati OS shutdown. Jika Anda tidak melihat opsi ini di konsol, opsi ini belum tersedia di konsol di Wilayah saat ini. Namun, Anda dapat mengakses fitur ini menggunakan AWS CLI atau SDK, atau mencoba Wilayah lain di konsol.
5. Pilih Berhenti.

AWS CLI

Untuk menghentikan instance dan melewati shutdown OS yang anggun

Gunakan perintah stop-instance dengan. `--skip-os-shutdown`

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --skip-os-shutdown
```

PowerShell

Untuk menghentikan instance dan melewati shutdown OS yang anggun

Gunakan Stop-EC2Instancecmdlet dengan. `-SkipOsShutdown $true`

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -SkipOsShutdown $true
```

Memulai instans

Anda dapat memulai instance yang dihentikan.

Console

Untuk memulai sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans.
3. Pilih instance, dan pilih Instance state, Start instance.

   Hal ini diperlukan waktu beberapa menit hingga instans memasuki status `running`.

AWS CLI

Untuk memulai sebuah instance

Gunakan perintah start-instances.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk memulai sebuah instance

Gunakan Start-EC2Instancecmdlet.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Menghentikan dan memulai instans Anda secara otomatis

Anda dapat mengotomatisasi penghentian dan pemulaian instans dengan layanan berikut:

Penjadwal Instance aktif AWS

Anda dapat menggunakan Penjadwal Instance aktif AWS untuk mengotomatiskan awal dan penghentian instans EC2. Untuk informasi selengkapnya, lihat Bagaimana cara menggunakan Penjadwal Instance untuk CloudFormation menjadwalkan instans EC2? Perhatikan bahwa biaya tambahan berlaku.

AWS Lambda dan EventBridge aturan Amazon

Anda dapat menggunakan Lambda dan EventBridge aturan untuk menghentikan dan memulai instance Anda sesuai jadwal. Untuk informasi selengkapnya, lihat Bagaimana cara menggunakan Lambda untuk menghentikan dan memulai instans Amazon EC2 secara berkala?

Amazon EC2 Auto Scaling

Guna memastikan Anda memiliki jumlah instans Amazon EC2 yang tepat untuk menangani beban untuk aplikasi, buat grup Auto Scaling. Amazon EC2 Auto Scaling memastikan bahwa aplikasi Anda selalu memiliki kapasitas yang tepat untuk menangani permintaan lalu lintas, dan menghemat biaya dengan meluncurkan instans hanya saat dibutuhkan. Perhatikan bahwa Amazon EC2 Auto Scaling mengakhiri, bukan menghentikan, instans yang tidak dibutuhkan. Untuk menyiapkan grup Auto Scaling, lihat Memulai Amazon EC2 Auto Scaling.

Temukan semua instans yang berjalan dan berhenti

Anda dapat menemukan semua instans yang berjalan dan berhenti di semua Wilayah AWS pada satu halaman menggunakan Amazon EC2 Global View. Kemampuan ini sangat berguna untuk mengambil inventaris dan menemukan instans yang terlupakan. Untuk informasi tentang cara menggunakan Tampilan Global, lihat Melihat sumber daya di seluruh Wilayah menggunakan Tampilan AWS Global.

Atau, Anda dapat menjalankan perintah atau cmdlet di setiap Wilayah tempat Anda memiliki instance.

AWS CLI

Untuk mendapatkan jumlah instans EC2 di suatu Wilayah

Gunakan perintah describe-instance berikut untuk menghitung instance di Region saat ini. Anda harus menjalankan perintah ini di setiap Wilayah di mana Anda memiliki instance.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "length(Reservations[].Instances[])"
```

Berikut ini adalah output contoh.

```
27
```

Untuk mendapatkan info ringkasan tentang instans EC2 Anda di Wilayah

Gunakan perintah describe-instance berikut. Anda harus menjalankan perintah ini di setiap Wilayah di mana Anda memiliki instance.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "Reservations[].Instances[].[InstanceId,InstanceType,PrivateIpAddress]"
 \
    --output table
```

Berikut ini adalah output contoh.

```
-----------------------------------------------------------
|                  DescribeInstances                      |
+---------------------+---------------+-----------------+
|  i-0e3e777f4362f1bf7|  t2.micro     |  10.0.12.9      |
|  i-09453945dcf1529e9|  t2.micro     |  10.0.143.213   |
|  i-08fd74f3f1595fdbd|  m7i.4xlarge  |  10.0.1.103     |
+---------------------+---------------+-----------------+
```

PowerShell

Untuk mendapatkan jumlah instans EC2 di suatu Wilayah

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance -Region us-east-2).Instances.Length
```

Berikut ini adalah output contoh.

```
27
```

Untuk mendapatkan info ringkasan tentang instans EC2 Anda di Wilayah

Gunakan Get-EC2Instancecmdlet. Anda harus menjalankan perintah ini di setiap Wilayah di mana Anda memiliki instance.

```
(Get-EC2Instance).Instances | Select InstanceId, InstanceType, PrivateIpAddress
```

Berikut ini adalah output contoh.

```
InstanceId          InstanceType PrivateIpAddress
----------          ------------ ----------------
i-0e3e777f4362f1bf7 t2.micro     10.0.12.9
i-09453945dcf1529e9 t2.micro     10.0.143.213
i-08fd74f3f1595fdbd m7i.4xlarge  10.0.1.103
```

Temukan waktu peluncuran awal dan terbaru

Ketika Anda menjelaskan sebuah instance, waktu peluncuran untuk instance adalah waktu peluncuran terbarunya. Setelah Anda berhenti dan memulai sebuah instance, waktu peluncuran mencerminkan waktu mulai instance baru. Untuk menemukan waktu peluncuran awal untuk sebuah instance, bahkan setelah berhenti dan memulainya, lihat waktu di mana antarmuka jaringan utama dilampirkan ke instance.

Console

Untuk menemukan waktu peluncuran terbaru

Pilih instance dan temukan Waktu peluncuran di bawah Detail instans pada tab Detail.

Untuk menemukan waktu peluncuran awal

Pilih instance dan temukan antarmuka jaringan utama (indeks perangkat adalah 0) di bawah Antarmuka jaringan pada tab Jaringan.

AWS CLI

Untuk menemukan waktu peluncuran awal dan terbaru

Gunakan perintah describe-instance berikut untuk menampilkan waktu peluncuran awal dan waktu peluncuran terbaru untuk instance yang ditentukan.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query 'Reservations[].Instances[].
{InstanceID:InstanceId,InitialLaunch:NetworkInterfaces[0].Attachment.AttachTime,LastLaunch:L
```

Berikut ini adalah output contoh.

```
[
    {
```

```
        "InstanceID": "i-1234567890abcdef0",
        "InitialLaunch": "2024-04-19T00:47:08+00:00",
        "LastLaunch": "2024-05-27T06:24:06+00:00"
    }
]
```

PowerShell

Untuk menemukan waktu peluncuran terbaru

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.LaunchTime
```

Berikut ini adalah output contoh.

```
Monday, May 27, 2024 6:24:06 AM
```

Untuk menemukan waktu peluncuran awal

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance -
InstanceId i-1234567890abcdef0).Instances.NetworkInterfaces.Attachment.AttachTime
```

Berikut ini adalah output contoh.

```
Friday, April 19, 2024 12:47:08 AM
```

Aktifkan perlindungan berhenti untuk instans EC2 Anda

Untuk mencegah instans Anda berhenti secara tidak sengaja, Anda dapat mengaktifkan perlindungan penghentian untuk instans. Perlindungan penghentian juga melindungi instans Anda dari penghentian yang tidak disengaja.

`DisableApiStop`Atribut `ModifyInstanceAttribute`API Amazon EC2 mengontrol apakah instans dapat dihentikan dengan menggunakan konsol Amazon EC2, API, AWS CLI atau Amazon EC2. Anda dapat mengatur nilai atribut ini saat Anda meluncurkan instans, saat instans berjalan, atau saat instans berhenti.

Pertimbangan-pertimbangan

- Mengaktifkan perlindungan penghentian tidak menghindarkan Anda dari penghentian instans secara tidak sengaja dengan memulai pematian dari instans menggunakan perintah sistem operasi seperti shutdown atau poweroff.
- Mengaktifkan perlindungan berhenti tidak AWS mencegah menghentikan instance ketika ada acara terjadwal untuk menghentikan instance.
- Mengaktifkan perlindungan penghentian tidak mencegah Amazon EC2 Auto Scaling untuk menghentikan instans saat instans tidak sehat atau selama peristiwa penskalaan ke dalam. Anda dapat mengontrol apakah grup Auto Scaling dapat mengakhiri instans tertentu saat meningkatkan skala dengan menggunakan perlindungan peningkatan skala instans.
- Stop protection tidak hanya mencegah instans Anda dihentikan secara tidak sengaja, tetapi juga dari penghentian yang tidak disengaja saat menggunakan konsol, AWS CLI, atau API. Namun, itu tidak secara otomatis mengatur atribut `DisableApiTermination`. Perhatikan bahwa ketika `DisableApiStop` atribut disetel `kefalse`, setelan `DisableApiTermination` atribut menentukan apakah instance dapat dihentikan menggunakan konsol, AWS CLI, atau API. Untuk mengetahui informasi selengkapnya, lihat Mengakhiri instans Amazon EC2.
- Anda tidak dapat mengaktifkan perlindungan berhenti untuk instance dengan volume root penyimpanan instance.
- Anda tidak dapat mengaktifkan perlindungan penghentian untuk Instans Spot.
- Amazon EC2 API mengikuti model konsistensi akhir saat Anda mengaktifkan atau menonaktifkan perlindungan penghentian. Ini berarti bahwa hasil dari menjalankan perintah untuk mengatur atribut perlindungan penghentian mungkin tidak langsung terlihat oleh semua perintah berikutnya yang Anda jalankan. Untuk informasi selengkapnya, lihat Konsistensi akhir di Panduan Pengembang Amazon EC2.

Hentikan tugas perlindungan

- Aktifkan perlindungan penghentian untuk instans saat peluncuran
- Aktifkan perlindungan penghentian untuk instans yang berjalan atau dihentikan
- Nonaktifkan perlindungan penghentian untuk instans yang berjalan atau berhenti

Aktifkan perlindungan penghentian untuk instans saat peluncuran

Anda dapat mengaktifkan perlindungan berhenti untuk sebuah instance saat meluncurkan instance.

Console

Untuk mengaktifkan perlindungan penghentian untuk sebuah instans saat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada dasbor, pilih Luncurkan instans.
3. Konfigurasikan instans Anda di wizard peluncuran instans baru.
4. Di wizard, aktifkan perlindungan penghentian dengan memilih Aktifkan untuk Perlindungan penghentian di bawah Detail lanjutan.

AWS CLI

Untuk mengaktifkan perlindungan penghentian untuk sebuah instans saat peluncuran

Gunakan perintah run-instance untuk meluncurkan instance. Tambahkan parameter berikut.

```
--disable-api-stop
```

PowerShell

Untuk mengaktifkan perlindungan penghentian untuk sebuah instans saat peluncuran

Gunakan New-EC2Instancecmdlet untuk meluncurkan instance. Tambahkan parameter berikut.

```
-DisableApiStop $true
```

Aktifkan perlindungan penghentian untuk instans yang berjalan atau dihentikan

Anda dapat mengaktifkan perlindungan berhenti untuk sebuah instance saat instance sedang berjalan atau dihentikan.

Console

Untuk mengaktifkan perlindungan berhenti untuk sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans.
3. Pilih instans, lalu pilih Tindakan > Pengaturan instans > Ubah perlindungan penghentian.

4. Pilih kotak centang Aktifkan, lalu pilih Simpan.

AWS CLI

Untuk mengaktifkan perlindungan berhenti untuk sebuah instance

Gunakan perintah modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

PowerShell

Untuk mengaktifkan perlindungan berhenti untuk sebuah instance

Gunakan Edit-EC2InstanceAttributecmdlet.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiStop $true
```

Nonaktifkan perlindungan penghentian untuk instans yang berjalan atau berhenti

Anda dapat menonaktifkan proteksi penghentian untuk instans yang sedang berjalan atau berhenti menggunakan salah satu metode berikut.

Console

Untuk menonaktifkan perlindungan penghentian untuk instans yang berjalan atau dihentikan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans.
3. Pilih instans, lalu pilih Actions, instans settings, Change stop protection.
4. Kosongkan kotak centang Aktifkan, lalu pilih Simpan.

AWS CLI

Untuk menonaktifkan perlindungan penghentian untuk instans yang berjalan atau dihentikan

Gunakan perintah modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

PowerShell

Untuk menonaktifkan perlindungan berhenti untuk sebuah instance

Gunakan Edit-EC2InstanceAttributecmdlet.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiStop $false
```

Hibernasi instans Amazon EC2 Anda

Saat Anda melakukan hibernasi instance, Amazon EC2 memberi sinyal pada sistem operasi untuk melakukan hibernasi (). suspend-to-disk Hibernasi menyimpan konten dari memori instans (RAM) ke volume root Amazon Elastic Block Store (Amazon EBS). Amazon EC2 mempertahankan volume root EBS instans dan semua volume data EBS yang terlampir. Saat instans Anda dimulai:

- Volume root EBS dipulihkan ke status sebelumnya
- Isi RAM dimuat ulang
- Proses yang sebelumnya berjalan pada instans dilanjutkan
- Volume data terlampir sebelumnya akan dilampirkan kembali dan instans akan mempertahankan ID instansnya

Anda dapat menghibernasi instans hanya jika diaktifkan untuk hibernasi dan memenuhi prasyarat hibernasi.

Jika sebuah instans atau aplikasi membutuhkan waktu lama untuk melakukan bootstrap dan membangun jejak memori agar menjadi produktif sepenuhnya, Anda dapat menggunakan hibernasi untuk menghangatkan instans. Untuk menghangatkan instans, Anda:

1. Luncurkan dengan hibernasi diaktifkan.
2. Bawa ke status yang diinginkan.

3. Hibernasi sehingga siap dilanjutkan ke kondisi yang diinginkan kapan pun dibutuhkan.

Anda tidak dikenai biaya untuk penggunaan instans untuk instans hibernasi saat berada di status `stopped` atau untuk transfer data saat konten RAM ditransfer ke volume root EBS. Anda dikenai biaya untuk penyimpanan volume EBS apa pun, termasuk penyimpanan untuk konten RAM.

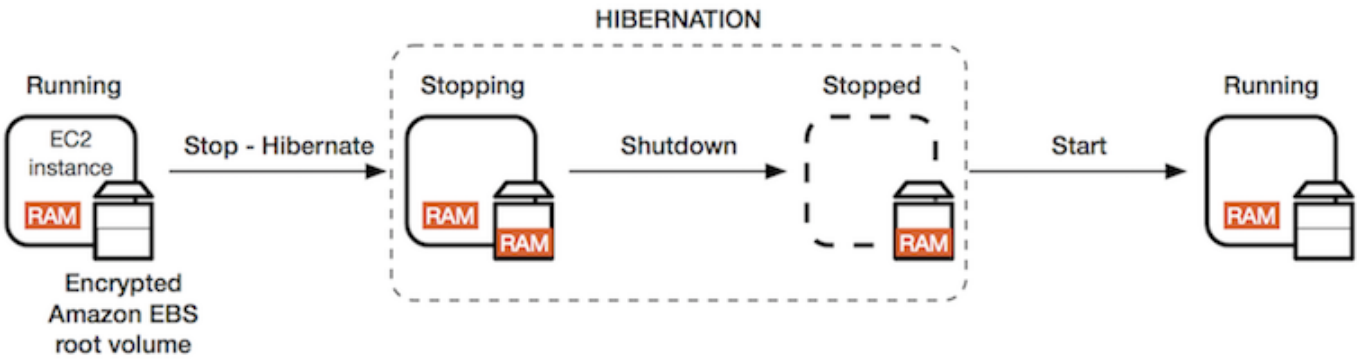
Jika Anda tidak lagi membutuhkan sebuah instans, Anda dapat mengakhirinya kapan saja, termasuk saat berada dalam status `stopped` (hibernasi). Untuk informasi selengkapnya, lihat Mengakhiri instans Amazon EC2.

Daftar Isi

- Cara kerja hibernasi instans Amazon EC2
- Prasyarat untuk hibernasi instans EC2
- Konfigurasikan AMI Linux untuk mendukung hibernasi
- Aktifkan hibernasi untuk instans Amazon EC2
- Nonaktifkan KASLR pada instans (khusus Ubuntu)
- Hibernasi instans Amazon EC2
- Memulai instans Amazon EC2 yang hibernasi
- Memecahkan masalah hibernasi instans Amazon EC2

Cara kerja hibernasi instans Amazon EC2

Diagram berikut menunjukkan gambaran dasar dari proses hibernasi untuk instans EC2.



Apa yang terjadi ketika Anda hibernasi sebuah instance

Saat Anda hibernasi sebuah instance, hal berikut terjadi:

- Contoh pindah ke `stopping` negara. Amazon EC2 memberi sinyal pada sistem operasi untuk melakukan hibernasi (). suspend-to-disk Hibernasi membekukan semua proses, menyimpan konten RAM ke volume root EBS, dan kemudian melakukan shutdown secara teratur.
- Setelah penonaktifan selesai, instans berpindah ke status `stopped`.
- Setiap volume EBS tetap terlampir pada instans, dan data tetap ada, termasuk konten RAM yang disimpan.
- Setiap volume penyimpanan instans Amazon EC2 tetap melekat pada instans, tetapi data pada volume penyimpanan instans hilang.
- Dalam kebanyakan kasus, instance dipindahkan ke komputer host baru yang mendasarinya saat dimulai. Ini juga yang terjadi ketika Anda berhenti dan memulai sebuah instans.
- Saat instans dimulai, instans melakukan booting dan sistem operasi membaca konten RAM dari volume root EBS, sebelum membatalkan proses untuk melanjutkan statusnya.
- Instans mempertahankan IPv4 alamat pribadinya dan IPv6 alamat apa pun. Ketika instance dimulai, instance terus mempertahankan IPv4 alamat pribadinya dan IPv6 alamat apa pun.
- Amazon EC2 merilis alamat IPv4 publik. Saat instans dimulai, Amazon EC2 memberikan IPv4 alamat publik baru ke instans.
- Instans mempertahankan alamat IP Elastis terkait Anda dikenai biaya untuk semua alamat IP Elastis yang terkait dengan instans hibernasi.

Untuk informasi tentang perbedaan hibernasi dari boot ulang, penghentian, dan pengakhiran, lihat Perbedaan antara status instance.

Batasan

- Ketika Anda menghibernasi suatu instans, data pada setiap volume penyimpanan instans akan hilang.
- (Instance Linux) Anda tidak dapat hibernasi instance Linux yang memiliki lebih dari 150 GiB RAM.
- (Instans Windows) Anda tidak dapat hibernasi instance Windows yang memiliki lebih dari 16 GiB RAM.
- Saat instance Anda hibernasi, Anda tidak dapat memodifikasinya. Ini berbeda dengan instance berhenti yang tidak hibernasi, di mana Anda dapat memodifikasi atribut tertentu, seperti jenis atau ukuran instance.
- Jika Anda membuat snapshot atau AMI dari instans yang hibernasi atau mengaktifkan hibernasi, Anda mungkin tidak dapat terhubung ke instans baru yang diluncurkan dari AMI, atau dari AMI yang dibuat dari snapshot.

- (Instans Spot saja) Jika Amazon EC2 menghibernasi Instans Spot Anda, hanya Amazon EC2 yang dapat melanjutkan instans Anda. Jika Anda hibernasi instans Spot (hibernasi yang dimulai pengguna), Anda dapat melanjutkan instans Anda. Instans Spot hibernasi hanya dapat dilanjutkan jika kapasitas tersedia dan harga Spot kurang dari atau sama dengan harga maksimum yang Anda tentukan.
- Anda tidak dapat menghibernasi instans yang berada dalam grup Auto Scaling atau digunakan oleh Amazon ECS. Jika instans Anda berada dalam grup Auto Scaling dan Anda mencoba untuk hibernasi, layanan Amazon EC2 Auto Scaling menandai instans yang dihentikan sebagai tidak sehat, dan mungkin mengakhirinya serta meluncurkan instans pengganti. Untuk informasi selengkapnya, lihat Health memeriksa instans di grup Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling.
- Anda tidak dapat hibernasi instance yang dikonfigurasi untuk boot dalam mode UEFI dengan UEFI Secure Boot diaktifkan.
- Jika Anda menghibernasi instans yang diluncurkan ke sebuah Reservasi Kapasitas, maka Reservasi Kapasitas tersebut tidak memastikan apakah instans yang dihibernasi dapat melanjutkan setelah Anda mencoba untuk memulainya.
- Anda tidak dapat menghibernasi instans yang menggunakan kernel di bawah 5.10 jika mode Federal Information Processing Standard (FIPS) diaktifkan.
- Kami tidak mendukung penyimpanan instans dalam mode hibernasi selama lebih dari 60 hari. Untuk mempertahankan instans lebih dari 60 hari, Anda harus memulai instans hibernasi, menghentikan instans, dan memulainya.
- Kami terus memperbarui platform kami dengan peningkatan dan tambalan keamanan, yang dapat bertentangan dengan instans hibernasi yang ada. Kami memberi tahu Anda tentang pembaruan penting yang memerlukan pemulaian untuk instans hibernasi sehingga kami dapat melakukan pematian atau boot ulang untuk menerapkan pemutakhiran dan patch keamanan yang diperlukan.

Pertimbangan untuk menghibernasi instans Spot

- Jika Anda menghibernasi Instans Spot, Anda hanya dapat memulai ulang jika kapasitas tersedia dan harga Spot kurang dari atau sama dengan harga maksimum yang Anda tentukan.
- Jika Amazon EC2 menghibernasi Instans Spot Anda:
  - Hanya Amazon EC2 yang dapat melanjutkan instans Anda.
  - Amazon EC2 melanjutkan Instans Spot hibernasi jika kapasitas tersedia dan harga Spot kurang dari atau sama dengan harga maksimum yang Anda tentukan.

- Sebelum Amazon EC2 menghibernasi Instans Spot, Anda akan menerima pemberitahuan interupsi dua menit sebelum hibernasi dimulai.

Untuk informasi selengkapnya, lihat Interupsi Instans Spot.

Prasyarat untuk hibernasi instans EC2

Anda dapat mengaktifkan dukungan hibernasi untuk Instans Sesuai Permintaan atau Instans Spot saat meluncurkannya. Anda tidak dapat mengaktifkan hibernasi pada instance yang ada, baik sedang berjalan atau dihentikan. Untuk informasi selengkapnya, lihat Aktifkan hibernasi instance.

Persyaratan untuk hibernasi sebuah instance

- Wilayah AWS
- AMIs
- Keluarga contoh
- Ukuran RAM instans
- Tipe volume root
- Ukuran volume akar
- Enkripsi volume root
- Jenis Volume EBS
- Permintaan Instans Spot

Wilayah AWS

Anda dapat menggunakan hibernasi dengan instance di semua. Wilayah AWS

AMIs

Anda harus menggunakan AMI HVM yang mendukung hibernasi. Berikut AMIs dukungan hibernasi:

Linux AMIs

AMIs untuk jenis instans Intel dan AMD

- AL2023 AMI dirilis 2023.09.20 atau lebih baru [1]
- AMI Amazon Linux 2 yang dirilis 29.08.2019 atau setelahnya

- AMI Amazon Linux 2018.03 yang dirilis 16.11.2018 atau setelahnya
- CentOS versi 8 AMI [2] (Diperlukan konfigurasi tambahan)
- Fedora versi 34 atau yang lebih baru AMI [2] (Diperlukan konfigurasi tambahan)
- Red Hat Enterprise Linux (RHEL) 9 AMI [2] (Diperlukan konfigurasi tambahan)
- Red Hat Enterprise Linux (RHEL) 8 AMI [2] (Diperlukan konfigurasi tambahan)
- Ubuntu 22.04.2 LTS (Jammy Jellyfish) AMI dirilis dengan nomor seri 20230303 atau lebih baru [3]
- Ubuntu 20.04 LTS (Focal Fossa) AMI dirilis dengan nomor seri 20210820 atau lebih baru [3]
- Ubuntu 18.04 LTS (Bionic Beaver) AMI dirilis dengan nomor seri 20190722.1 atau yang lebih baru [3]
- Ubuntu 16.04 LTS (Xenial Xerus) AMI [3] ↲ (Konfigurasi tambahan diperlukan)

AMIs untuk jenis instance Graviton

- AL2023 AMI (64-bit Arm) dirilis 2024.07.01 atau lebih baru [1]
- Amazon Linux 2 AMI (64-bit Arm) dirilis 2024.06.20 atau lebih baru
- Ubuntu 22.04.2 LTS (64-bit Arm) (Jammy Jellyfish) AMI dirilis dengan nomor seri 20240701 atau lebih baru [3]
- Ubuntu 20.04 LTS (64-bit Arm) (Focal Fossa) AMI dirilis dengan nomor seri 20240701 atau lebih baru [3]

[1] Untuk AMI AL2023 minimal, konfigurasi tambahan diperlukan.

[2] Untuk CentOS, Fedora, dan Red Hat Enterprise Linux, hibernasi hanya didukung pada instans berbasis Nitro.

[3] Kami merekomendasikan untuk menonaktifkan KASLR pada instance dengan Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver), dan Ubuntu 16.04 LTS (Xenial Xerus). Untuk informasi selengkapnya, lihat Nonaktifkan KASLR pada instans (khusus Ubuntu).

Untuk AMI Ubuntu 16.04 LTS (Xenial Xerus), hibernasi tidak didukung pada jenis instance. `t3.nano` Tidak ada tambalan yang akan tersedia karena Ubuntu (Xenial Xerus) mengakhiri dukungan pada April 2021. Jika Anda ingin menggunakan tipe instans `t3.nano`, kami sarankan Anda untuk memutakhirkan ke Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa) AMI, atau AMI Ubuntu 18.04 LTS (Bionic Beaver).

Dukungan untuk Ubuntu 18.04 LTS (Bionic Beaver) dan Ubuntu 16.04 LTS (Xenial Xerus) telah mencapai akhir hayat.

Untuk mengonfigurasi AMI Anda sendiri untuk mendukung hibernasi, lihat Konfigurasikan AMI Linux untuk mendukung hibernasi.

Dukungan untuk versi lain dari Ubuntu dan sistem operasi lain akan segera hadir.

Jendela AMIs

- AMI Windows Server 2022 yang dirilis 13.09.2023 atau setelahnya.
- AMI Windows Server 2019 yang dirilis 11.09.2019 atau setelahnya.
- AMI Windows Server 2016 yang dirilis 11.09.2019 atau setelahnya.
- AMI Windows Server 2012 R2 yang dirilis 11.09.2019 atau setelahnya
- AMI Windows Server 2012 yang dirilis 11.09.2019 atau setelahnya.

Keluarga contoh

Anda harus menggunakan keluarga instance yang mendukung hibernasi. Namun, instans bare metal tidak didukung.

- Tujuan umum: M3, M4, M5, M5a, M5ad, M5d, M6a, M6g, M6gd, M6i, M6id, M6iDN, M6in, M7a, M7g, M7gD, M7i, M7i-flex, M8a, M8AZN, M8g, M8GB, M8gd, M8gn, M8i, M8i-flex, T2, T3, T3a, T4g
- Komputasi dioptimalkan: C3, C4, C5, C5d, C6a, C6g, C6gd, C6GN, C6i, C6id, C6in, C7a, C7g, C7gd, C7gN, C7i, C7i-flex, C8a, C8g, C8GB, C8gD, C8gD, C8gD, C8gN, C8i, C8i-Flex
- Memori dioptimalkan: R3, R4, R5, R5a, R5ad, R5d, R6a, R6g, R6gd, R6iDn, R6in, R7a, R7g, R7gd, R7i, R7iZ, R8a, R8g, R8GB, R8gd, R8gD, R8gn, R8i, R8i Fleksibel, X2GD, X8AEDZ, X8i
- Penyimpanan dioptimalkan: I3, i3en, i4G, i7i, i7ie, i8g, i8ge, iM4gn, Is4gen

Console

Untuk mendapatkan jenis instance yang mendukung hibernasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Tipe Instans.
3. Tambahkan filter On-Demand Hibernation support = true.

4. (Opsional) Tambahkan filter ke cakupan lebih lanjut ke jenis instans tertentu yang menarik.

AWS CLI

Untuk mendapatkan jenis instance yang mendukung hibernasi

Gunakan perintah describe-instance-types. Perhatikan bahwa jenis instans yang tersedia bervariasi menurut Wilayah.

```
aws ec2 describe-instance-types \
    --filters Name=hibernation-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Untuk mendapatkan jenis instance yang mendukung hibernasi

Gunakan Get-EC2InstanceTypecmdlet. Perhatikan bahwa jenis instans yang tersedia bervariasi menurut Wilayah.

```
(Get-EC2InstanceType `
    -Filter @{Name="hibernation-supported"; Values="true"}).InstanceType | Sort-
Object
```

Ukuran RAM instans

Instans Linux — Harus kurang dari 150 GiB.

Instans Windows — Harus kurang dari atau sama dengan 16 GiB. Untuk hibernasi instance Windows T3 atau T3a, kami merekomendasikan setidaknya 1 GiB RAM.

Tipe volume root

Volume root harus berupa volume EBS, bukan volume penyimpanan instans.

Ukuran volume akar

Volume root harus cukup besar untuk menyimpan konten RAM dan mengakomodasi penggunaan yang Anda harapkan, misalnya, OS atau aplikasi. Jika Anda mengaktifkan hibernasi, ruang dialokasikan pada volume root saat peluncuran untuk menyimpan RAM.

Enkripsi volume root

Volume root harus dienkripsi untuk memastikan perlindungan konten sensitif yang ada di memori pada saat hibernasi. Ketika data RAM dipindahkan ke volume root EBS, data itu selalu dienkripsi. Enkripsi volume root diberlakukan saat peluncuran instans.

Gunakan salah satu dari tiga opsi berikut untuk memastikan bahwa volume root adalah volume EBS terenkripsi:

- Enkripsi EBS secara default — Anda dapat mengaktifkan enkripsi EBS secara default untuk memastikan bahwa semua volume EBS baru yang dibuat di AWS akun Anda dienkripsi. Dengan cara ini, Anda dapat mengaktifkan hibernasi untuk instans Anda tanpa menentukan maksud enkripsi pada peluncuran instans. Untuk informasi selengkapnya, lihat Mengaktifkan enkripsi secara default.
- Enkripsi "satu langkah" EBS – Anda dapat meluncurkan instans EC2 yang didukung EBS terenkripsi dari AMI yang tidak terenkripsi dan juga mengaktifkan hibernasi pada saat yang bersamaan. Untuk informasi selengkapnya, lihat Gunakan enkripsi dengan dukungan EBS AMIs.
- AMI terenkrips – Anda dapat mengaktifkan enkripsi EBS dengan menggunakan AMI terenkripsi untuk meluncurkan instans Anda. Jika AMI Anda tidak memiliki snapshot root terenkripsi, Anda dapat menyalinnya ke AMI baru dan meminta enkripsi. Untuk informasi selengkapnya, lihat Mengenkripsikan gambar yang tidak dienkripsi selama penyalinan dan Menyalin AMI.

Jenis Volume EBS

Volume EBS harus menggunakan salah satu jenis volume EBS berikut:

- SSD Tujuan Umum (`gp2` dan `gp3`)
- SSD IOPS yang Tersedia (`io1` dan `io2`)

Jika Anda memilih tipe volume SSD IOPS yang Tersedia, Anda harus menyediakan volume EBS dengan IOPS yang sesuai untuk mencapai performa yang optimal untuk hibernasi. Untuk informasi selengkapnya, lihat Jenis volume Amazon EBS di Panduan Pengguna Amazon EBS.

Permintaan Instans Spot

Untuk Instans Spot, persyaratan berikut berlaku:

- Tipe permintaan Instans Spot harus `persistent`.

- Anda tidak dapat menentukan grup peluncuran dalam permintaan Instans Spot.

Konfigurasikan AMI Linux untuk mendukung hibernasi

AMI Linux berikut dapat mendukung hibernasi instans Amazon EC2, asalkan Anda menyelesaikan langkah-langkah konfigurasi tambahan yang dijelaskan di bagian ini.

Konfigurasi tambahan diperlukan untuk:

- AL2023 AMI minimal dirilis 2023.09.20 atau lebih baru
- AMI minimal Amazon Linux 2 yang dirilis 29.08.2019 atau setelahnya
- AMI Amazon Linux 2 yang dirilis 29.08.2019
- Amazon Linux yang dirilis sebelum 16.11.2018
- CentOS versi 8 atau setelahnya
- Fedora versi 34 atau setelahnya
- Red Hat Enterprise Linux versi 8 atau 9
- Ubuntu 20.04 LTS (Focal Fossa) dirilis sebelum nomor seri 20210820
- Ubuntu 18.04 (Bionic Beaver) dirilis dengan nomor seri 20190722.1
- Ubuntu 16.04 (Xenial Xerus)

Untuk Linux dan Windows AMIs yang mendukung hibernasi dan yang tidak diperlukan konfigurasi tambahan, lihat. AMIs

Untuk informasi selengkapnya, lihat Memperbarui perangkat lunak instans di instans Amazon Linux 2 Anda.

AL2023 AMI minimal dirilis 2023.09.20 atau lebih baru

Untuk mengonfigurasi AMI AL2023 minimal yang dirilis 2023.09.20 atau yang lebih baru untuk mendukung hibernasi

1. Instal paket `ec2-hibinit-agent` dari repositori.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

2. Mulai ulang layanan.

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

AMI minimal Amazon Linux 2 yang dirilis 29.08.2019 atau setelahnya

Untuk mengonfigurasi AMI minimal Amazon Linux 2 yang dirilis 29.08.2019 atau setelahnya untuk mendukung hibernasi

1. Instal paket `ec2-hibinit-agent` dari repositori.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Mulai ulang layanan.

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

AMI Amazon Linux 2 yang dirilis 29.08.2019

Untuk mengonfigurasi AMI Amazon Linux 2 yang dirilis sebelum 29.08.2019 untuk mendukung hibernasi

1. Perbarui kernel ke `4.14.138-114.102` atau lebih baru.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instal paket `ec2-hibinit-agent` dari repositori.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

4. Konfirmasikan bahwa versi kernel telah diperbarui ke `4.14.138-114.102` atau setelahnya.

```
[ec2-user ~]$ uname -a
```

5. Hentikan instans dan buat AMI. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.

Amazon Linux yang dirilis sebelum 16.11.2018

Untuk mengonfigurasi AMI Amazon Linux 2 yang dirilis sebelum 16.11.2018 untuk mendukung hibernasi

1. Perbarui kernel ke `4.14.77-70.59` atau lebih baru.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instal paket `ec2-hibinit-agent` dari repositori.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

4. Konfirmasikan bahwa versi kernel telah diperbarui ke `4.14.77-70.59` atau yang lebih tinggi.

```
[ec2-user ~]$ uname -a
```

5. Hentikan instans dan buat AMI. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.

CentOS versi 8 atau setelahnya

Untuk mengonfigurasi CentOS versi 8 atau AMI setelahnya untuk mendukung hibernasi

1. Perbarui kernel ke `4.18.0-305.7.1.el8_4.x86_64` atau lebih baru.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instal repositori Fedora Extra Packages for Enterprise Linux (EPEL).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-
latest-8.noarch.rpm
```

3. Instal paket `ec2-hibinit-agent` dari repositori.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Aktifkan agen hibernasi untuk memulai saat boot.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

6. Konfirmasikan bahwa versi kernel telah diperbarui ke `4.18.0-305.7.1.el8_4.x86_64` atau setelahnya.

```
[ec2-user ~]$ uname -a
```

Fedora versi 34 atau setelahnya

Untuk mengkonfigurasi Fedora versi 34 atau AMI setelahnya untuk mendukung hibernasi

1. Perbarui kernel ke `5.12.10-300.fc34.x86_64` atau lebih baru.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instal paket `ec2-hibinit-agent` dari repositori.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Aktifkan agen hibernasi untuk memulai saat boot.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

5. Konfirmasikan bahwa versi kernel telah diperbarui ke `5.12.10-300.fc34.x86_64` atau setelahnya.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux versi 8 atau 9

Untuk mengonfigurasi Red Hat Enterprise Linux 8 atau 9 AMI untuk mendukung hibernasi

1. Perbarui kernel ke `4.18.0-305.7.1.el8_4.x86_64` atau lebih baru.

   ```
   [ec2-user ~]$ sudo yum update kernel
   ```

2. Instal repositori Fedora Extra Packages for Enterprise Linux (EPEL).

   RHEL versi 8:

   ```
   [ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

   RHEL versi 9:

   ```
   [ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

3. Instal paket `ec2-hibinit-agent` dari repositori.

   ```
   [ec2-user ~]$ sudo yum install ec2-hibinit-agent
   ```

4. Aktifkan agen hibernasi untuk memulai saat boot.

   ```
   [ec2-user ~]$ sudo systemctl enable hibinit-agent.service
   ```

5. Boot ulang instans.

   ```
   [ec2-user ~]$ sudo reboot
   ```

6. Konfirmasikan bahwa versi kernel telah diperbarui ke `4.18.0-305.7.1.el8_4.x86_64` atau setelahnya.

   ```
   [ec2-user ~]$ uname -a
   ```

Ubuntu 20.04 LTS (Focal Fossa) dirilis sebelum nomor seri 20210820

Untuk mengonfigurasi AMI Ubuntu 20.04 LTS (Focal Fossa) yang dirilis sebelum nomor seri 20210820 untuk mendukung hibernasi

1. Perbarui linux-aws-kernel ke `5.8.0-1038.40` atau yang lebih baru, dan grub2 ke `2.04-1ubuntu26.13` atau lebih baru.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

3. Konfirmasikan bahwa versi kernel telah diperbarui ke `5.8.0-1038.40` atau setelahnya.

```
[ec2-user ~]$ uname -a
```

4. Konfirmasikan bahwa versi grub2 diperbarui ke `2.04-1ubuntu26.13` atau lebih baru.

```
[ec2-user ~]$ dpkg --list | grep grub2-common
```

Ubuntu 18.04 (Bionic Beaver) dirilis dengan nomor seri 20190722.1

Untuk mengonfigurasi AMI Ubuntu 18.04 LTS yang dirilis sebelum nomor seri 20190722.1 untuk mendukung hibernasi

1. Perbarui kernel ke `4.15.0-1044` atau lebih baru.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Instal paket `ec2-hibinit-agent` dari repositori.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

4. Konfirmasikan bahwa versi kernel telah diperbarui ke `4.15.0-1044` atau setelahnya.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Untuk mengkonfigurasi Ubuntu 16.04 LTS untuk mendukung hibernasi, Anda perlu menginstal paket linux-aws-hwe kernel versi 4.15.0-1058-aws atau yang lebih baru dan ec2-hibinit-agent.

> **Important**
>
> Paket kernel `linux-aws-hwe` didukung sepenuhnya oleh Canonical. Dukungan standar untuk Ubuntu 16.04 LTS berakhir pada April 2021, dan paket tidak lagi menerima pembaruan rutin. Namun, ini akan menerima pembaruan keamanan tambahan hingga dukungan Pemeliharaan Keamanan Diperpanjang berakhir pada 2024. Untuk informasi selengkapnya, lihat Hibernasi Amazon EC2 untuk Ubuntu 16.04 LTS sekarang tersedia di Blog Ubuntu Canonical.
> Kami menyarankan Anda untuk memutakhirkan ke AMI Ubuntu 20.04 LTS (Focal Fossa) atau AMI Ubuntu 18.04 LTS (Bionic Beaver).

Untuk mengonfigurasi AMI Ubuntu 16.04 LTS untuk mendukung hibernasi

1. Perbarui kernel ke `4.15.0-1058-aws` atau lebih baru.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Instal paket `ec2-hibinit-agent` dari repositori.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

4. Konfirmasikan bahwa versi kernel telah diperbarui ke `4.15.0-1058-aws` atau setelahnya.

```
[ec2-user ~]$ uname -a
```

Aktifkan hibernasi untuk instans Amazon EC2

Untuk menghibernasi instans, Anda harus terlebih dahulu mengaktifkannya untuk hibernasi saat meluncurkan instans.

> **Important**
>
> Anda tidak dapat mengaktifkan atau menonaktifkan hibernasi untuk sebuah instans setelah Anda meluncurkannya.

Tugas

- Aktifkan hibernasi pada Instans Sesuai Permintaan
- Aktifkan hibernasi untuk Instans Spot
- Untuk melihat apakah instans diaktifkan untuk hibernasi

Aktifkan hibernasi pada Instans Sesuai Permintaan

Anda dapat mengaktifkan hibernasi untuk Instans Sesuai Permintaan.

Console

Untuk mengaktifkan hibernasi pada Instans Sesuai Permintaan

1. Ikuti prosedur untuk meluncurkan instans, tetapi jangan meluncurkan instans sampai Anda menyelesaikan langkah-langkah berikut untuk mengaktifkan hibernasi.
2. Untuk mengaktifkan hibernasi, konfigurasikan bidang berikut di wizard peluncuran instans:
   a. Pada Aplikasi dan Gambar OS (Amazon Machine Image), pilih AMI yang mendukung hibernasi. Untuk informasi selengkapnya, lihat AMIs.
   b. Pada Tipe instans, pilih tipe instans yang didukung. Untuk informasi selengkapnya, lihat Keluarga contoh.
   c. Pada Konfigurasikan penyimpanan, pilih Lanjutan (di sebelah kanan), dan tentukan informasi berikut untuk volume root:
      - Untuk Ukuran (GiB), masukkan ukuran volume root EBS. Volume harus cukup besar untuk menyimpan konten RAM dan mengakomodasi penggunaan yang Anda harapkan.

- Untuk Tipe volume, pilih tipe volume EBS yang didukung, SSD Tujuan Umum (gp2 dan gp3) atau SSD IOPS yang Tersedia (io1 dan io2).
- Untuk Terenkripsi, pilih Ya. Jika Anda mengaktifkan enkripsi secara default di AWS Wilayah ini, Ya dipilih.
- Untuk Kunci KMS, pilih kunci enkripsi untuk volume. Jika Anda mengaktifkan enkripsi secara default di AWS Wilayah ini, kunci enkripsi default dipilih.

Untuk informasi selengkapnya tentang prasyarat volume root, lihat Prasyarat untuk hibernasi instans EC2.

d. Perluas Detail lanjutan, dan untuk Perilaku Hentikan - Hibernasi, pilih Aktifkan.

3. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

AWS CLI

Untuk mengaktifkan hibernasi pada Instans Sesuai Permintaan

Gunakan perintah run-instances untuk meluncurkan instans. Tentukan parameter volume root EBS menggunakan parameter `--block-device-mappings file://mapping.json`, dan aktifkan hibernasi menggunakan parameter `--hibernation-options Configured=true`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

Tentukan hal berikut dalam `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
```

```
            "Encrypted": true
        }
    }
]
```

Nilai untuk `DeviceName` harus cocok dengan nama perangkat root yang terkait dengan AMI. Untuk menemukan nama perangkat root, gunakan perintah describe-images.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Jika Anda mengaktifkan enkripsi secara default di AWS Wilayah ini, Anda dapat menghilangkannya`"Encrypted": true`.

PowerShell

Untuk mengaktifkan hibernasi pada Instans Sesuai Permintaan

Gunakan New-EC2Instanceperintah untuk meluncurkan sebuah instance. Tentukan volume root EBS dengan menentukan pemetaan perangkat blok terlebih dahulu, lalu menambahkannya ke perintah menggunakan parameter `-BlockDeviceMappings`. Aktifkan hibernasi menggunakan parameter `-HibernationOptions_Configured $true`.

```
$ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
$ebs_encrypt.DeviceName = "/dev/xvda"
$ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs_encrypt.Ebs.VolumeSize = 30
$ebs_encrypt.Ebs.VolumeType = "gp2"
$ebs_encrypt.Ebs.Encrypted = $true

New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair
```

Nilai untuk `DeviceName` harus cocok dengan nama perangkat root yang terkait dengan AMI. Untuk menemukan nama perangkat root, gunakan Get-EC2Imageperintah.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Jika Anda mengaktifkan enkripsi secara default di AWS Wilayah ini, Anda dapat menghilangkan `Encrypted = $true` pemetaan perangkat blok.

Aktifkan hibernasi untuk Instans Spot

Anda dapat mengaktifkan hibernasi untuk Instans Spot Anda. Untuk informasi selengkapnya tentang hibernasi instans Spot saat interupsi, lihat Interupsi Instans Spot.

Console

Untuk mengaktifkan hibernasi untuk Instans Spot

1. Ikuti prosedur untuk meminta Instans Spot menggunakan wizard peluncuran instans, tetapi jangan luncurkan instans sampai Anda menyelesaikan langkah-langkah berikut untuk mengaktifkan hibernasi.
2. Untuk mengaktifkan hibernasi, konfigurasikan bidang berikut di wizard peluncuran instans:
   a. Pada Aplikasi dan Gambar OS (Amazon Machine Image), pilih AMI yang mendukung hibernasi. Untuk informasi selengkapnya, lihat AMIs.
   b. Pada Tipe instans, pilih tipe instans yang didukung. Untuk informasi selengkapnya, lihat Keluarga contoh.
   c. Pada Konfigurasikan penyimpanan, pilih Lanjutan (di sebelah kanan), dan tentukan informasi berikut untuk volume root:
      - Untuk Ukuran (GiB), masukkan ukuran volume root EBS. Volume harus cukup besar untuk menyimpan konten RAM dan mengakomodasi penggunaan yang Anda harapkan.
      - Untuk Tipe volume, pilih tipe volume EBS yang didukung, SSD Tujuan Umum (`gp2` dan `gp3`) atau SSD IOPS yang Tersedia (`io1` dan `io2`).
      - Untuk Terenkripsi, pilih Ya. Jika Anda mengaktifkan enkripsi secara default di AWS Wilayah ini, Ya dipilih.
      - Untuk Kunci KMS, pilih kunci enkripsi untuk volume. Jika Anda mengaktifkan enkripsi secara default di AWS Wilayah ini, kunci enkripsi default dipilih.

      Untuk informasi selengkapnya tentang prasyarat volume root, lihat Prasyarat untuk hibernasi instans EC2.

d. Perluas Detail lanjutan, dan, selain bidang untuk mengonfigurasi instans Spot, lakukan hal berikut:

   i. Untuk Tipe permintaan, pilih Persisten.

   ii. Untuk Perilaku interupsi, pilih Hibernasi. Atau, untuk perilaku Berhenti - Hibernasi, pilih Aktifkan. Kedua bidang mengaktifkan hibernasi pada Instans Spot Anda. Anda hanya perlu mengonfigurasi salah satunya.

3. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

AWS CLI

Untuk mengaktifkan hibernasi untuk Instans Spot

Gunakan perintah run-instances untuk meminta Instans Spot. Tentukan parameter volume root EBS menggunakan parameter `--block-device-mappings file://mapping.json`, dan aktifkan hibernasi menggunakan parameter `--hibernation-options Configured=true`. Tipe permintaan Spot (`SpotInstanceType`) harus `persistent`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
              "SpotInstanceType":"persistent"
            }
        }
```

Tentukan parameter volume root EBS `mapping.json` sebagai berikut.

```
[
    {
```

```
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

Nilai untuk `DeviceName` harus cocok dengan nama perangkat root yang terkait dengan AMI. Untuk menemukan nama perangkat root, gunakan perintah describe-images.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Jika Anda mengaktifkan enkripsi secara default di AWS Wilayah ini, Anda dapat menghilangkannya`"Encrypted": true`.

PowerShell

Untuk mengaktifkan hibernasi untuk Instans Spot

Gunakan New-EC2Instanceperintah untuk meminta Instance Spot. Tentukan volume root EBS dengan menentukan pemetaan perangkat blok terlebih dahulu, lalu menambahkannya ke perintah menggunakan parameter `-BlockDeviceMappings`. Aktifkan hibernasi menggunakan parameter `-HibernationOptions_Configured $true`.

```
$ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
$ebs_encrypt.DeviceName = "/dev/xvda"
$ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs_encrypt.Ebs.VolumeSize = 30
$ebs_encrypt.Ebs.VolumeType = "gp2"
$ebs_encrypt.Ebs.Encrypted = $true

New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair `
    -InstanceMarketOption @(
```

```
        MarketType = spot;
        SpotOptions @{
        MaxPrice = 1;
        SpotInstanceType = persistent}
    )
```

Nilai untuk `DeviceName` harus cocok dengan nama perangkat root yang terkait dengan AMI. Untuk menemukan nama perangkat root, gunakan Get-EC2Imageperintah.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Jika Anda mengaktifkan enkripsi secara default di AWS Wilayah ini, Anda dapat menghilangkan `Encrypted = $true` pemetaan perangkat blok.

Untuk melihat apakah instans diaktifkan untuk hibernasi

Anda dapat memeriksa apakah sebuah instance diaktifkan untuk hibernasi.

Console

Untuk melihat apakah instans diaktifkan untuk hibernasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans dan, pada tab Detail, di bagian Detail instans, periksa Perilaku berhenti - hibernasi. Enabled menunjukkan bahwa instans diaktifkan untuk hibernasi.

AWS CLI

Untuk melihat apakah instans diaktifkan untuk hibernasi

Gunakan perintah describe-instances dan tentukan parameter `--filters "Name=hibernation-options.configured,Values=true"` untuk memfilter instans yang diaktifkan untuk hibernasi.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

Bidang berikut di keluaran menunjukkan bahwa instans diaktifkan untuk hibernasi.

```
"HibernationOptions": {
    "Configured": true
}
```

PowerShell

Untuk melihat apakah instans diaktifkan untuk hibernasi

Gunakan Get-EC2Instancecmdlet dan filter instance yang diaktifkan untuk hibernasi.

```
(Get-EC2Instance `
    -Filter @{Name="hibernation-options.configured"; Values="true"}).Instances
```

Nonaktifkan KASLR pada instans (khusus Ubuntu)

Untuk menjalankan hibernasi pada instans yang baru diluncurkan dengan Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver) yang dirilis dengan nomor seri 20190722.1 atau setelahnya, atau Ubuntu 20.04 LTS (Focal Fossa) yang dirilis dengan nomor seri 20210820 atau setelahnya, kami sarankan untuk menonaktifkan KASLR (Kernel Address Space Randomization). Di Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, atau Ubuntu 20.04 LTS, KASLR diaktifkan secara default.

KASLR adalah fitur keamanan kernel Linux standar yang membantu mengurangi paparan dan konsekuensi dari kerentanan akses memori yang belum ditemukan dengan mengacak nilai alamat dasar kernel. Dengan KASLR diaktifkan, ada kemungkinan bahwa instans tidak dapat dilanjutkan setelah hibernasi.

Untuk mempelajari selengkapnya tentang KASLR, lihat Fitur Ubuntu.

Untuk menonaktifkan KASLR pada instans yang diluncurkan dengan Ubuntu

1. Hubungkan ke instans Anda menggunakan SSH. Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..
2. Buka file `/etc/default/grub.d/50-cloudimg-settings.cfg` dengan editor pilihan Anda. Edit baris `GRUB_CMDLINE_LINUX_DEFAULT` untuk menambahkan opsi `nokaslr` ke akhirnya, seperti yang ditunjukkan pada contoh berikut.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295 nokaslr"
```

3. Simpan file dan keluar dari editor Anda.
4. Jalankan perintah berikut untuk membangun ulang konfigurasi grub.

```
sudo update-grub
```

5. Boot ulang instans.

```
sudo reboot
```

6. Jalankan perintah berikut untuk mengonfirmasi bahwa `nokaslr` telah ditambahkan.

```
cat /proc/cmdline
```

Output dari perintah harus menyertakan opsi `nokaslr`.

Hibernasi instans Amazon EC2

Anda dapat memulai hibernasi pada instans Sesuai Permintaan atau instans Spot jika instans tersebut merupakan instans yang didukung EBS, diaktifkan untuk hibernasi, dan memenuhi prasyarat hibernasi. Jika sebuah instans tidak berhasil melakukan hibernasi, pematian normal akan terjadi.

Console

Untuk menghibernasi instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih sebuah instans, dan pilih instans state, Hibernate instans. Jika instans Hibernasi dinonaktifkan, instans tersebut sudah hibernasi atau dihentikan, atau tidak dapat dihibernasi. Untuk informasi selengkapnya, lihat Prasyarat untuk hibernasi instans EC2.
4. Ketika diminta konfirmasi, pilih Hibernasi. Perlu waktu beberapa menit agar instans mengalami hibernasi. Status instans pertama berubah menjadi Berhenti, lalu berubah menjadi Berhenti saat instans telah hibernasi.

AWS CLI

Untuk menghibernasi instans

Gunakan perintah stop-instances dan tentukan parameter `--hibernate`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

Untuk menghibernasi instans

Gunakan Stop-EC2Instancecmdlet.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Anda dapat memeriksa apakah hibernasi dimulai pada sebuah instance.

Console

Untuk melihat apakah hibernasi dimulai pada sebuah instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans dan, pada tab Detail, di bagian Detail instans, periksa nilai untuk Pesan transisi status.

   Klien. UserInitiatedHibernate: Hibernasi yang dimulai pengguna menunjukkan bahwa Anda memulai hibernasi pada Instans Sesuai Permintaan atau Instans Spot.

AWS CLI

Untuk melihat apakah hibernasi dimulai pada sebuah instans

Gunakan perintah describe-instances dan tentukan filter `state-reason-code` untuk melihat instans tempat hibernasi diinisiasi.

```
aws ec2 describe-instances \
```

```
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

Bidang berikut di keluaran menunjukkan bahwa hibernasi telah dimulai pada Instans Sesuai Permintaan atau Instans Spot.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Untuk melihat apakah hibernasi dimulai pada sebuah instans

Gunakan Get-EC2Instancecmdlet dan tentukan `state-reason-code` filter untuk melihat contoh di mana hibernasi dimulai.

```
Get-EC2Instance `
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

Memulai instans Amazon EC2 yang hibernasi

Mulai instans hibernasi dengan memulainya dengan cara yang sama seperti Anda memulai instans yang dihentikan.

Untuk Instans Spot, jika Amazon EC2 melakukan hibernasi instans, maka hanya Amazon EC2 yang dapat melanjutkannya. Anda hanya dapat melanjutkan Instans Spot yang hibernasi jika Anda menghibernasinya. Instans Spot hanya dapat dilanjutkan jika kapasitas tersedia dan harga Spot kurang dari atau sama dengan harga maksimum yang Anda tentukan.

Console

Untuk memulai instans yang dihibernasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans hibernasi, dan pilih Status instans, Mulai instans. Hal ini diperlukan waktu beberapa menit hingga instans memasuki status `running`. Selama waktu ini, pemeriksaan status instans menunjukkan instans dalam status gagal sampai instans dimulai.

AWS CLI

Untuk memulai instans yang dihibernasi

Gunakan perintah start-instances.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk memulai instans yang dihibernasi

Gunakan Start-EC2Instancecmdlet.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Memecahkan masalah hibernasi instans Amazon EC2

Gunakan informasi ini untuk membantu mendiagnosis dan memperbaiki masalah yang mungkin Anda temui saat menghibernasi sebuah instans.

Masalah hibernasi

- Tidak dapat berhibernasi segera setelah peluncuran
- Terlalu lama untuk transisi dari stopping ke stopped, dan status memori tidak dipulihkan setelah dimulai
- Contoh “macet” di stopping negara bagian
- Tidak dapat memulai Instans Spot segera setelah hibernasi
- Gagal melanjutkan Instans Spot

Tidak dapat berhibernasi segera setelah peluncuran

Jika Anda mencoba untuk menghibernasi sebuah instans terlalu cepat setelah Anda meluncurkannya, Anda mendapatkan pesan kesalahan.

Anda harus menunggu sekitar dua menit untuk instance Linux dan sekitar lima menit untuk instance Windows setelah peluncuran sebelum hibernasi.

Terlalu lama untuk transisi dari stopping ke stopped, dan status memori tidak dipulihkan setelah dimulai

Jika instans hibernasi Anda memerlukan waktu lama untuk bertransisi dari status `stopping` ke `stopped`, dan jika status memori tidak dipulihkan setelah Anda memulainya, ini mungkin menunjukkan bahwa hibernasi tidak dikonfigurasi dengan benar.

Contoh Linux

Periksa log sistem instans dan cari pesan yang terkait dengan hibernasi. Untuk mengakses log sistem, sambungkan ke instance atau gunakan get-console-outputperintah. Menemukan baris log dari `hibinit-agent`. Jika garis log menunjukkan kegagalan atau garis log hilang, kemungkinan besar ada kegagalan dalam mengonfigurasi hibernasi saat peluncuran.

Misalnya, pesan berikut menunjukkan bahwa volume root instans tidak cukup besar: `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Jika baris log terakhir dari `hibinit-agent` adalah `hibinit-agent: Running: swapoff / swap`, hibernasi berhasil dikonfigurasi.

Jika Anda tidak melihat log apa pun dari proses ini, AMI Anda mungkin tidak mendukung hibernasi. Untuk informasi tentang dukungan AMIs, lihatPrasyarat untuk hibernasi instans EC2. Jika Anda menggunakan AMI Linux Anda sendiri, pastikan Anda mengikuti instruksi untukKonfigurasikan AMI Linux untuk mendukung hibernasi.

Windows Server 2016 dan setelahnya

Periksa log peluncuran EC2 dan cari pesan yang terkait dengan hibernasi. Untuk mengakses log peluncuran EC2, hubungkan ke instans dan buka file `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` di editor teks. Jika Anda menggunakan EC2 Launch v2, buka`C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Secara default, Windows menyembunyikan file dan folder di bawah `C:\ProgramData`. Untuk melihat direktori dan file EC2Launch, masukkan jalur di Windows Explorer atau ubah properti folder untuk menampilkan file dan folder tersembunyi.

Temukan garis log untuk hibernasi. Jika garis log menunjukkan kegagalan atau garis log hilang, kemungkinan besar ada kegagalan dalam mengonfigurasi hibernasi saat peluncuran.

Misalnya, pesan berikut menunjukkan bahwa hibernasi gagal dikonfigurasi: `Message: Failed to enable hibernation.` Jika pesan kesalahan tersebut menyertakan nilai ASCII desimal, Anda dapat mengonversi nilai ASCII menjadi teks biasa untuk membaca pesan kesalahan lengkap.

Jika baris log berisi `HibernationEnabled: true`, hibernasi berhasil dikonfigurasi.

Windows Server 2012 R2 dan sebelumnya

Periksa log konfigurasi EC2 dan cari pesan yang terkait dengan hibernasi. Untuk mengakses log konfigurasi EC2, hubungkan ke instans dan buka file `C:\Program Files\Amazon \Ec2ConfigService\Logs\Ec2ConfigLog.txt` di editor teks. Temukan baris log untuk `SetHibernateOnSleep`. Jika baris log menunjukkan kegagalan atau baris log hilang, kemungkinan besar ada kegagalan dalam mengonfigurasi hibernasi saat peluncuran.

Misalnya, pesan berikut menunjukkan bahwa volume root instans tidak cukup besar: `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Jika baris log adalah `SetHibernateOnSleep: HibernationEnabled: true`, hibernasi berhasil dikonfigurasi.

Ukuran instans Windows

Jika Anda menggunakan instance Windows T3 atau T3a dengan RAM kurang dari 1 GiB, coba tingkatkan ukuran instans ke instans yang memiliki setidaknya 1 GiB RAM.

Contoh “macet” di stopping negara bagian

Jika Anda menghibernasi instans Anda dan instans tersebut tampak "macet" di status `stopping`, Anda dapat menghentikannya secara paksa. Untuk informasi selengkapnya, lihat Memecahkan masalah penghentian EC2 instans Amazon.

Tidak dapat memulai Instans Spot segera setelah hibernasi

Jika Anda mencoba memulai instans Spot dalam waktu dua menit setelah hibernasi, Anda mungkin mendapatkan kesalahan berikut:

`You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.`

Tunggu sekitar dua menit untuk instance Linux dan sekitar lima menit untuk instance Windows dan kemudian coba lagi memulai instance.

Gagal melanjutkan Instans Spot

Jika Instans Spot berhasil dihibernasi tetapi gagal dilanjutkan, dan sebagai gantinya di-boot ulang (restart baru di mana status hibernasi tidak dipertahankan), itu mungkin karena data pengguna berisi skrip berikut:

```
/usr/bin/enable-ec2-spot-hibernation
```

Hapus skrip ini dari bidang Data pengguna di templat peluncuran, lalu minta instans Spot baru.

Perhatikan bahwa meskipun instans gagal dilanjutkan, tanpa status hibernasi yang dipertahankan, instans masih dapat dimulai dengan cara yang sama seperti memulai dari status. `stopped`

Nyalakan ulang EC2 instans Amazon Anda

Sebuah instans yang melakukan boot ulang setara dengan penyalaan ulang sistem operasi. Dalam kebanyakan kasus, hanya diperlukan beberapa menit untuk melakukan boot ulang instans Anda.

Saat Anda melakukan boot ulang sebuah instans, hal-hal berikut akan tetap:

- Nama DNS publik () IPv4
- IPv4 Alamat pribadi
- IPv4 Alamat publik
- IPv6 alamat (jika ada)
- Setiap data pada volume penyimpanan instansnya

Mem-boot ulang instans tidak memulai periode penagihan instans baru, tidak seperti menghentikan dan memulai instance (yang memulai periode penagihan baru dengan biaya minimum satu menit).

Reboot instance dapat dimulai oleh pengguna (di mana Anda me-reboot instance secara manual) atau dimulai oleh AWS (untuk pemulihan instans otomatis, atau sebagai respons terhadap peristiwa reboot terjadwal untuk pemeliharaan yang diperlukan, seperti menerapkan pembaruan yang memerlukan reboot).

Untuk reboot yang dimulai pengguna, sebaiknya gunakan konsol Amazon EC2 , CLI, atau API alih-alih menjalankan perintah reboot sistem operasi dari instance Anda. Saat menggunakan Amazon

EC2, jika instance tidak dimatikan dengan bersih dalam beberapa menit, Amazon EC2 melakukan hard reboot. Selanjutnya, AWS CloudTrail buat catatan API saat instance Anda di-boot ulang.

Topik ini menjelaskan cara melakukan reboot yang dimulai pengguna. Untuk informasi tentang reboot yang dilakukan oleh AWS, lihat Pemulihan instans otomatis danKelola instans Amazon EC2 yang dijadwalkan untuk reboot.

> **Important**
>
> Jika pembaruan diinstal pada instans Anda, kami sarankan Anda tidak mem-boot ulang atau mematikan instance Anda menggunakan EC2 konsol Amazon atau baris perintah sampai semua pembaruan diinstal. Saat Anda menggunakan EC2 konsol Amazon atau baris perintah untuk me-reboot atau mematikan instance Anda, ada risiko instans Anda akan sulit di-boot ulang. Boot ulang paksa saat pembaruan sedang diinstal dapat membuat instans Anda menjadi tidak stabil.

Console

Untuk melakukan boot ulang instans

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih instans dan pilih instans state, Reboot instans.
4. Pilih Boot ulang ketika diminta untuk konfirmasi.

   Instans tetap dalam status `running`.

AWS CLI

Untuk melakukan boot ulang instans

Gunakan perintah reboot-instance.

```
aws ec2 reboot-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk melakukan boot ulang instans

Gunakan Restart-EC2Instancecmdlet.

```
Restart-EC2Instance -InstanceId i-1234567890abcdef0
```

Untuk menjalankan eksperimen injeksi kesalahan terkontrol

Anda dapat menggunakan AWS Fault Injection Service untuk menguji bagaimana aplikasi Anda merespons ketika instance Anda di-boot ulang. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Fault Injection Service.

Mengakhiri instans Amazon EC2

> **Warning**
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
> Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Anda dapat menghapus instans Anda saat tidak lagi membutuhkannya. Hal ini disebut sebagai mengakhiri instans Anda. Segera setelah status instans berubah menjadi `shutting-down` atau `terminated`, Anda tidak lagi dikenai biaya untuk instans itu.

Anda tidak dapat terhubung ke atau memulai sebuah instans setelah mengakhirinya. Namun, Anda dapat meluncurkan instance baru menggunakan AMI yang sama.

Jika Anda lebih suka menghentikan atau hibernasi instance Anda, lihat Hentikan dan mulai instans Amazon EC2 atau. Hibernasi instans Amazon EC2 Anda Untuk informasi selengkapnya, lihat Perbedaan antara status instance.

Daftar Isi

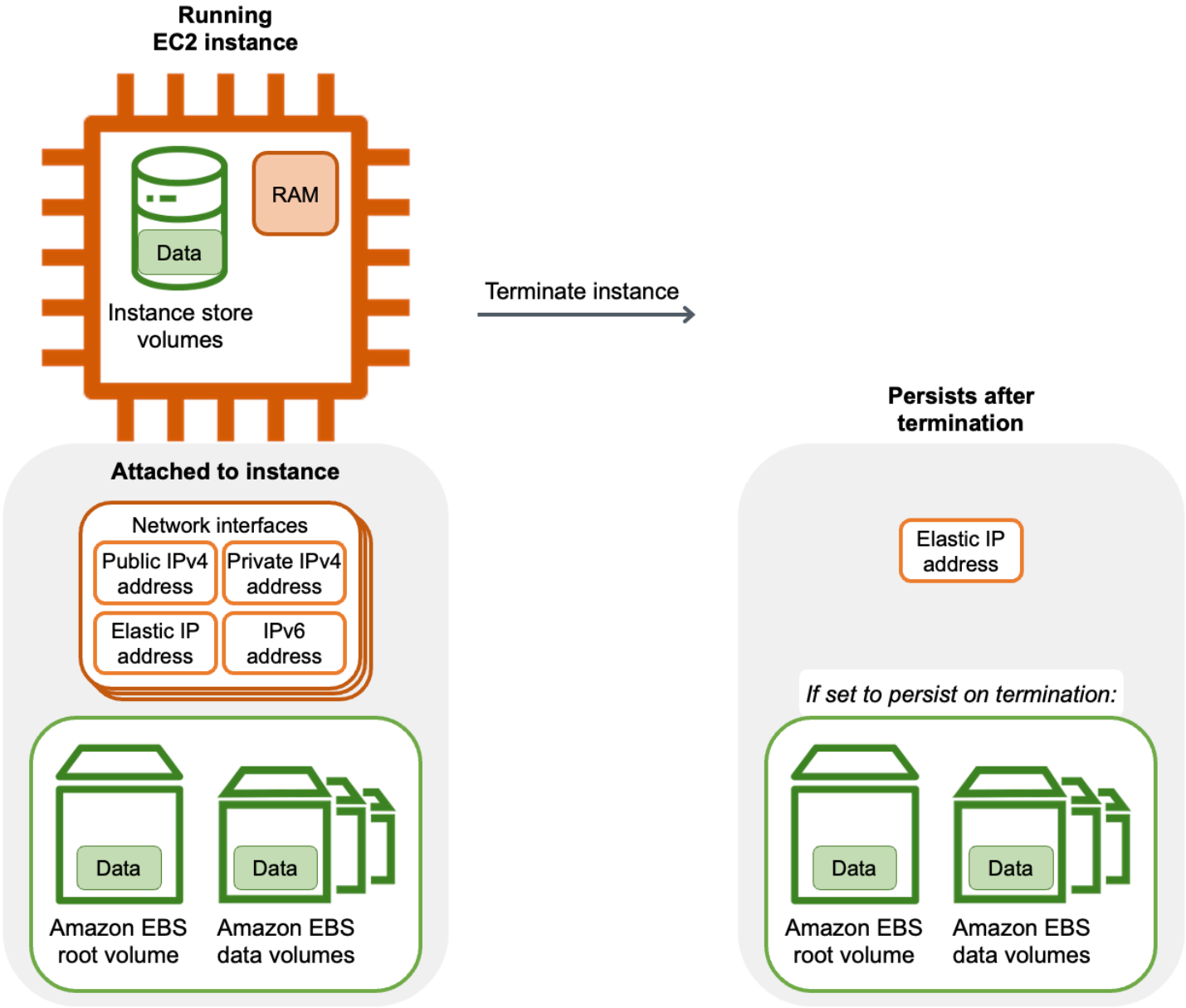
- Cara kerja penghentian instance

- Metode untuk mengakhiri sebuah instance
- Mengakhiri instance dengan shutdown OS yang anggun
- Hentikan instance dan lewati shutdown OS yang anggun
- Memecahkan masalah pengakhiran instans
- Ubah perlindungan penghentian instance
- Ubah perilaku shutdown yang dimulai instance
- Pertahankan data saat instans diakhiri

Cara kerja penghentian instance

Ketika Anda menghentikan sebuah instance, perubahan terdaftar pada tingkat sistem operasi (OS) instans, beberapa sumber daya hilang, dan beberapa sumber daya tetap ada.

Diagram berikut menunjukkan apa yang hilang dan apa yang bertahan ketika instans Amazon EC2 dihentikan. Ketika sebuah instance berakhir, data pada volume penyimpanan instans apa pun dan data yang disimpan dalam RAM instance dihapus. Alamat IP Elastis apa pun yang terkait dengan instance terlepas. Untuk volume root Amazon EBS dan volume data, hasilnya bergantung pada pengaturan Hapus pada penghentian setiap volume.



Pertimbangan-pertimbangan

- Ketekunan data
  - Volume penyimpanan instans: Semua data dihapus secara permanen saat instance berakhir.
  - Volume akar EBS:
    - Saat dilampirkan saat peluncuran, dihapus secara default saat instance berakhir.
    - Saat dilampirkan setelah peluncuran, tetap secara default saat instance berakhir.
  - Volume data EBS:

  - Saat dilampirkan saat peluncuran menggunakan konsol: Bertahan secara default saat instance berakhir.
  - Saat dilampirkan saat peluncuran menggunakan CLI: Dihapus secara default saat instance berakhir.
  - Saat dilampirkan setelah peluncuran menggunakan konsol atau CLI: Bertahan secara default saat instance berakhir.

> **Note**
>
> Setiap volume yang tidak dihapus pada penghentian instans terus dikenakan biaya. Anda dapat mengubah pengaturan sehingga volume dihapus atau tetap pada penghentian instans. Untuk informasi selengkapnya, lihat Pertahankan data saat instans diakhiri.

- Perlindungan terhadap penghentian yang tidak disengaja
  - Untuk mencegah instance dihentikan secara tidak sengaja oleh seseorang, aktifkan perlindungan penghentian.
  - Untuk mengontrol apakah instance berhenti atau berakhir saat shutdown dimulai dari instance, ubah perilaku shutdown yang dimulai instance.
- Skrip shutdown — Jika Anda menjalankan skrip pada penghentian instans, instans Anda mungkin mengalami penghentian abnormal karena kami tidak memiliki cara untuk memastikan bahwa skrip shutdown berjalan. Amazon EC2 mencoba mematikan instance dengan bersih dan menjalankan skrip shutdown sistem apa pun; namun, peristiwa tertentu (seperti kegagalan perangkat keras) dapat mencegah skrip shutdown sistem ini berjalan.
- Instans bare metal — instans bare metal x86 tidak mendukung shutdown kooperatif.

Hal yang terjadi ketika Anda mengakhiri sebuah instans

Perubahan terdaftar di tingkat OS

- Permintaan API akan mengirimkan peristiwa penekanan tombol kepada tamu.
- Berbagai layanan sistem dihentikan sebagai akibat dari peristiwa penekanan tombol. Shutdown sistem yang anggun disediakan oleh systemd (Linux) atau proses Sistem (Windows). Pematian yang tertib dipicu oleh peristiwa penekanan tombol pematian ACPI dari hypervisor.
- Pematian ACPI dimulai.

- Instance dimatikan setelah proses shutdown yang anggun keluar. Tidak ada waktu pematian OS yang dapat dikonfigurasi. Instans akan tetap terlihat di konsol untuk beberapa saat, kemudian entri tersebut akan dihapus secara otomatis.

Sumber daya hilang

- Data disimpan di volume penyimpanan instans.
- Volume root EBS jika `DeleteOnTermination` atribut diatur ke`true`.
- Volume data EBS (dilampirkan saat peluncuran atau setelah) jika `DeleteOnTermination` atribut disetel ke`true`.

Sumber daya yang bertahan

- Volume root EBS jika `DeleteOnTermination` atribut diatur ke`false`.
- Volume data EBS (dilampirkan saat peluncuran atau setelah) jika `DeleteOnTermination` atribut disetel ke`false`.

Uji respons aplikasi terhadap pengakhiran instans

Anda dapat menggunakan AWS Fault Injection Service untuk menguji bagaimana aplikasi Anda merespons ketika instance Anda dihentikan. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Fault Injection Service.

Metode untuk mengakhiri sebuah instance

> **Warning**
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen.
> Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
> Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Ada empat cara untuk melakukan terminasi instance yang dimulai pengguna: default terminate, terminate with skip OS shutdown, force terminate, dan force terminate dengan skip OS shutdown. Tabel berikut membandingkan perbedaan utama antara metode terminasi:

> **Note**
>
> Anda tidak dapat menghentikan instance jika perlindungan terminasi diaktifkan. Untuk informasi selengkapnya, lihat Mengubah perlindungan penghentian instans.

Metode penghentian	Tujuan utama	Kasus penggunaan	Perintah CLI
Mengakhiri default	Penonaktifan instance normal dengan upaya shutdown OS yang anggun.	Pengakhiran contoh tipikal.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0`
Hentikan dengan lewati shutdown OS	Melewati shutdown OS yang anggun saat mengakhiri sebuah instance.	Saat melewati shutdown OS yang anggun diperlukan.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --skip-os-shutdown`
Paksa mengakhiri	Menangani instance yang macet. Mencoba penghentian default terlebih dahulu; jika instance gagal untuk mengakhiri, maka secara paksa mengakhiri instance.	Ketika instance macet dalam `shutting-down` keadaan.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \`

Metode penghentian	Tujuan utama	Kasus penggunaan	Perintah CLI
			`--force`
Paksa terminate dengan skip OS shutdown	Force mengakhiri dan melewati shutdown OS yang anggun saat mengakhiri sebuah instance.	Ketika penghentian paksa dan melewati shutdown OS yang anggun diperlukan.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --force \ --skip-os-shutdown`

Untuk petunjuk tentang cara menggunakan setiap metode, lihat berikut ini:

- Mengakhiri instance dengan shutdown OS yang anggun
- Hentikan instance dan lewati shutdown OS yang anggun
- Paksa menghentikan sebuah instance

Mengakhiri instance dengan shutdown OS yang anggun

Anda dapat menghentikan instance menggunakan metode terminate default, yang mencakup upaya shutdown OS yang anggun. Untuk informasi selengkapnya, lihat Metode untuk mengakhiri sebuah instance.

Console

Untuk mengakhiri sebuah instance menggunakan metode terminate default

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance, dan pilih Instance state, Terminate (delete) instance.
4. Pilih Hentikan (hapus) saat diminta konfirmasi.

5. Setelah Anda menghentikan sebuah instance, instans tetap terlihat untuk sementara waktu, dengan status. `terminated`

   Jika penghentian gagal atau jika instance yang dihentikan terlihat selama lebih dari beberapa jam, lihatInstans yang dihentikan masih ditampilkan.

AWS CLI

Untuk mengakhiri sebuah instance menggunakan metode terminate default

Gunakan perintah terminate-instance.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk mengakhiri sebuah instance menggunakan metode terminate default

Gunakan Remove-EC2Instancecmdlet.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Hentikan instance dan lewati shutdown OS yang anggun

Anda dapat melewati shutdown OS yang anggun saat mengakhiri sebuah instance. Untuk informasi selengkapnya, lihat Metode untuk mengakhiri sebuah instance.

Console

Untuk menghentikan instance dan melewati shutdown OS yang anggun

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance, dan pilih Instance state, Terminate (delete) instance.
4. Di bawah Lewati shutdown OS, pilih kotak centang Lewati OS shutdown. Jika Anda tidak melihat opsi ini di konsol, opsi ini belum tersedia di konsol di Wilayah saat ini. Namun, Anda dapat mengakses fitur ini menggunakan AWS CLI atau SDK, atau mencoba Wilayah lain di konsol.
5. Pilih Hentikan (hapus).

6. Setelah Anda menghentikan sebuah instance, instans tetap terlihat untuk sementara waktu, dengan status. `terminated`

   Jika penghentian gagal atau jika instance yang dihentikan terlihat selama lebih dari beberapa jam, lihatInstans yang dihentikan masih ditampilkan.

AWS CLI

Untuk menghentikan instance dan melewati shutdown OS yang anggun

Gunakan perintah terminate-instance dengan.. `--skip-os-shutdown`

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --skip-os-shutdown
```

PowerShell

Untuk menghentikan instance dan melewati shutdown OS yang anggun

Gunakan Remove-EC2Instancecmdlet dengan.. `-SkipOsShutdown $true`

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -SkipOsShutdown $true
```

Memecahkan masalah pengakhiran instans

Pemohon harus memiliki izin untuk meneleponec2:TerminateInstances. Untuk informasi selengkapnya, lihat Contoh kebijakan untuk bekerja dengan instance.

Jika Anda mengakhiri instans Anda dan instans lain dimulai, kemungkinan besar Anda telah mengonfigurasi penskalaan otomatis melalui fitur seperti Armada EC2 atau Amazon EC2 Auto Scaling. Untuk informasi selengkapnya, lihat Instans diluncurkan atau dihentikan secara otomatis.

> **Note**
>
> Anda tidak dapat menghentikan instance jika perlindungan terminasi diaktifkan. Untuk informasi selengkapnya, lihat Mengubah perlindungan penghentian instans.

Jika instans Anda berada dalam `shutting-down` status lebih lama dari biasanya, Anda dapat mencoba untuk menghentikannya secara paksa. Jika tetap dalam `shutting-down` keadaan, itu harus dibersihkan (dihentikan) oleh proses otomatis dalam layanan Amazon EC2. Untuk informasi selengkapnya, lihat Penghentian instans yang tertunda.

Ubah perlindungan penghentian instance

Untuk mencegah instans Anda dihentikan secara tidak sengaja menggunakan Amazon EC2 API, baik Anda `TerminateInstances` menelepon secara langsung atau menggunakan antarmuka lain seperti konsol Amazon EC2, aktifkan perlindungan penghentian untuk instans. `DisableApiTermination`Atribut mengontrol apakah instance dapat dihentikan. Secara default, perlindungan pengakhiran dinonaktifkan untuk instans Anda. Anda dapat mengatur nilai atribut ini saat meluncurkan instance, atau saat instance sedang berjalan atau dihentikan.

`DisableApiTermination`Atribut tidak mencegah Anda menghentikan instance dengan memulai shutdown dari instance (misalnya, dengan menggunakan perintah sistem operasi untuk shutdown sistem) ketika `InstanceInitiatedShutdownBehavior` atribut disetel ke. `terminate` Untuk informasi selengkapnya, lihat Ubah perilaku shutdown yang dimulai instance.

Pertimbangan

- Mengaktifkan perlindungan terminasi tidak AWS mencegah penghentian instance ketika ada acara terjadwal untuk menghentikan instance.
- Mengaktifkan perlindungan pengakhiran tidak mencegah Amazon EC2 Auto Scaling untuk mengakhiri instans saat instans tidak dalam kondisi baik atau selama peristiwa penskalaan ke dalam. Anda dapat mengontrol apakah grup Auto Scaling dapat mengakhiri instans tertentu saat menskalakan menggunakan perlindungan penskalaan ke dalam instans. Anda dapat mengontrol apakah grup Auto Scaling dapat mengakhiri instans yang tidak sehat dengan menangguhkan proses penskalaan ReplaceUnhealthy.
- Anda tidak dapat mengaktifkan perlindungan pengakhiran untuk Instans Spot.

Console

Untuk mengaktifkan perlindungan terminasi untuk sebuah instans saat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada dasbor, pilih Luncurkan instans.
3. Perluas Detail lanjutan. Untuk perlindungan Terminasi, pilih Aktifkan.

4. Saat Anda selesai menentukan detail untuk instance Anda, pilih Launch instance.

Untuk mengubah perlindungan terminasi untuk sebuah instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pilih Tindakan, Pengaturan instans, Ubah perlindungan penghentian.
5. Untuk perlindungan Terminasi pilih atau hapus Aktifkan.
6. Pilih Simpan.

AWS CLI

Untuk mengaktifkan perlindungan terminasi untuk sebuah instance

Gunakan perintah modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-termination
```

Untuk menonaktifkan perlindungan terminasi untuk sebuah instance

Gunakan perintah modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-termination
```

PowerShell

Untuk mengaktifkan perlindungan terminasi untuk sebuah instance

Gunakan Edit-EC2InstanceAttributecmdlet.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiTermination $true
```

Untuk menonaktifkan perlindungan terminasi untuk sebuah instance

Gunakan Edit-EC2InstanceAttributecmdlet.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiTermination $false
```

Mengakhiri beberapa instans dengan perlindungan terminasi

Jika Anda menghentikan beberapa instans di beberapa Availability Zone dalam permintaan yang sama, dan satu atau beberapa instance yang ditentukan diaktifkan untuk perlindungan penghentian, permintaan akan gagal dengan hasil berikut:

- Instans yang ditentukan yang berada dalam Zona Ketersediaan yang sama dengan instans yang dilindungi tidak diakhiri.
- Instans yang ditentukan yang berada di Zona Ketersediaan yang berbeda, di mana tidak ada instans yang ditentukan lainnya yang dilindungi, berhasil diakhiri.

Contoh

Misalkan Anda memiliki empat contoh berikut di dua Availability Zone.

Instans	Zona Ketersediaan	Perlindungan pengakhiran
Contoh 1	AZ	`Disabled`
Contoh 2		`Disabled`
Contoh 3	AZ B	`Enabled`
Contoh 4		`Disabled`

Jika Anda mencoba untuk mengakhiri semua instans ini dalam permintaan yang sama, maka permintaan tersebut akan melaporkan kegagalan dengan hasil sebagai berikut:

- Instance 1 dan Instance 2 berhasil dihentikan karena tidak ada instance yang diaktifkan untuk perlindungan terminasi.

- Instance 3 dan Instance 4 gagal dihentikan karena Instance 3 diaktifkan untuk perlindungan terminasi.

Ubah perilaku shutdown yang dimulai instance

> **Warning**
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen.
> Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
> Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Saat Anda memulai pematian dari instans yang didukung Amazon EBS (menggunakan perintah seperti shutdown atau poweroff), instans akan berhenti secara default. Anda dapat mengubah perilaku ini sehingga instans berakhir dengan mengubah atribut `InstanceInitiatedShutdownBehavior` untuk instans. Anda dapat mengubah atribut ini saat instans sedang berjalan atau berhenti.

Perintah halt tidak memulai pematian. Jika digunakan, instans tidak diakhiri. Sebaliknya, instans menempatkan CPU ke `HLT` dan instans tersebut tetap berjalan.

> **Note**
>
> Atribut `InstanceInitiatedShutdownBehavior` hanya berlaku ketika Anda melakukan pematian dari sistem operasi instans itu sendiri. Ini tidak berlaku saat Anda menghentikan instans menggunakan API `StopInstances` atau konsol Amazon EC2.

Console

Untuk mengubah perilaku pematian yang dinisiasi instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pilih Tindakan, Pengaturan instans, Ubah perilaku pematian.

   Perilaku pematian menampilkan perilaku saat ini.
5. Untuk mengubah perilaku, pada Perilaku pematian, pilih Hentikan atau Akhiri.
6. Pilih Simpan.

AWS CLI

Untuk mengubah perilaku pematian yang dinisiasi instans

Gunakan perintah modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --instance-initiated-shutdown-behavior terminate
```

PowerShell

Untuk mengubah perilaku pematian yang dinisiasi instans

Gunakan Edit-EC2InstanceAttributecmdlet.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -InstanceInitiatedShutdownBehavior terminate
```

Pertahankan data saat instans diakhiri

Saat instans Amazon EC2 dihentikan, Anda dapat menyimpan data pada volume penyimpanan instans atau volume Amazon EBS. Topik ini menjelaskan cara memastikan data Anda tetap ada setelah penghentian instans.

Bagaimana penghentian instance memengaruhi volume root dan data

Volume penyimpanan instans

Ketika sebuah instance dihentikan, volume penyimpanan instance secara otomatis dihapus dan data hilang. Untuk menyimpan data ini di luar masa pakai instans, sebelum menghentikan instans, salin data secara manual ke penyimpanan persisten, seperti volume Amazon EBS, bucket Amazon S3, atau sistem file Amazon EFS. Untuk informasi selengkapnya, lihat Opsi penyimpanan untuk EC2 instans Amazon Anda.

Volume Amazon EBS

Ketika sebuah instance dihentikan, volume EBS akan dihapus atau dipertahankan, tergantung pada nilai `DeleteOnTermination` atribut untuk setiap volume:

- Ya (konsol)/`true`(CLI) - Volume dihapus saat instance dihentikan.
- No (console)/`false`(CLI) - Volume dipertahankan saat instance dihentikan. Volume yang diawetkan terus dikenakan biaya.

> **Note**
>
> Setelah instance berakhir, Anda dapat mengambil snapshot dari volume yang diawetkan atau melampirkannya ke instance lain. Untuk menghindari biaya yang dikenakan, Anda harus menghapus volume.

Perilaku penghapusan default untuk volume EBS

`DeleteOnTermination`Nilai default berbeda tergantung pada jenis volume, apakah volume dilampirkan saat peluncuran atau sesudahnya, dan metode (konsol atau CLI) yang digunakan untuk melampirkan volume:

Tipe volume	Terlampir saat	Metode untuk melampirkan	Perilaku default pada penghentian instance
Volume root	Saat peluncuran	Konsol atau CLI	Delete
Volume root	Setelah peluncuran	Konsol atau CLI	Pertahankan
Volume data	Saat peluncuran	Konsol	Pertahankan
Volume data	Saat peluncuran	CLI	Delete

Tipe volume	Terlampir saat	Metode untuk melampirkan	Perilaku default pada penghentian instance
Volume data	Setelah peluncuran	Konsol dan CLI	Pertahankan

Periksa pengaturan persistensi volume

Nilai default saat peluncuran untuk volume EBS ditentukan oleh `DeleteOnTermination` atribut yang ditetapkan pada AMI. Anda dapat mengubah nilai saat peluncuran instance, mengesampingkan setelan AMI. Kami menyarankan Anda memverifikasi pengaturan default untuk `DeleteOnTermination` atribut setelah Anda meluncurkan instance.

Untuk memeriksa apakah volume Amazon EBS akan dihapus saat penghentian instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pilih tab Penyimpanan.
5. Di bawah Blokir perangkat, gulir ke kanan untuk memeriksa kolom Hapus pada penghentian.
   - Jika Ya, volume akan dihapus saat instance dihentikan.
   - Jika Tidak, volume tidak akan dihapus ketika instance dihentikan. Setiap volume yang tidak dihapus terus dikenakan biaya.

Ubah volume root untuk bertahan saat peluncuran

Anda dapat mengubah `DeleteOnTermination` atribut volume root EBS saat meluncurkan instance. Anda juga dapat menggunakan prosedur berikut untuk volume data.

Console

Untuk mengubah volume root dari sebuah instance agar tetap ada saat peluncuran

1. Ikuti prosedur untuk meluncurkan instans, tetapi jangan meluncurkan instans sampai Anda menyelesaikan langkah-langkah berikut guna mengubah volume root agar tetap ada.
2. Pada panel Configure storage, pilih Advanced.
3. Di bawah volume EBS, perluas informasi volume root.

4. Untuk Hapus saat pengakhiran, pilih Tidak.
5. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

AWS CLI

Untuk mengubah volume root dari sebuah instance agar tetap ada saat peluncuran

Gunakan perintah run-instance untuk mengubah nilai `DeleteOnTermination` dalam pemetaan perangkat blok.

Tambahkan `--block-device-mappings` opsi:

```
--block-device-mappings file://mapping.json
```

Dalam `mapping.json`, tentukan nama perangkat, misalnya `/dev/sda1` atau `/dev/xvda`, dan untuk `DeleteOnTermination`, tentukan `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

Untuk mengubah volume root dari sebuah instance agar tetap ada saat peluncuran

Gunakan New-EC2Instancecmdlet untuk mengubah nilai `DeleteOnTermination` dalam pemetaan perangkat blok.

Tambahkan `-BlockDeviceMapping` opsi:

```
-BlockDeviceMapping $bdm
```

Dalam `bdm`, tentukan nama perangkat, misalnya `/dev/sda1` atau `/dev/xvda`, dan untuk `DeleteOnTermination`, tentukan `false`.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Ubah volume root dari instance yang sedang berjalan untuk bertahan

Anda dapat mengubah volume root EBS dari instance yang sedang berjalan menjadi bertahan. Anda juga dapat menggunakan prosedur berikut untuk volume data.

AWS CLI

Untuk mengubah volume root untuk bertahan

Gunakan perintah modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0  \
    --block-device-mappings file://mapping.json
```

Dalam `mapping.json`, tentukan nama perangkat, misalnya `/dev/sda1` atau `/dev/xvda`, dan untuk `--DeleteOnTermination`, tentukan `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

Untuk mengubah volume root untuk bertahan

Gunakan Edit-EC2InstanceAttributecmdlet.

Tambahkan `-BlockDeviceMapping` opsi:

```
-BlockDeviceMapping $bdm
```

Dalam `bdm`, tentukan nama perangkat, misalnya `/dev/sda1` atau `/dev/xvda`, dan untuk `DeleteOnTermination`, tentukan `false`.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Pensiun instans

Sebuah instance dijadwalkan untuk dihentikan ketika AWS mendeteksi kegagalan yang tidak dapat diperbaiki dari perangkat keras yang mendasari yang menjadi tuan rumah instance. Jenis volume root instance menentukan perilaku pensiun instance:

- Jika volume root instans Anda adalah volume Amazon EBS, instans dihentikan, dan Anda dapat memulainya lagi kapan saja. Memulai instans yang dihentikan, migrasikan ke perangkat keras baru.
- Jika volume root instance Anda adalah volume penyimpanan instance, instance akan dihentikan, dan tidak dapat digunakan lagi.

Untuk informasi selengkapnya tentang tipe peristiwa instans, lihat Acara terjadwal untuk instans Amazon EC2.

Daftar Isi

- Identifikasi instans yang dijadwalkan untuk pensiun
- Tindakan yang harus diambil untuk instans yang didukung EBS yang dijadwalkan untuk pensiun
- Tindakan yang harus diambil untuk instans yang didukung penyimpanan instans yang dijadwalkan untuk pensiun

Identifikasi instans yang dijadwalkan untuk pensiun

Jika instans Anda dijadwalkan untuk pensiun, Anda akan menerima email sebelum peristiwa itu disertai dengan ID instans dan tanggal pensiun. Anda juga dapat memeriksa contoh yang dijadwalkan untuk pensiun.

> **Important**
>
> Jika sebuah instans dijadwalkan untuk pensiun, kami sarankan Anda mengambil tindakan sesegera mungkin, karena instans mungkin sudah tidak dapat dijangkau. Untuk informasi selengkapnya, lihat Check if your instance is reachable.

Opsi untuk mengidentifikasi contoh yang dijadwalkan untuk pensiun

- Pantau email untuk kontak akun
- Periksa instans Anda

Pantau email untuk kontak akun

Jika sebuah instance dijadwalkan untuk pensiun, kontak utama untuk akun dan kontak operasi menerima email sebelum acara. Email ini menyertakan ID instans dan tanggal pensiun terjadwal. Untuk informasi selengkapnya, lihat Memperbarui kontak utama untuk AWS akun Anda dan Memperbarui kontak alternatif untuk AWS akun Anda di Panduan AWS Account Management Referensi.

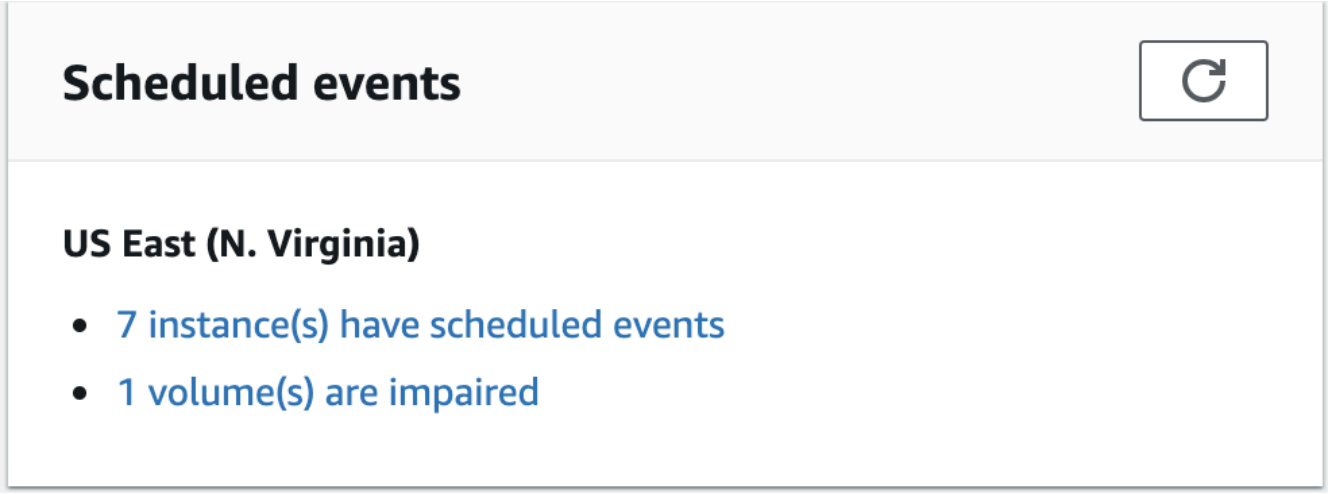
Periksa instans Anda

Jika Anda menggunakan akun email yang tidak Anda periksa secara teratur, Anda mungkin melewatkan pemberitahuan pensiun misalnya. Anda dapat memeriksa apakah salah satu contoh Anda dijadwalkan untuk pensiun kapan saja.

Console

Untuk mengidentifikasi contoh yang dijadwalkan untuk pensiun

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor EC2. Di bawah Peristiwa terjadwal, Anda dapat melihat peristiwa yang terkait dengan instans dan volume Amazon EC2 Anda, yang diatur menurut Wilayah.



3. Jika Anda memiliki instans dengan peristiwa terjadwal yang terdaftar, pilih tautannya di bawah nama Wilayah untuk membuka halaman Peristiwa.
4. Halaman Peristiwa mencantumkan semua sumber daya yang memiliki peristiwa yang terkait dengannya. Untuk melihat instans yang dijadwalkan untuk pensiun, pilih sumber daya instans dari daftar filter pertama, kemudian instans atau pensiun dari daftar filter kedua.
5. Jika hasil filter menunjukkan bahwa sebuah instans dijadwalkan untuk pensiun, pilih instans itu, dan catat tanggal serta waktu di bidang Waktu mulai di panel detail. Ini adalah tanggal pensiun instans Anda.

AWS CLI

Untuk menemukan contoh yang dijadwalkan untuk pensiun

Gunakan perintah berikut describe-instance-status. Ulangi di setiap Wilayah tempat Anda menjalankan instance.

```
aws ec2 describe-instance-status --filters Name=event.code,Values=instance-
retirement
```

PowerShell

Untuk menemukan contoh yang dijadwalkan untuk pensiun

Gunakan Get-EC2InstanceStatuscmdlet. Ulangi di setiap Wilayah tempat Anda menjalankan instance.

```
Get-EC2InstanceStatus -Filter @{Name="event.code"; Values="instance-retirement"}
```

Tindakan yang harus diambil untuk instans yang didukung EBS yang dijadwalkan untuk pensiun

Untuk menyimpan data pada instans Anda yang pensiun, Anda dapat melakukan salah satu dari tindakan berikut. Anda harus mengambil tindakan ini sebelum tanggal pensiun instans untuk mencegah waktu henti dan kehilangan data yang tidak terduga.

Untuk instance Linux, jika Anda tidak yakin apakah instans Anda didukung oleh EBS atau instans store, lihat. Volume root untuk instans Amazon EC2

Periksa apakah instans Anda dapat dijangkau

Saat Anda mendapat notifikasi bahwa instans Anda dijadwalkan untuk pensiun, kami menyarankan agar Anda mengambil tindakan berikut secepat mungkin:

- Periksa apakah instans Anda dapat dijangkau dengan menghubungkan atau melakukan ping ke instans Anda.
- Jika instans Anda dapat dijangkau, Anda harus merencanakan instans stop/start Anda pada waktu yang tepat sebelum tanggal pensiun yang dijadwalkan, ketika dampaknya minimal. Untuk informasi selengkapnya tentang menghentikan dan memulai instans Anda, dan apa yang akan terjadi saat instans Anda dihentikan, seperti efek pada alamat IP publik, privat, dan Elastis yang terkait dengan instans Anda, lihat Hentikan dan mulai instans Amazon EC2. Perhatikan bahwa data pada volume penyimpanan instans hilang saat Anda menghentikan dan memulai instans Anda.
- Jika instans Anda tidak dapat dijangkau, Anda harus segera mengambil tindakan dan melakukan penghentian/mulai untuk memulihkan instans Anda.
- Atau, jika Anda ingin mengakhiri instans Anda, rencanakan untuk melakukannya sesegera mungkin agar Anda tidak lagi dikenai biaya untuk instans tersebut.

Buat cadangan instans Anda

Buat AMI yang didukung EBS dari instans Anda sehingga Anda memiliki cadangan. Untuk memastikan integritas data, hentikan instans sebelum Anda membuat AMI. Anda dapat menunggu tanggal pensiun yang dijadwalkan saat instans dihentikan, atau hentikan sendiri instans tersebut sebelum tanggal pensiun. Anda dapat memulai kembali instans kapan saja. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.

Luncurkan instans pengganti

Setelah Anda membuat AMI dari instans, Anda dapat menggunakan AMI untuk meluncurkan instans pengganti. Dari konsol Amazon EC2, pilih AMI baru Anda, lalu pilih Launch instance dari AMI. Konfigurasikan parameter untuk instance Anda dan kemudian pilih Launch instance. Untuk informasi lebih lanjut tentang setiap bidang, lihatLuncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

Tindakan yang harus diambil untuk instans yang didukung penyimpanan instans yang dijadwalkan untuk pensiun

Untuk menyimpan data pada instans Anda yang pensiun, Anda dapat melakukan salah satu dari tindakan berikut. Anda harus mengambil tindakan ini sebelum tanggal pensiun instans untuk mencegah waktu henti dan kehilangan data yang tidak terduga.

> **Warning**
>
> Jika instans Anda memiliki volume root penyimpanan instance dan melewati tanggal pensiunnya, instans akan dihentikan dan Anda tidak dapat memulihkan instance atau data apa pun yang disimpan di dalamnya. Terlepas dari jenis volume root instance Anda, data pada volume penyimpanan instans hilang saat instance dihentikan, bahkan jika volume dilampirkan ke instance dengan volume root EBS.

Periksa apakah instans Anda dapat dijangkau

Saat Anda mendapat notifikasi bahwa instans Anda dijadwalkan untuk pensiun, kami menyarankan agar Anda mengambil tindakan berikut secepat mungkin:

- Periksa apakah instans Anda dapat dijangkau dengan menghubungkan atau melakukan ping ke instans Anda.
- Jika instans Anda tidak dapat dijangkau, kemungkinan sangat sedikit yang dapat dilakukan untuk memulihkan instans Anda. Untuk informasi lebih lanjut, lihatMemecahkan masalah instans Amazon EC2 yang tidak terjangkau. AWS akan mengakhiri instance Anda pada tanggal pensiun yang dijadwalkan, jadi, untuk contoh yang tidak terjangkau, Anda dapat segera menghentikan instance itu sendiri.

Luncurkan instans pengganti

Buat AMI yang didukung Amazon S3 dari instans Anda menggunakan alat AMI, seperti yang dijelaskan dalam. Buat AMI yang didukung Amazon S3 Dari konsol Amazon EC2, pilih AMI baru Anda, lalu pilih Launch instance dari AMI. Konfigurasikan parameter untuk instance Anda dan kemudian pilih Launch instance. Untuk informasi lebih lanjut tentang setiap bidang, lihatLuncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

Ubah instans Anda menjadi instans yang didukung EBS

Transfer data Anda ke volume EBS, ambil snapshot dari volume tersebut, lalu buat AMI dari snapshot. Anda dapat meluncurkan instans pengganti dari AMI baru Anda. Lihat informasi yang lebih lengkap di Konversikan AMI yang didukung Amazon S3 Anda ke AMI yang didukung EBS.

Pemulihan instans otomatis

> **Important**
>
> Bagian ini menjelaskan cara mengkonfigurasi mekanisme pemulihan secara proaktif pada instans EC2. Mekanisme pemulihan ini dirancang untuk mengembalikan ketersediaan instance ketika AWS mendeteksi masalah perangkat keras atau perangkat lunak yang mendasari yang menyebabkan pemeriksaan status sistem gagal. Jika saat ini Anda mengalami masalah saat mengakses instans, lihat Memecahkan masalah instans EC2.

Jika AWS mendeteksi bahwa instans tidak tersedia karena masalah perangkat keras atau perangkat lunak yang mendasarinya, ada dua mekanisme yang dapat secara otomatis memulihkan ketersediaan instans — pemulihan otomatis yang disederhanakan dan pemulihan berbasis CloudWatch tindakan Amazon. Memulihkan ketersediaan instance juga dikenal sebagai pemulihan instance.

Selama proses pemulihan instans, AWS akan mencoba memindahkan instance Anda dari host dengan masalah perangkat keras atau perangkat lunak yang mendasarinya ke host yang berbeda. Jika berhasil, proses pemulihan instance akan muncul ke instance sebagai reboot yang tidak direncanakan. Anda dapat memverifikasi apakah pemulihan instans terjadi.

Jika proses pemulihan tidak berhasil, instance mungkin terus berjalan di host dengan masalah perangkat keras atau perangkat lunak yang mendasarinya. Dalam hal ini, intervensi manual diperlukan. Jika instans menjadi tidak dapat dijangkau atau pemeriksaan status sistem terus gagal, kami sarankan Anda menghentikan dan memulai instance secara manual. Ketika Anda memulai

sebuah instance, biasanya dimigrasikan ke komputer host baru yang mendasarinya. Namun, tidak seperti pemulihan instans otomatis, di mana instance mempertahankan IPv4 alamat publiknya, instance yang dimulai ulang menerima IPv4 alamat publik baru kecuali jika memiliki alamat IP Elastis.

Untuk mendapatkan manfaat dari mekanisme pemulihan otomatis, mereka harus dikonfigurasi terlebih dahulu pada sebuah instance sebelum pemeriksaan status sistem gagal. Secara default, pemulihan otomatis yang disederhanakan diaktifkan selama peluncuran instance. Anda dapat mengonfigurasi pemulihan berbasis CloudWatch tindakan Amazon secara opsional setelah peluncuran. Memiliki salah satu mekanisme ini yang dikonfigurasi membuat instans Anda lebih tangguh.

Pemulihan otomatis yang disederhanakan dan pemulihan berbasis CloudWatch tindakan Amazon hanya tersedia pada instans yang didukung. Untuk informasi selengkapnya, lihat Persyaratan untuk mengaktifkan pemulihan otomatis yang disederhanakan dan Persyaratan untuk mengaktifkan pemulihan berbasis CloudWatch tindakan.

> **Warning**
>
> Ketika AWS memulihkan instans Anda karena masalah perangkat keras atau perangkat lunak yang mendasarinya, perhatikan konsekuensi berikut: data yang disimpan dalam memori volatil (RAM) akan hilang dan uptime sistem operasi akan dimulai dari nol. Selanjutnya, dengan pemulihan berbasis CloudWatch tindakan, data pada volume penyimpanan instance juga akan hilang. Untuk membantu melindungi dari kehilangan data, kami sarankan Anda secara teratur membuat cadangan data berharga. Untuk informasi selengkapnya tentang praktik terbaik pencadangan dan pemulihan untuk instans EC2, lihat Praktik terbaik untuk Amazon EC2.
>
> Mekanisme pemulihan instans otomatis dirancang untuk instance individual. Untuk panduan tentang membangun sistem yang tangguh, lihat. Membangun sistem yang tangguh

Topik

- Konsep kunci pemulihan instans otomatis
- Perbedaan antara pemulihan otomatis yang disederhanakan dan pemulihan berbasis CloudWatch tindakan
- Membangun sistem yang tangguh
- Verifikasi apakah pemulihan instans otomatis terjadi
- Konfigurasikan pemulihan otomatis yang disederhanakan pada instans Amazon EC2

- Konfigurasikan pemulihan berbasis CloudWatch tindakan pada instans EC2

Konsep kunci pemulihan instans otomatis

Pemulihan instans otomatis adalah fitur Amazon EC2 yang secara otomatis memulihkan ketersediaan instans saat terjadi kegagalan perangkat keras atau perangkat lunak yang mendasari, meningkatkan ketahanan dan keandalan instans EC2 Anda.

Berikut ini adalah konsep kunci dari pemulihan instans otomatis:

Opsi konfigurasi

Dua mekanisme dapat dikonfigurasi untuk mendukung pemulihan instans otomatis:

- Pemulihan otomatis yang disederhanakan: Diaktifkan secara default pada instance yang didukung.
- CloudWatch pemulihan berbasis tindakan: Memerlukan konfigurasi manual pada instance yang didukung.

Pemeriksaan status sistem

Pemeriksaan status sistem secara otomatis memantau AWS infrastruktur tempat instans EC2 Anda berjalan.

- Jika pemeriksaan status sistem gagal, AWS memulai pemulihan instans otomatis, yang mencoba memigrasikan instance yang terpengaruh ke perangkat keras yang berbeda.
- Pemeriksaan status sistem yang gagal menunjukkan masalah dengan perangkat keras atau perangkat lunak host, dan bukan masalah dengan instance itu sendiri. Pemulihan instans otomatis dapat memulihkan instance yang gagal dalam pemeriksaan status sistem. Namun, pemulihan instans otomatis tidak beroperasi jika hanya pemeriksaan status instance yang gagal.
- Untuk perbedaan antara pemeriksaan status instance dan sistem, lihat Jenis pemeriksaan status.

Contoh masalah perangkat keras atau perangkat lunak yang mendasarinya

Masalah perangkat keras atau perangkat lunak yang dapat menyebabkan pemeriksaan status sistem gagal termasuk hilangnya konektivitas jaringan, hilangnya daya sistem, masalah perangkat lunak pada host fisik, dan masalah perangkat keras pada host fisik yang memengaruhi jangkauan jaringan.

Karakteristik contoh yang dipulihkan

Sebuah instance yang dipulihkan identik dengan instance asli, kecuali untuk elemen yang hilang.

Elemen yang diawetkan:

- ID Instans
- Alamat IP publik, pribadi, dan Elastis
- Metadata instans
- Grup penempatan
- Volume EBS terlampir
- Zona Ketersediaan

Elemen yang hilang:

- Data disimpan dalam memori volatil (RAM)
- Data yang disimpan pada volume penyimpanan instance (hanya berlaku untuk pemulihan berbasis CloudWatch tindakan)
- Uptime sistem operasi disetel ulang ke nol

Memantau pemeriksaan status sistem dengan CloudWatch

Metrik StatusCheckFailed_System di CloudWatch menunjukkan apakah pemeriksaan status sistem lulus atau gagal.

Nilai metrik:

- 0 — Pemeriksaan status sistem lulus.
- 1 — Pemeriksaan status sistem gagal.

Acara di Dasbor Health

Selama upaya pemulihan instans otomatis, AWS kirimkan peristiwa ke Anda Dasbor Health berdasarkan mekanisme pemulihan yang dikonfigurasi dan hasilnya:

- Pemulihan otomatis yang disederhanakan
  - Acara sukses: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
  - Peristiwa kegagalan: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`
- CloudWatch pemulihan berbasis tindakan

- Acara sukses: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
- Peristiwa kegagalan: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Perbedaan antara pemulihan otomatis yang disederhanakan dan pemulihan berbasis CloudWatch tindakan

Tabel berikut membandingkan perbedaan utama antara pemulihan otomatis yang disederhanakan dan pemulihan berbasis CloudWatch tindakan.

Titik perbandingan	Pemulihan otomatis yang disederhanakan	CloudWatch pemulihan berbasis tindakan
Konfigurasi	Diaktifkan secara default pada instance yang didukung	Membutuhkan konfigura si CloudWatch alarm dan tindakan secara manual
Fleksibilitas	Perilaku pemulihan tetap dikelola oleh AWS	Tindakan dan kondisi yang dapat disesuaikan
Notifikasi	Pemberitahuan dasar melalui Dasbor Health	Pemberitahuan yang dapat disesuaikan melalui SNS
Ukuran contoh logam	Dikecualikan	Termasuk
Volume penyimpanan instans terlampir saat peluncuran	Tidak didukung untuk instance yang melampirkan volume penyimpanan instance saat peluncuran	Didukung pada jenis instans yang dipilih. Perhatikan bahwa data pada volume penyimpan an instance hilang selama pemulihan instance.
Waktu pemulihan	Upaya pemulihan standar	Upaya pemulihan lebih cepat daripada pemulihan otomatis yang disederhanakan
Masalah host teratasi selama migrasi	Migrasi mungkin dibatalkan dan instance tetap berada di host asli	Migrasi berlanjut ke host baru

Titik perbandingan	Pemulihan otomatis yang disederhanakan	CloudWatch pemulihan berbasis tindakan
Biaya	Tidak ada biaya tambahan	Mungkin dikenakan biaya CloudWatch

Membangun sistem yang tangguh

Meskipun pemulihan otomatis yang disederhanakan dan pemulihan berbasis CloudWatch tindakan efektif untuk menjaga ketersediaan instans individu, AWS merekomendasikan penerapan arsitektur ketersediaan tinggi yang memungkinkan failover lalu lintas ke instance yang sehat.

Untuk mencapai hal ini, pertimbangkan untuk menggunakan AWS layanan seperti Elastic Load Balancing (yang mendistribusikan lalu lintas masuk di beberapa instans EC2) dan Amazon EC2 Auto Scaling (yang secara otomatis menyesuaikan jumlah instans berdasarkan permintaan dan kesehatan).

Untuk informasi selengkapnya tentang membangun sistem yang tangguh dan toleran terhadap kesalahan dengan instans EC2, lihat sumber daya berikut:

- Kembali ke Dasar: Merancang untuk Kegagalan dengan EC2 di saluran AWS YouTube
- Arsitektur Pemulihan Bencana (DR) pada AWS, Bagian I: Strategi Pemulihan di Cloud di situs Blog AWS Arsitektur
- Panduan Pengguna Penyeimbang Beban Aplikasi
- Panduan Pengguna Penskalaan Otomatis Amazon EC2
- REL11- BP02 Gagal menggunakan sumber daya yang sehat dalam Reliability Pillar AWS Well-Architected Framework

Verifikasi apakah pemulihan instans otomatis terjadi

Jika instans Anda tampaknya telah offline dan kemudian di-boot ulang secara tak terduga, itu mungkin telah mengalami pemulihan instans otomatis sebagai respons terhadap masalah perangkat keras atau perangkat lunak yang mendasarinya. Anda dapat memverifikasi ini dengan memeriksa peristiwa pemulihan instans otomatis di Anda Dasbor Health. Anda juga dapat memeriksa apakah masalah perangkat keras atau perangkat lunak yang mendasarinya terdeteksi untuk instans Anda dengan memeriksa CloudWatch metrik StatusCheckFailed_System Amazon.

Periksa acara di Dasbor Health

Ketika upaya pemulihan instans otomatis terjadi, AWS kirimkan acara ke Anda Dasbor Health. Peristiwa spesifik tergantung pada mekanisme pemulihan yang dikonfigurasi dan apakah upaya berhasil atau gagal.

Untuk memeriksa peristiwa pemulihan instans otomatis di Dasbor Health

1. Buka di Dasbor Health https://phd.aws.amazon.com/phd/rumah #/.
2. Cari peristiwa yang terkait dengan pemulihan instans otomatis. Kehadiran peristiwa ini dapat mengkonfirmasi apakah upaya pemulihan instance otomatis terjadi dan hasilnya.

   - Pemulihan otomatis yang disederhanakan
     - Acara sukses: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
     - Peristiwa kegagalan: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`
   - CloudWatch pemulihan berbasis tindakan
     - Acara sukses: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
     - Peristiwa kegagalan: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Memantau pemeriksaan status sistem dengan CloudWatch

Anda dapat memverifikasi apakah masalah perangkat keras atau perangkat lunak yang mendasarinya terdeteksi untuk instance Anda dengan memeriksa metrik StatusCheckFailed_System di CloudWatch. Nilai metrik menunjukkan apakah pemeriksaan status sistem lulus (tidak ada masalah perangkat keras atau perangkat lunak) atau gagal (masalah perangkat keras atau perangkat lunak).

Untuk memverifikasi apakah masalah perangkat keras atau perangkat lunak yang mendasarinya terdeteksi

1. Buka halaman Metrik CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/rumah? #metricsV2.
2. Verifikasi bahwa Anda berada di Wilayah yang sama dengan instans EC2 Anda.
3. Tempel metrik berikut di bidang pencarian Metrik, dan tekan Enter.

   ```
   StatusCheckFailed_System
   ```

4. Pilih EC2 > Metrik Per-Instance.

5. Dalam tabel, pilih kotak centang di sebelah contoh yang ingin Anda centang.
6. Ubah periode kueri ke waktu yang Anda curigai peristiwa pemulihan terjadi.
7. Pilih tab Graphed metrics, dan untuk StatusCheckFailed_System, lakukan hal berikut:
   a. Untuk Statistik, pilih Rata-rata, Maksimum, atau Minimum.
   b. Untuk Periode, pilih 1 menit.
8. Periksa nilai untuk StatusCheckFailed_System.
   - Nilai 0: Pemeriksaan status sistem lulus, menunjukkan tidak ada masalah perangkat keras atau perangkat lunak yang mendasarinya.
   - Nilai 1: Pemeriksaan status sistem gagal, menunjukkan masalah perangkat keras atau perangkat lunak yang mendasarinya.

Untuk informasi selengkapnya, lihat Pemulihan instans otomatis.

Konfigurasikan pemulihan otomatis yang disederhanakan pada instans Amazon EC2

> **Important**
>
> Bagian ini menjelaskan cara mengkonfigurasi mekanisme pemulihan secara proaktif pada instans EC2. Mekanisme pemulihan ini dirancang untuk mengembalikan ketersediaan instance ketika AWS mendeteksi masalah perangkat keras atau perangkat lunak yang mendasari yang menyebabkan pemeriksaan status sistem gagal. Jika saat ini Anda mengalami masalah saat mengakses instans, lihat Memecahkan masalah instans EC2.

Jika AWS mendeteksi bahwa instance tidak tersedia karena masalah perangkat keras atau perangkat lunak yang mendasarinya, pemulihan otomatis yang disederhanakan dapat secara otomatis memulihkan ketersediaan instance dengan memindahkan instance dari host dengan masalah mendasar ke host lain.

Jika pemulihan otomatis yang disederhanakan terjadi, AWS kirimkan salah satu peristiwa berikut ke Anda Dasbor AWS Health, tergantung pada hasilnya:

- Acara sukses: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
- Peristiwa kegagalan: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`

Untuk diberitahu tentang peristiwa ini, Anda dapat mengonfigurasi pemberitahuan. Untuk informasi selengkapnya, lihat Membuat konfigurasi notifikasi pertama Anda Notifikasi Pengguna AWS di Panduan Notifikasi Pengguna AWS Pengguna. Anda juga dapat menggunakan EventBridge aturan Amazon untuk memantau peristiwa pemulihan otomatis yang disederhanakan.

Pemulihan otomatis yang disederhanakan diaktifkan secara default pada semua instance yang didukung selama peluncuran instans. Namun, itu hanya dapat beroperasi jika instance dalam `running` keadaan, tidak ada peristiwa layanan yang tercantum di Dasbor AWS Health, dan ada kapasitas yang tersedia untuk jenis instance. Dalam beberapa situasi, seperti pemadaman yang signifikan, kendala kapasitas dapat menyebabkan upaya pemulihan gagal. Untuk informasi selengkapnya, lihat the section called “Memecahkan masalah kegagalan pemulihan otomatis yang disederhanakan”.

Anda dapat menonaktifkan pemulihan otomatis yang disederhanakan selama atau setelah peluncuran, dan mengaktifkannya kembali nanti jika diperlukan.

> **Warning**
>
> Ketika AWS memulihkan instans Anda karena masalah perangkat keras atau perangkat lunak yang mendasarinya, perhatikan konsekuensi berikut: data yang disimpan dalam memori volatil (RAM) akan hilang dan uptime sistem operasi akan dimulai dari nol. Untuk membantu melindungi dari kehilangan data, kami sarankan Anda secara teratur membuat cadangan data berharga. Untuk informasi selengkapnya tentang praktik terbaik pencadangan dan pemulihan untuk instans EC2, lihat Praktik terbaik untuk Amazon EC2.
> Mekanisme pemulihan instans otomatis dirancang untuk instance individual. Untuk panduan tentang membangun sistem yang tangguh, lihat. Membangun sistem yang tangguh

Daftar Isi

- Persyaratan untuk mengaktifkan pemulihan otomatis yang disederhanakan
- Konfigurasikan pemulihan otomatis yang disederhanakan
- Memecahkan masalah kegagalan pemulihan otomatis yang disederhanakan

Persyaratan untuk mengaktifkan pemulihan otomatis yang disederhanakan

Pemulihan otomatis yang disederhanakan dapat diaktifkan pada instans yang memenuhi kriteria berikut:

Tipe instans

- Tujuan umum: A1, M3, M4, M5, M5a, M5n, M5Zn, M6a, M6g, M6i, M6in, M7a, M7g, M7i, M7i-flex, M8a, M8AZN, M8g, M8GB, M8Gn, M8i, M8i-flex, T1, T2, T3, T3a, T4G
- Komputasi dioptimalkan: C3, C4, C5, C5a, C5n, C6a, C6g, C6Gn, C6i, C6in, C7a, C7g, C7gN, C7i, C7i-flex, C8a, C8g, C8gB, C8gn, C8i, C8i-flex
- Memori dioptimalkan: R3, R4, R5, R5a, R5b, R5n, R6a, R6g, R6i, R6in, R7a, R7g, R7i, R7iZ, R8a, R8g, R8gb, R8gn, R8i, R8i-flex, U-3TB1, U-6TB1, U-96TB1 TB1, U-12TB1, U-18TB1, U-24tb1, U7I-6TB, U7I-8tb, U7i-12TB, U7in-16TB, U7in-24tb, U7in-32tb, U7inh-32tb, X1, X1e, X2iEZN, X8g, X8i
- Komputasi yang dipercepat: G3, G5g, Inf1, P3, VT1
- Komputasi kinerja tinggi: HPC6a, hPC7a, hPC7g, hPC8a

Penghunian

- Bersama
- Instans Khusus

  Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.

Batasan

Pemulihan otomatis yang disederhanakan tidak didukung untuk instance dengan karakteristik sebagai berikut:

- Ukuran instans: `metal` contoh
- Sewa: Tuan Rumah Khusus. Untuk Host Khusus, gunakan Pemulihan Otomatis Host Khusus sebagai gantinya.
- Penyimpanan: Instans dengan volume penyimpanan instans
- Jaringan: Contoh menggunakan Adaptor Kain Elastis
- Auto Scaling: Instans yang merupakan bagian dari grup Auto Scaling
- Pemeliharaan: Instans yang sedang menjalani acara pemeliharaan terjadwal

Konfigurasikan pemulihan otomatis yang disederhanakan

Pemulihan otomatis yang disederhanakan diaktifkan secara default saat Anda meluncurkan instans yang didukung. Anda dapat mengatur perilaku pemulihan otomatis `disabled` selama atau setelah meluncurkan instance.

`default`Konfigurasi tidak mengaktifkan pemulihan otomatis yang disederhanakan untuk instance yang tidak didukung.

Console

Untuk menonaktifkan pemulihan otomatis simpel saat peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Instans, kemudian pilih Luncurkan instans.
3. Di bagian Detail lanjutan, untuk Pemulihan otomatis Instans, pilih Dinonaktifkan.
4. Konfigurasikan pengaturan peluncuran instans yang tersisa sesuai kebutuhan kemudian luncurkan instans.

Untuk menonaktifkan pemulihan otomatis yang disederhanakan setelah peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Tindakan, Pengaturan instans, Ubah perilaku pemulihan otomatis.
4. Pilih Nonaktif, lalu pilih Simpan.

Untuk mengaktifkan pemulihan otomatis yang disederhanakan setelah peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Tindakan, Pengaturan instans, Ubah perilaku pemulihan otomatis.
4. Pilih Default (Aktif), lalu pilih Simpan.

AWS CLI

Untuk menonaktifkan pemulihan otomatis simpel saat peluncuran

Gunakan perintah run-instance dengan opsi. `--maintenance-options`

```
--maintenance-options AutoRecovery=Disabled
```

Untuk menonaktifkan pemulihan otomatis yang disederhanakan setelah peluncuran

Gunakan perintah modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-1234567890abcdef0 \
    --auto-recovery disabled
```

Untuk mengaktifkan pemulihan otomatis yang disederhanakan setelah peluncuran

Gunakan perintah modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-1234567890abcdef0 \
    --auto-recovery default
```

PowerShell

Untuk menonaktifkan pemulihan otomatis simpel saat peluncuran

Gunakan New-EC2Instancecmdlet.

```
-MaintenanceOptions_AutoRecovery Disabled
```

Untuk menonaktifkan pemulihan otomatis yang disederhanakan setelah peluncuran

Gunakan Edit-EC2InstanceMaintenanceOptioncmdlet.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -AutoRecovery Disabled
```

Untuk mengaktifkan pemulihan otomatis yang disederhanakan setelah peluncuran

Gunakan Edit-EC2InstanceMaintenanceOptioncmdlet.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -AutoRecovery Enabled
```

Memecahkan masalah kegagalan pemulihan otomatis yang disederhanakan

Jika pemulihan otomatis yang disederhanakan gagal memulihkan instans Anda, pertimbangkan masalah berikut:

- AWS acara layanan sedang berjalan

  Pemulihan otomatis yang disederhanakan tidak beroperasi selama acara layanan di Dasbor AWS Health. Anda mungkin tidak menerima notifikasi kegagalan pemulihan untuk peristiwa semacam itu. Untuk informasi ketersediaan layanan terbaru, lihat halaman Status kesehatan layanan.

- Kapasitas tidak mencukupi

  Perangkat keras pengganti sementara tidak cukup untuk memigrasikan instance.

- Upaya pemulihan harian maksimum tercapai

  Instans telah mencapai tunjangan harian maksimum untuk upaya pemulihan. Instans Anda kemudian dapat dihentikan jika pemulihan otomatis gagal dan degradasi perangkat keras ditentukan sebagai akar penyebab pemeriksaan status sistem gagal asli.

Jika kegagalan pemeriksaan status sistem instans tetap ada meskipun beberapa upaya pemulihan, lihat Memecahkan masalah instance dengan pemeriksaan status gagal untuk panduan tambahan.

Konfigurasikan pemulihan berbasis CloudWatch tindakan pada instans EC2

> **Important**
>
> Bagian ini menjelaskan cara mengkonfigurasi mekanisme pemulihan secara proaktif pada instans EC2. Mekanisme pemulihan ini dirancang untuk mengembalikan ketersediaan instance ketika AWS mendeteksi masalah perangkat keras atau perangkat lunak yang mendasari yang menyebabkan pemeriksaan status sistem gagal. Jika saat ini Anda mengalami masalah saat mengakses instans, lihat Memecahkan masalah instans EC2.

Jika AWS mendeteksi bahwa instance tidak tersedia karena masalah perangkat keras atau perangkat lunak yang mendasarinya, pemulihan berbasis CloudWatch tindakan dapat secara otomatis memulihkan ketersediaan instance dengan memindahkan instance dari host dengan masalah mendasar ke host lain.

Jika pemulihan berbasis CloudWatch tindakan terjadi, AWS kirimkan salah satu peristiwa berikut ke Anda Dasbor AWS Health, tergantung pada hasilnya:

- Acara sukses: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
- Peristiwa kegagalan: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Anda dapat mengonfigurasi pemulihan berbasis CloudWatch tindakan untuk menambahkan tindakan pemulihan ke CloudWatch alarm Amazon. CloudWatch pemulihan berbasis tindakan bekerja dengan `StatusCheckFailed_System` metrik. CloudWatchpemulihan berbasis tindakan memberikan perincian waktu respons to-the-minute pemulihan dan pemberitahuan Amazon Simple Notification Service (Amazon SNS) tentang tindakan dan hasil pemulihan. Opsi konfigurasi ini memungkinkan upaya pemulihan yang lebih cepat dengan kontrol yang lebih terperinci atas respons peristiwa kegagalan pemeriksaan status sistem dibandingkan dengan pemulihan otomatis yang disederhanakan. Untuk informasi selengkapnya tentang CloudWatch opsi yang tersedia, lihat Pemeriksaan status untuk instans Anda.

Namun, pemulihan berbasis CloudWatch tindakan hanya dapat beroperasi jika instance dalam `running` keadaan, tidak ada peristiwa layanan yang tercantum di Dasbor AWS Health, dan ada kapasitas yang tersedia untuk jenis instans. Dalam beberapa situasi, seperti pemadaman yang signifikan, kendala kapasitas dapat menyebabkan upaya pemulihan gagal. Untuk informasi selengkapnya, lihat the section called “Pemecahan Masalah”.

> **Warning**
>
> Saat AWS memulihkan instans Anda karena masalah perangkat keras atau perangkat lunak yang mendasarinya, perhatikan konsekuensi berikut: data yang disimpan dalam memori volatil (RAM) dan volume penyimpanan instans akan hilang, dan waktu aktif sistem operasi akan dimulai dari nol. Untuk membantu melindungi dari kehilangan data, kami sarankan Anda secara teratur membuat cadangan data berharga. Untuk informasi selengkapnya tentang praktik terbaik pencadangan dan pemulihan untuk instans EC2, lihat Praktik terbaik untuk Amazon EC2.
>
> Mekanisme pemulihan instans otomatis dirancang untuk instance individual. Untuk panduan tentang membangun sistem yang tangguh, lihat. Membangun sistem yang tangguh

Daftar Isi

- Persyaratan untuk mengaktifkan pemulihan berbasis CloudWatch tindakan

- Konfigurasikan pemulihan berbasis CloudWatch tindakan
- Memecahkan masalah kegagalan CloudWatch pemulihan berbasis tindakan

Persyaratan untuk mengaktifkan pemulihan berbasis CloudWatch tindakan

CloudWatch pemulihan berbasis tindakan dapat diaktifkan pada instance yang memenuhi kriteria berikut:

Tipe instans

- Tujuan umum: A1, M3, M4, M5, M5a, M5n, M5Zn, M6a, M6g, M6i, M6in, M7a, M7g, M7i, M7i-flex, M8a, M8AZN, M8g, M8GB, M8Gn, M8i, M8i-flex, T1, T2, T3, T3a, T4G
- Komputasi dioptimalkan: C3, C4, C5, C5a, C5n, C6a, C6g, C6Gn, C6i, C6in, C7a, C7g, C7gN, C7i, C7i-flex, C8a, C8g, C8gB, C8gn, C8i, C8i-flex
- Memori dioptimalkan: R3, R4, R5, R5a, R5b, R5n, R6a, R6g, R6i, R6in, R7a, R7g, R7i, R7iZ, R8a, R8g, R8gb, R8gn, R8i, R8i-flex, U-3TB1, U-6TB1, U-96TB1 TB1, U-12TB1, U-18TB1, U-24tb1, U7I-6TB, U7I-8TB, U7i-12TB, U7in-16TB, U7in-24TB, U7in-32TB, U7inh-32TB, X1, X1E, X2iEDN, X2iEZN, X8g, X8i
- Komputasi yang dipercepat: G3, G5g, Inf1, P3, VT1
- Komputasi kinerja tinggi: HPC6a, hPC7a, hPC7g, hPC8a
- Contoh logam: Salah satu jenis contoh di atas dengan ukuran instans logam.
- Jika volume penyimpanan instance ditambahkan saat peluncuran: Maka hanya jenis instance berikut yang didukung: M3, C3, R3, X1, X1e, X2idn, X2IEdn

Penghunian

- Bersama
- Instans Khusus

  Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.

Batasan

CloudWatch pemulihan berbasis tindakan tidak didukung untuk instance dengan karakteristik sebagai berikut:

- Sewa: Tuan Rumah Khusus. Untuk Host Khusus, gunakan Pemulihan Otomatis Host Khusus sebagai gantinya.

- Jaringan: Contoh menggunakan Adaptor Kain Elastis
- Auto Scaling: Instans yang merupakan bagian dari grup Auto Scaling
- Pemeliharaan: Instans yang sedang menjalani acara pemeliharaan terjadwal

Temukan jenis instans yang didukung

Anda dapat melihat jenis instance yang mendukung pemulihan berbasis CloudWatch tindakan.

Console

Untuk melihat jenis instance yang mendukung pemulihan berbasis CloudWatch tindakan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Tipe Instans.
3. Di bilah filter, tambahkan filter Auto Recovery support = true. Tabel tipe Instance menampilkan semua tipe instance yang mendukung pemulihan berbasis CloudWatch tindakan.
4. (Opsional) Tambahkan filter ke cakupan lebih lanjut ke jenis instans tertentu yang menarik.

AWS CLI

Untuk melihat jenis instance yang mendukung pemulihan berbasis CloudWatch tindakan

Gunakan describe-instance-typesperintah dengan `auto-recovery-supported` filter.

```
aws ec2 describe-instance-types \
    --filters Name=auto-recovery-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Untuk melihat jenis instance yang mendukung pemulihan berbasis CloudWatch tindakan

Gunakan Get-EC2InstanceTypecmdlet dengan filter. `auto-recovery-supported`

```
Get-EC2InstanceType `
    -Filter @{Name="auto-recovery-supported";Values="true"} | `
    Select InstanceType | Sort-Object InstanceType
```

Konfigurasikan pemulihan berbasis CloudWatch tindakan

Untuk mengonfigurasi pemulihan berbasis CloudWatch tindakan untuk instans EC2, buat CloudWatch alarm yang memantau `StatusCheckFailed_System` metrik untuk instance yang ditentukan. Atur alarm untuk dipicu saat nilai metrik adalah 1, yang menunjukkan pemeriksaan status sistem yang gagal. Konfigurasikan tindakan alarm untuk memulihkan instance secara otomatis saat dipicu.

Anda dapat mengonfigurasi alarm menggunakan konsol Amazon EC2 atau konsol. CloudWatch Untuk petunjuknya, lihat Tambahkan tindakan pemulihan ke CloudWatch alarm Amazon di panduan pengguna ini, atau Menambahkan tindakan pemulihan ke CloudWatch alarm Amazon di Panduan CloudWatch Pengguna Amazon.

Memecahkan masalah kegagalan CloudWatch pemulihan berbasis tindakan

Jika pemulihan berbasis CloudWatch tindakan gagal memulihkan instans Anda, pertimbangkan masalah berikut:

- AWS acara layanan sedang berjalan

  CloudWatch pemulihan berbasis tindakan tidak beroperasi selama acara layanan di Dasbor AWS Health. Anda mungkin tidak menerima notifikasi kegagalan pemulihan untuk peristiwa semacam itu. Untuk informasi ketersediaan layanan terbaru, lihat halaman Status kesehatan layanan.
- Kapasitas tidak mencukupi

  Perangkat keras pengganti sementara tidak cukup untuk memigrasikan instance.
- Upaya pemulihan harian maksimum tercapai

  Instans telah mencapai tunjangan harian maksimum untuk upaya pemulihan. Instans Anda kemudian dapat dihentikan jika pemulihan otomatis gagal dan degradasi perangkat keras ditentukan sebagai akar penyebab pemeriksaan status sistem gagal asli.

Jika kegagalan pemeriksaan status sistem instans tetap ada meskipun beberapa upaya pemulihan, lihat Memecahkan masalah instance dengan pemeriksaan status gagal untuk panduan tambahan.

Gunakan metadata instans untuk mengelola instans EC2

Metadata instans adalah data tentang instans Anda yang dapat Anda gunakan untuk mengonfigurasi atau mengelola instans berjalan. Metadata instance meliputi yang berikut:

Properti metadata contoh

Properti metadata instance dibagi ke dalam kategori, misalnya, nama host, acara, dan grup keamanan.

Data dinamis

Data dinamis adalah metadata yang dihasilkan saat instance diluncurkan, seperti dokumen identitas instance. Untuk informasi selengkapnya, lihat Kategori data dinamis.

Data pengguna

Anda juga dapat menggunakan metadata instance untuk mengakses data pengguna yang Anda tentukan saat meluncurkan instans. Misalnya, Anda dapat menentukan parameter untuk mengonfigurasi instans Anda, atau menyertakan skrip sederhana. Anda juga dapat membangun generik AMIs dan menggunakan data pengguna untuk memodifikasi file konfigurasi yang disediakan pada waktu peluncuran. Misalnya, jika Anda menjalankan server web untuk berbagai bisnis kecil, mereka semua dapat menggunakan AMI generik yang sama dan mengambil kontennya dari bucket Amazon S3 yang Anda tentukan dalam data pengguna saat peluncuran. Untuk menambahkan pelanggan baru kapan saja, buat bucket untuk pelanggan, tambahkan konten mereka, dan luncurkan AMI Anda dengan nama keranjang bucket unik yang diberikan untuk kode Anda di data pengguna. Jika Anda meluncurkan beberapa instance menggunakan `RunInstances` panggilan yang sama, data pengguna tersedia untuk semua instance dalam reservasi tersebut. Setiap instance yang merupakan bagian dari reservasi yang sama memiliki `ami-launch-index` nomor unik, sehingga Anda dapat menulis kode yang mengontrol apa yang dilakukan instance. Misalnya, host pertama mungkin memilih dirinya sendiri sebagai simpul asli dalam sebuah klaster. Untuk contoh peluncuran AMI mendetail, lihat .Identifikasi setiap instance yang diluncurkan dalam satu permintaan

Important

Meskipun Anda hanya dapat mengakses metadata instans dan data pengguna dari dalam instans itu sendiri, data tersebut tidak dilindungi oleh metode autentikasi atau kriptografi. Siapa pun yang memiliki akses langsung ke instans, dan perangkat lunak apa pun yang kemungkinan berjalan di instans, akan dapat melihat metadatanya. Oleh karena itu, Anda tidak boleh menyimpan data sensitif, seperti sandi atau kunci enkripsi yang tahan lama, sebagai data pengguna.

Daftar Isi

- Kategori metadata instans
- Kategori data dinamis
- Akses metadata instans untuk instans EC2
- Konfigurasikan opsi Layanan Metadata Instance
- Jalankan perintah saat Anda meluncurkan instans EC2 dengan input data pengguna
- Identifikasi setiap instance yang diluncurkan dalam satu permintaan

Kategori metadata instans

Properti metadata instance dibagi menjadi beberapa kategori. Untuk mengambil properti metadata instance, Anda menentukan kategori dalam permintaan, dan metadata dikembalikan dalam respons.

Saat kategori baru dirilis, build metadata instans baru dibuat dengan nomor versi baru. Dalam tabel berikut, kolom Versi saat kategori dirilis menentukan versi build saat kategori metadata instans dirilis. Untuk menghindari keharusan memperbarui kode Anda setiap kali Amazon EC2 merilis build metadata instans baru, gunakan `latest`, bukan nomor versi, di permintaan metadata Anda. Untuk informasi selengkapnya, lihat Dapatkan versi metadata instans yang tersedia.

Saat Amazon EC2 merilis kategori metadata instans baru, metadata instans untuk kategori baru mungkin tidak tersedia untuk instans yang sudah ada. Dengan instans berbasis Nitro, Anda dapat mengambil metadata instance hanya untuk kategori yang tersedia saat peluncuran. Untuk instans dengan hypervisor Xen, Anda dapat menghentikan dan kemudian memulai instans untuk memperbarui kategori yang tersedia untuk instans tersebut.

Tabel berikut mencantumkan kategori metadata instans. Beberapa nama kategori menyertakan placeholder untuk data yang unik untuk instans Anda. Misalnya, *`mac`* mewakili alamat MAC untuk antarmuka jaringan. Anda harus mengganti placeholder dengan nilai sebenarnya saat Anda mengambil metadata instans.

Kategori	Deskripsi	Versi ketika kategori dirilis
`ami-id`	ID AMI yang digunakan untuk meluncurkan instans.	1.0

Kategori	Deskripsi	Versi ketika kategori dirilis
`ami-launch-index`	Jika Anda meluncurkan beberapa instance menggunakan `RunInstances` panggilan yang sama, nilai ini menunjukkan urutan peluncuran untuk setiap instance. Nilai instans pertama yang diluncurkan adalah 0. Jika Anda meluncurkan instans menggunakan Auto Scaling atau armada EC2, nilai ini selalu 0.	1.0
`ami-manifest-path`	Jalur ke file manifes AMI di Amazon S3. Jika Anda menggunakan AMI yang didukung Amazon EBS untuk meluncurkan instans, hasil yang dikembalikan adalah `unknown`.	1.0
`ancestor-ami-ids`	AMI IDs dari setiap instance yang dibundel ulang untuk membuat AMI ini. Nilai ini hanya akan ada jika file manifes AMI berisi kunci `ancestor-amis` .	10/10/2007

Kategori	Deskripsi	Versi ketika kategori dirilis
`autoscaling/target-lifecycle-state`	Nilai yang menunjukkan status siklus hidup Auto Scaling target yang dialihkan oleh instans Auto Scaling. Anda pada saat instans bertransisi ke salah satu status siklus hidup target setelah 10 Maret 2022. Nilai yang mungkin: `Detached` `InService` | `Standby` | `Terminated` | `Warmed:Hibernated` | `Warmed:Running` | `Warmed:Stopped` | `Warmed:Terminated`. Lihat Mengambil status siklus hidup target melalui metadata instans di Panduan Pengguna Amazon EC2 Auto Scaling.	2021-07-15
`block-device-mapping/ami`	Perangkat virtual yang berisi sistem root/boot file.	15/12/2007
`block-device-mapping/ebsN`	Perangkat virtual yang terkait dengan volume Amazon EBS apa pun. Volume Amazon EBS hanya tersedia dalam metadata jika volume itu ada pada waktu peluncuran atau saat instans terakhir kali dimulai. N menunjukkan indeks volume Amazon EBS (seperti `ebs1` atau `ebs2`).	15/12/2007

Kategori	Deskripsi	Versi ketika kategori dirilis
`block-device-mapping/ephemeral N`	Perangkat virtual untuk setiap volume penyimpanan NVMe non-instance. N menunjukkan indeks setiap volume. Jumlah volume penyimpanan instans dalam pemetaan perangkat blok mungkin tidak cocok dengan jumlah volume penyimpanan instans yang sebenarnya untuk instans tersebut. Tipe instans menentukan jumlah volume penyimpanan instans yang tersedia untuk sebuah instans. Jika jumlah volume penyimpanan instans dalam pemetaan perangkat blok melebihi jumlah yang tersedia untuk sebuah instans, volume penyimpanan instans tambahan akan diabaikan.	15/12/2007
`block-device-mapping/root`	Perangkat virtual atau partisi yang terkait dengan perangkat atau partisi root pada perangkat virtual, di mana sistem file root (/ atau C:) dikaitkan dengan instans tertentu.	15/12/2007
`block-device-mapping/swap`	Perangkat virtual yang terkait dengan `swap`. Tidak selalu ada.	15/12/2007
`events/maintenance/history`	Jika ada peristiwa pemeliharaan yang diselesaikan atau dibatalkan untuk instans tersebut, berisi string JSON dengan informasi tentang peristiwa tersebut.	17/08/2018

Kategori	Deskripsi	Versi ketika kategori dirilis
`events/maintenance/scheduled`	Jika ada peristiwa pemeliharaan aktif untuk instans tersebut, berisi string JSON dengan informasi tentang peristiwa tersebut. Untuk informasi selengkapnya, lihat Melihat peristiwa terjadwal yang memengaruhi instans Amazon EC2 Anda.	17/08/2018
`events/recommendations/rebalance`	Perkiraan waktu, dalam UTC, ketika notifikasi rekomendasi penyeimbangan ulang instans EC2 dikeluarkan untuk instans tersebut. Berikut adalah contoh metadata untuk kategori ini: `{"noticeTime": "2020-11-05T08:22:00Z"}` . Kategori ini hanya tersedia setelah notifikasi dikeluarkan. Untuk informasi selengkapnya, lihat Rekomendasi penyeimbangan ulang instans EC2.	2020-10-27

Kategori	Deskripsi	Versi ketika kategori dirilis
`hostname`	Jika instans EC2 menggunakan Penamaan berbasis IP (IPBN), ini adalah nama host DNS IPv4 privat dari instans tersebut. Jika instans EC2 menggunakan Penamaan berbasis sumber Daya (RBN), ini adalah RBN. Jika ada banyak antarmuka jaringan, ini mengacu pada perangkat eth0 (perangkat yang nomor perangkatnya adalah 0). Untuk informasi selengkapnya tentang IPBN dan RBN, lihat Nama host dan domain instans EC2.	1.0
`iam/info`	Jika ada peran IAM yang terkait dengan instance, berisi informasi tentang terakhir kali profil instans diperbarui, termasuk LastUpdated tanggal instans, InstanceProfileArn , danInstanceProfileId. Jika tidak, tidak ada.	12/01/2012
`iam/security-credentials/role-name`	Jika ada peran IAM yang terkait dengan instance, *`role-name`* adalah nama peran, dan *`role-name`* berisi kredensil keamanan sementara yang terkait dengan peran tersebut (untuk informasi selengkapnya, lihat). Mengambil kredensial keamanan dari metadata instans Jika tidak, tidak ada.	12/01/2012

Kategori	Deskripsi	Versi ketika kategori dirilis
`identity-credentials/ec2/info`	Informasi tentang kredensial di `identity-credentials/ec2/security-credentials/ec2-instance` .	23/05/2018
`identity-credentials/ec2/security-credentials/ec2-instance`	Kredensil untuk peran identitas instans yang memungkinkan perangkat lunak on-instance mengidentifikasi dirinya AWS untuk mendukung fitur seperti EC2 Instance Connect AWS Systems Manager dan Default Host Management Configuration. Kredensi ini tidak memiliki kebijakan yang dilampirkan, sehingga mereka tidak memiliki izin AWS API tambahan selain mengidentifikasi instance ke fitur tersebut. AWS Untuk informasi selengkapnya, lihat Peran identitas instans untuk instans Amazon EC2.	23/05/2018
`instance-action`	Memberi tahu instans bahwa instans harus di-boot ulang sebagai persiapan untuk pemaketan. Nilai yang valid: `none` | `shutdown` | `bundle-pending` .	01/09/2008
`instance-id`	ID instans ini.	1.0

Kategori	Deskripsi	Versi ketika kategori dirilis
`instance-life-cycle`	Opsi pembelian instans ini. Untuk informasi selengkapnya, lihat Opsi penagihan dan pembelian Amazon EC2.	01/10/2019
`instance-type`	Tipe instans. Untuk informasi selengkapnya, lihat Tipe instans Amazon EC2.	29/08/2007
`ipv6`	IPv6 Alamat instance. Dalam kasus di mana beberapa antarmuka jaringan hadir, ini mengacu pada perangkat eth0 (perangkat yang nomor perangkat nya 0) antarmuka jaringan dan IPv6 alamat pertama yang ditetapkan. Jika tidak ada IPv6 alamat di antarmuka jaringan [0], item ini tidak disetel dan menghasil kan respons HTTP 404.	2021-01-03
`kernel-id`	ID kernel yang diluncurkan dengan instans ini, jika ada.	01/02/2008

Kategori	Deskripsi	Versi ketika kategori dirilis
`local-hostname`	Jika ada banyak antarmuka jaringan, ini mengacu pada perangkat eth0 (perangkat yang nomor perangkatnya adalah 0). Jika instans EC2 menggunakan Penamaan berbasis IP (IPBN), ini adalah nama host DNS IPv4 privat dari instans tersebut. Jika instans EC2 menggunakan Penamaan berbasis sumber Daya (RBN), ini adalah RBN. Untuk informasi selengkapnya tentang penamaan IPBN, RBN, dan EC2, lihat Nama host dan domain instans EC2.	19/01/2007
`local-ipv4`	IPv4 Alamat pribadi dari instance. Jika ada banyak antarmuka jaringan, ini mengacu pada perangkat eth0 (perangkat yang nomor perangkatnya adalah 0). Jika ini adalah instance IPv6 -only, item ini tidak disetel dan menghasilkan respons HTTP 404.	1.0
`mac`	Alamat kontrol akses media (MAC) instans. Jika ada banyak antarmuka jaringan, ini mengacu pada perangkat eth0 (perangkat yang nomor perangkatnya adalah 0).	01/01/2011
`metrics/vhostmd`	Tidak lagi tersedia.	01/05/2011

Kategori	Deskripsi	Versi ketika kategori dirilis
`network/interfaces/macs/mac/device-number`	Nomor perangkat unik yang terkait dengan antarmuka itu. Nomor perangkat sesuai dengan nama perangkat; misalnya, `device-number` pada 2 adalah untuk perangkat eth2. Kategori ini sesuai dengan bidang `DeviceIndex` dan `device-index` yang digunakan oleh API Amazon EC2 dan perintah EC2 untuk AWS CLI.	01-01-2011
`network/interfaces/macs/mac/interface-id`	ID antarmuka jaringan.	01-01-2011
`network/interfaces/macs/mac/ipv4-associations/public-ip`	IPv4 Alamat pribadi yang terkait dengan setiap alamat IP publik dan ditetapkan ke antarmuka itu.	01-01-2011
`network/interfaces/macs/mac/ipv6s`	IPv6 Alamat yang ditetapkan ke antarmuka.	30/06/2016
`network/interfaces/macs/mac/ipv6-prefix`	IPv6 Awalan yang ditetapkan ke antarmuka jaringan.	
`network/interfaces/macs/mac/local-hostname`	Nama host IPv4 DNS pribadi dari instance. Jika ada banyak antarmuka jaringan, ini mengacu pada perangkat eth0 (perangkat yang nomor perangkatnya adalah 0). Jika ini adalah instance IPv6 -only, ini adalah nama berbasis sumber daya. Untuk informasi selengkapnya tentang IPBN dan RBN, lihat Nama host dan domain instans EC2.	19/01/2007

Kategori	Deskripsi	Versi ketika kategori dirilis
`network/interfaces/macs/mac/local-ipv4s`	IPv4 Alamat pribadi yang terkait dengan antarmuka. Jika ini adalah antarmuka jaringan IPv6 -only, item ini tidak disetel dan menghasilkan respons HTTP 404.	01-01-2011
`network/interfaces/macs/mac/mac`	Alamat MAC instans.	01/01/2011
`network/interfaces/macs/`*`mac`*`/network-card`	Indeks kartu jaringan. Beberapa tipe instans mendukung banyak kartu jaringan.	01/11/2020
`network/interfaces/macs/mac/owner-id`	ID pemilik antarmuka jaringan. Di lingkungan multi-antarmuka, antarmuka dapat dipasang oleh pihak ketiga, seperti Elastic Load Balancing. Lalu lintas pada antarmuka selalu ditagihkan ke pemilik antarmuka.	01-01-2011
`network/interfaces/macs/mac/public-hostname`	DNS publik antarmuka (IPv4). Kategori ini hanya ditampilkan jika atribut `enableDnsHostnames` diatur ke `true`. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda dalam Panduan Pengguna Amazon VPC. Jika instance hanya memiliki IPv6 alamat publik dan tidak ada IPv4 alamat publik, item ini tidak disetel dan menghasilkan respons HTTP 404.	01-01-2011

Kategori	Deskripsi	Versi ketika kategori dirilis
`network/interfaces/macs/mac/public-ipv4s`	Alamat IP publik atau alamat IP Elastis yang terkait dengan antarmuka. Mungkin ada beberapa IPv4 alamat pada sebuah instance.	01-01-2011
`network/interfaces/macs/mac/security-groups`	Grup keamanan yang memiliki antarmuka jaringan.	01-01-2011
`network/interfaces/macs/mac/security-group-ids`	Grup keamanan tempat antarmuka jaringan berada. IDs	01-01-2011
`network/interfaces/macs/mac/subnet-id`	ID subnet tempat antarmuka berada.	01-01-2011
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	Blok IPv4 CIDR dari subnet tempat antarmuka berada.	01-01-2011
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	Blok IPv6 CIDR dari subnet tempat antarmuka berada.	30/06/2016
`network/interfaces/macs/mac/vpc-id`	ID VPC tempat antarmuka berada.	01-01-2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	Blok IPv4 CIDR utama dari VPC.	01-01-2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	Blok IPv4 CIDR untuk VPC.	30/06/2016

Kategori	Deskripsi	Versi ketika kategori dirilis
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	Blok IPv6 CIDR dari VPC tempat antarmuka berada.	30/06/2016
`placement/availability-zone`	Zona Ketersediaan tempat instans diluncurkan.	01/02/2008
`placement/availability-zone-id`	ID Zona Ketersediaan statis tempat instans diluncurkan. ID Zona Ketersediaan konsisten di semua akun. Namun, ini mungkin berbeda dari Zona Ketersediaan, yang dapat berbeda tergantung pada akun.	01/10/2019
`placement/group-name`	Nama grup penempatan tempat instans diluncurkan.	24/08/2020
`placement/host-id`	ID host tempat instans diluncurkan. Hanya berlaku untuk Host Khusus.	24/08/2020
`placement/partition-number`	Jumlah partisi tempat instans diluncurkan.	24/08/2020
`placement/region`	AWS Wilayah di mana instance diluncurkan.	24/08/2020
`product-codes`	AWS Marketplace kode produk yang terkait dengan instance, jika ada.	01/03/2007

Kategori	Deskripsi	Versi ketika kategori dirilis
`public-hostname`	DNS publik instans (IPv4). Kategori ini hanya ditampilkan jika atribut `enableDnsHostnames` diatur ke `true`. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda dalam Panduan Pengguna Amazon VPC. Jika instance hanya memiliki IPv6 alamat publik dan tidak ada IPv4 alamat publik, item ini tidak disetel dan menghasilkan respons HTTP 404.	19/01/2007
`public-ipv4`	IPv4 Alamat publik. Jika alamat IP Elastis dikaitkan dengan instans, nilai yang ditampilkan adalah alamat IP Elastis.	19/01/2007
`public-keys/0/openssh-key`	Kunci publik. Hanya tersedia jika disediakan pada waktu peluncuran instans.	1.0
`ramdisk-id`	ID dari RAM disk ditentukan pada waktu peluncuran, jika ada.	10/10/2007
`reservation-id`	ID reservasi.	1.0

Kategori	Deskripsi	Versi ketika kategori dirilis
`security-groups`	Nama-nama grup keamanan yang diterapkan ke instans. Setelah peluncuran, Anda dapat mengubah grup keamanan instans. Perubahan tersebut tercermin di sini dan dinetwork /interfaces/macs/*`mac`*/security-groups.	1.0
`services/domain`	Domain untuk AWS sumber daya untuk Wilayah.	25/02/2014
`services/partition`	Partisi tempat sumber daya berada. Untuk AWS Wilayah standar, partisi adalah`aws`. Jika Anda memiliki sumber daya di partisi lain, maka partisi-nya adalah `aws-`*`partitionname`* . Contohnya, partisi untuk sumber daya di Wilayah Tiongkok (Beijing) adalah `aws-cn`.	20/10/2015
`spot/instance-action`	Tindakan (hibernasi, berhenti, atau berakhir) dan perkiraan waktu, dalam UTC, saat tindakan akan terjadi. Item ini ada hanya jika Instans Spot telah ditandai untuk hibernasi, berhenti, atau berakhir. Untuk informasi selengkapnya, lihat instance-action.	15/11/2016

Kategori	Deskripsi	Versi ketika kategori dirilis
`spot/termination-time`	Perkiraan waktu, dalam UTC, sistem operasi untuk Instans Spot Anda akan menerima sinyal shutdown. Item ini ada dan berisi nilai waktu (misalnya, 2015-01-05T18: 02: 00Z) hanya jika Instans Spot telah ditandai untuk penghentian oleh Amazon EC2. Item waktu pengakhiran tidak diatur ke suatu waktu jika Anda sendiri mengakhiri Instans Spot. Untuk informasi selengkapnya, lihat termination-time.	05/11/2014
`system`	Jenis virtualisasi yang mendasari (hypervisor) dari instance.	2022-09-24
`tags/instance`	Tanda instans yang terkait dengan instans. Hanya tersedia jika Anda secara eksplisit mengizinkan akses ke tanda dalam metadata instans. Untuk informasi selengkapnya, lihat Aktifkan akses ke tag dalam metadata contoh.	2021-03-23

Kategori data dinamis

Tabel berikut mencantumkan kategori data dinamis.

Kategori	Deskripsi	Versi ketika kategori dirilis
`fws/instance-monitoring`	Nilai yang menunjukkan apakah pelanggan telah mengaktifkan pemantauan satu menit secara terperinci CloudWatch. Nilai yang valid: `enabled | disabled`	04/04/2009
`instance-identity/document`	JSON berisi atribut instans, seperti instance-id, alamat IP privat, dll. Lihat Dokumen identitas instans untuk EC2 instans Amazon.	04/04/2009
`instance-identity/pkcs7`	Digunakan untuk memverifikasi keaslian dokumen dan konten terhadap tanda tangan. Lihat Dokumen identitas instans untuk EC2 instans Amazon.	04/04/2009
`instance-identity/signature`	Data yang dapat digunakan pihak lain untuk memverifikasi asal dan keasliannya. Lihat Dokumen identitas instans untuk EC2 instans Amazon.	04/04/2009

Akses metadata instans untuk instans EC2

Anda dapat mengakses metadata instans EC2 dari dalam instans itu sendiri atau dari konsol EC2, API, SDKs atau. AWS CLI Untuk mendapatkan pengaturan metadata instance saat ini untuk instance dari konsol atau baris perintah, lihat. Mengueri opsi metadata instans untuk instans yang ada

Anda juga dapat memodifikasi data pengguna untuk instance dengan volume root EBS. Instans harus berada dalam status berhenti. Untuk petunjuk konsol, lihat Perbarui data pengguna instance. Untuk contoh Linux yang menggunakan AWS CLI, lihat modify-instance-attribute. Untuk contoh Windows yang menggunakan Alat untuk Windows PowerShell, lihatthe section called “Data pengguna dan Alat untuk Windows PowerShell”.

> **Note**
>
> Anda tidak dikenai biaya untuk permintaan HTTP yang digunakan untuk mengambil metadata instans dan data pengguna.

Pertimbangan akses metadata instance

Untuk menghindari masalah dengan metadata instance, pertimbangkan hal berikut.

Kegagalan peluncuran instans karena IMDSv2 penegakan (**`HttpTokensEnforced=enabled`**)

Sebelum mengaktifkan IMDSv2 penegakan hukum, Anda memerlukan semua perangkat lunak Anda pada instans untuk mendukung IMDSv2, setelah itu Anda dapat mengubah default untuk menonaktifkan IMDSv1 (`httpTokens=required`), setelah itu Anda dapat mengaktifkan penegakan hukum. Untuk informasi selengkapnya, lihat Transisi ke penggunaan Layanan Metadata Instans Versi 2.

Format perintah

Format perintah berbeda, tergantung pada apakah Anda menggunakan Instance Metadata Service Version 1 (IMDSv1) atau Instance Metadata Service Version 2 (). IMDSv2 Secara default, Anda dapat menggunakan kedua versi Layanan Metadata Instans. Untuk membutuhkan penggunaanIMDSv2 , LihatGunakan Layanan Metadata Instance untuk mengakses metadata instans .

Jika IMDSv2 diperlukan, IMDSv1 tidak berfungsi

Jika Anda menggunakan IMDSv1 dan tidak menerima tanggapan, kemungkinan itu IMDSv2 diperlukan. Untuk memeriksa apakah IMDSv2 diperlukan, pilih instance untuk melihat detailnya. IMDSv2Nilai menunjukkan baik Diperlukan (Anda harus menggunakan IMDSv2) atau Opsional (Anda dapat menggunakan salah satu IMDSv2 atauIMDSv1).

(IMDSv2) Gunakan /latest/api/token untuk mengambil token

Menerbitkan PUT permintaan ke jalur khusus versi apa pun, misalnya`/2021-03-23/api/token`, menghasilkan layanan metadata yang mengembalikan 403 kesalahan Terlarang. Perilaku ini memang disengaja.

Versi metadata

Untuk menghindari keharusan memperbarui kode Anda setiap kali Amazon EC2 merilis build metadata instans baru, sebaiknya gunakan `latest` di jalur, dan bukan nomor versi.

IPv6 dukungan

Untuk mengambil metadata instance menggunakan IPv6 alamat, pastikan Anda mengaktifkan dan menggunakan IPv6 alamat IMDS `[fd00:ec2::254]` alih-alih alamatnya. IPv4 `169.254.169.254` Instance harus berupa instance berbasis Nitro yang diluncurkan di subnet yang mendukung. IPv6

(Windows) Buat kustom AMIs menggunakan Windows Sysprep

Untuk memastikan bahwa IMDS berfungsi saat Anda meluncurkan instance dari AMI Windows kustom, AMI harus berupa gambar standar yang dibuat dengan Windows Sysprep. Jika tidak, IMDS tidak akan bekerja. Untuk informasi selengkapnya, lihat Buat Amazon EC2 AMI menggunakan Windows Sysprep.

Di lingkungan kontainer, pertimbangkan konfigurasi ulang atau tingkatkan batas hop menjadi 2

IMDSv2 Panggilan AWS SDKs penggunaan secara default. Jika IMDSv2 panggilan tidak menerima respons, beberapa AWS SDKs mencoba lagi panggilan dan, jika masih tidak berhasil, gunakan. IMDSv1 Hal ini dapat mengakibatkan penundaan, terutama di lingkungan kontainer. Bagi mereka AWS SDKs yang membutuhkan IMDSv2, jika batas hop adalah 1 di lingkungan kontainer, panggilan mungkin tidak menerima respons sama sekali karena pergi ke wadah dianggap sebagai hop jaringan tambahan.

Untuk mengurangi masalah ini di lingkungan kontainer, pertimbangkan untuk mengubah konfigurasi untuk meneruskan pengaturan (seperti AWS Region) langsung ke wadah, atau pertimbangkan untuk meningkatkan batas hop menjadi 2. Untuk informasi tentang dampak batas hop, lihat Menambahkan pertahanan secara mendalam terhadap firewall terbuka, proxy terbalik, dan kerentanan SSRF dengan penyempurnaan pada Layanan Metadata Instans EC2. Untuk informasi tentang mengubah batas hop, lihatMengubah batas hop respons PUT.

Batas paket per detik (PPS)

Ada batas 1024 paket per detik (PPS) untuk layanan yang menggunakan alamat link-lokal. Batas ini mencakup agregat Kueri DNS Route 53 Resolver, permintaan Layanan Metadata Instans (IMDS), permintaan Amazon Time Service Network Time Protocol (NTP), dan permintaan Layanan Lisensi Windows (untuk instance berbasis Microsoft Windows).

Pertimbangan tambahan untuk akses data pengguna

- Data pengguna diperlakukan sebagai data buram: apa yang Anda tentukan adalah apa yang Anda dapatkan kembali setelah pengambilan. Terserah instance untuk menafsirkan dan bertindak berdasarkan data pengguna.
- Data pengguna harus dienkode base64. Bergantung pada alat atau SDK yang Anda gunakan, pengkodean base64 mungkin dilakukan untuk Anda. Contoh:
  - Konsol Amazon EC2 dapat mengenkode base64 untuk Anda atau menerima input yang dienkode base64.

  - AWS CLI versi 2 melakukan pengkodean parameter biner base64 untuk Anda secara default. AWS CLI versi 1 melakukan pengkodean `--user-data` base64-parameter untuk Anda.
  - AWS SDK for Python (Boto3) Melakukan pengkodean `UserData` base64-parameter untuk Anda.
- Data pengguna dibatasi hingga 16 KB, dalam bentuk mentah, sebelum dienkode base64. Ukuran string dengan panjang n setelah enkode base64 adalah ceil(n/3)*4.
- Data pengguna harus didekode base64 saat Anda mengambilnya. Jika Anda mengambil data menggunakan metadata instans atau konsol, data akan didekode untuk Anda secara otomatis.
- Jika Anda menghentikan sebuah instans, mengubah data penggunanya, dan memulai instans, data pengguna yang diperbarui tidak akan dijalankan secara otomatis saat Anda memulai instans. Dengan instance Windows, Anda dapat mengonfigurasi pengaturan sehingga skrip data pengguna yang diperbarui dijalankan satu kali ketika Anda memulai instance atau setiap kali Anda reboot atau memulai instance.
- Data pengguna adalah atribut instans. Jika Anda membuat AMI dari instans, data pengguna instans tidak disertakan dalam AMI.

Akses metadata instans dari dalam instans EC2

Karena metadata instans Anda tersedia dari instans berjalan, Anda tidak perlu menggunakan konsol Amazon EC2 atau AWS CLI. Hal ini berguna saat Anda menulis skrip yang akan dijalankan dari instans Anda. Misalnya, Anda dapat mengakses alamat IP lokal instans Anda dari metadata instans untuk mengelola koneksi ke aplikasi eksternal.

Semua hal berikut dianggap metadata contoh, tetapi mereka diakses dengan cara yang berbeda. Pilih tab yang mewakili jenis metadata instance yang ingin Anda akses untuk melihat informasi selengkapnya.

Metadata

Properti metadata instance dibagi menjadi beberapa kategori. Untuk deskripsi setiap kategori metadata instans, lihat Kategori metadata instans.

Untuk mengakses properti metadata instance dari dalam instance yang sedang berjalan, dapatkan data dari berikut IPv4 atau. IPv6 URIs Alamat IP ini adalah alamat link-lokal dan hanya valid dari instance. Untuk informasi selengkapnya, lihat Alamat link-lokal.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Dynamic data

Untuk mengambil data dinamis dari dalam instance yang sedang berjalan, gunakan salah satu dari berikut URIs ini.

IPv4

```
http://169.254.169.254/latest/dynamic/
```

IPv6

```
http://[fd00:ec2::254]/latest/dynamic/
```

Contoh: Akses dengan cURL

Contoh berikut digunakan cURL untuk mengambil kategori identitas instance tingkat tinggi.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
```

```
document
signature
dsa2048
```

Contoh: Akses dengan PowerShell

Contoh berikut digunakan PowerShell untuk mengambil kategori identitas instance tingkat tinggi.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Untuk informasi lebih lanjut tentang data dinamis dan contoh cara mengambilnya, lihat Dokumen identitas instans untuk EC2 instans Amazon.

User data

Untuk mengambil data pengguna dari sebuah instance, gunakan salah satu dari berikut URIs ini. Untuk mengambil data pengguna menggunakan IPv6 alamat, Anda harus mengaktifkannya, dan instance harus berupa instance berbasis Nitro di subnet yang mendukung. IPv6

IPv4

```
http://169.254.169.254/latest/user-data
```

IPv6

```
http://[fd00:ec2::254]/latest/user-data
```

Permintaan untuk data pengguna mengembalikan data apa adanya (tipe konten `application/octet-stream`). Jika instans tidak memiliki data pengguna, permintaan akan mengembalikan `404 - Not Found`.

Contoh: Akses dengan cURL untuk mengambil teks yang dipisahkan koma

Contoh berikut digunakan `cURL` untuk mengambil data pengguna yang ditetapkan sebagai teks yang dipisahkan koma.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Contoh: Akses dengan PowerShell untuk mengambil teks yang dipisahkan koma

Contoh berikut digunakan PowerShell untuk mengambil data pengguna yang ditetapkan sebagai teks yang dipisahkan koma.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod -Headers
 @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Contoh: Akses dengan cURL untuk mengambil skrip

Contoh berikut digunakan cURL untuk mengambil data pengguna yang ditentukan sebagai skrip.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Contoh: Akses dengan PowerShell untuk mengambil skrip

Contoh berikut digunakan PowerShell untuk mengambil data pengguna yang ditentukan sebagai skrip.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/user-data
```

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Mengueri opsi metadata instans untuk instans yang ada

Anda dapat menanyakan opsi metadata instans untuk instans yang ada.

Console

Untuk menanyakan opsi metadata instance untuk instance yang ada

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih contoh Anda dan periksa bidang berikut:
   - IMDSv2— Nilai adalah Wajib atau Opsional.
   - Izinkan tag dalam metadata contoh - Nilainya Diaktifkan atau Dinonaktifkan.
4. Dengan instans yang dipilih, pilih Actions, Instance settings, Modify instance metadata options.

   Kotak dialog menampilkan apakah layanan metadata instance diaktifkan atau dinonaktifkan untuk instance yang dipilih.

AWS CLI

Untuk menanyakan opsi metadata instance untuk instance yang ada

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Untuk menanyakan opsi metadata instance untuk instance yang ada menggunakan Tools for PowerShell

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Respons dan pesan kesalahan

Semua metadata instans ditampilkan sebagai teks (tipe konten HTTP `text/plain`).

Permintaan untuk sumber daya metadata tertentu mengembalikan nilai yang sesuai, atau kode kesalahan HTTP `404 - Not Found` jika sumber daya tidak tersedia.

Permintaan untuk sumber daya metadata umum (URI diakhiri dengan a /) mengembalikan daftar sumber daya yang tersedia, atau kode kesalahan HTTP `404 - Not Found` jika tidak ada sumber daya seperti itu. Item daftar berada di baris terpisah, diakhiri oleh feed baris (ASCII 10).

Jika IMDSv1 permintaan tidak menerima tanggapan, kemungkinan itu IMDSv2 diperlukan.

Untuk permintaan yang dibuat menggunakan IMDSv2, kode kesalahan HTTP berikut dapat dikembalikan:

- `400 - Missing or Invalid Parameters` – Permintaan PUT tidak valid.
- `401 - Unauthorized` – Permintaan GET menggunakan token yang tidak valid. Tindakan yang disarankan adalah membuat token baru.
- `403 - Forbidden` – Permintaan tidak diperbolehkan atau IMDS dimatikan.
- `404 - Not Found`— Sumber daya tidak tersedia atau tidak ada sumber daya seperti itu.
- `503`— Permintaan tidak dapat diselesaikan. Coba lagi permintaannya.

Jika IMDS mengembalikan kesalahan, curl mencetak pesan kesalahan dalam output dan mengembalikan kode status sukses. Pesan kesalahan disimpan dalam `TOKEN` variabel, yang menyebabkan curl perintah yang menggunakan token gagal. Jika Anda memanggil curl dengan `-f` opsi, ia mengembalikan kode status kesalahan jika terjadi kesalahan server HTTP. Jika Anda mengaktifkan penanganan kesalahan, shell dapat menangkap kesalahan dan menghentikan skrip.

Throttling kueri

Kami membatasi kueri ke IMDS per instans, dan kami membatasi jumlah koneksi simultan dari sebuah instans ke IMDS.

Jika Anda menggunakan IMDS untuk mengambil kredensil AWS keamanan, hindari kueri kredensil selama setiap transaksi atau secara bersamaan dari sejumlah besar thread atau proses, karena hal ini dapat menyebabkan pembatasan. Sebagai gantinya, kami menyarankan Anda menyimpan kredensial dalam cache hingga kredensial itu mendekati waktu kedaluwarsanya. Untuk informasi selengkapnya tentang peran IAM dan kredensial keamanan yang terkait dengan peran tersebut, lihat Mengambil kredensial keamanan dari metadata instans.

Jika Anda mengalami throttling saat mengakses IMDS, coba lagi kueri Anda dengan strategi mundur eksponensial.

Gunakan Layanan Metadata Instance untuk mengakses metadata instans

Anda dapat mengakses metadata instans dari instans yang sedang berjalan menggunakan salah satu metode berikut:

- Instance Metadata Service Version 2 (IMDSv2) — metode yang berorientasi pada sesi

  Sebagai contoh, lihat Contoh untuk IMDSv2.
- Layanan Metadata Instance Versi 1 (IMDSv1) — sebuah metode request/response

  Sebagai contoh, lihat Contoh untuk IMDSv1.

Secara default, Anda dapat menggunakan salah satu IMDSv1 atau IMDSv2, atau keduanya.

Anda dapat mengonfigurasi Layanan Metadata Instance (IMDS) pada setiap instance untuk hanya menerima IMDSv2 panggilan, yang akan menyebabkan IMDSv1 panggilan gagal. Untuk informasi tentang cara mengonfigurasi instans yang akan digunakan IMDSv2, lihatKonfigurasikan opsi Layanan Metadata Instance.

GETHeader PUT atau unik untuk IMDSv2. Jika header ini ada dalam permintaan, maka permintaan tersebut dimaksudkan untukIMDSv2. Jika tidak ada header yang hadir, diasumsikan permintaan dimaksudkan untukIMDSv1.

Untuk tinjauan ekstensif IMDSv2, lihat Menambahkan pertahanan secara mendalam terhadap firewall terbuka, proxy terbalik, dan kerentanan SSRF dengan penyempurnaan pada Layanan Metadata Instans EC2.

Topik

- Bagaimana cara kerja Layanan Metadata Instans Versi 2
- Menggunakan AWS SDK yang didukung
- Contoh untuk IMDSv2
- Contoh untuk IMDSv1

Bagaimana cara kerja Layanan Metadata Instans Versi 2

IMDSv2 menggunakan permintaan berorientasi sesi. Dengan permintaan berorientasi sesi, Anda membuat token sesi yang menentukan durasi sesi, yang bisa minimal satu detik dan maksimal enam jam. Selama durasi yang ditentukan, Anda dapat menggunakan token sesi yang sama untuk permintaan selanjutnya. Setelah durasi yang ditentukan berakhir, Anda harus membuat token sesi baru yang akan digunakan untuk permintaan di masa mendatang.

> **Note**
>
> Contoh di bagian ini menggunakan IPv4 alamat Layanan Metadata Instans (IMDS):. `169.254.169.254` Jika Anda mengambil metadata instans untuk instans EC2 melalui IPv6 alamat, pastikan Anda mengaktifkan dan menggunakan alamat sebagai gantinya:. IPv6 `[fd00:ec2::254]` IPv6 Alamat IMDS kompatibel dengan IMDSv2 perintah. IPv6 Alamat hanya dapat diakses pada instance berbasis Nitro di subnet yang IPv6 didukung -(tumpukan ganda atau hanya). IPv6

Contoh berikut menggunakan skrip shell dan IMDSv2 untuk mengambil item metadata instance tingkat atas. Setiap contoh:

- Membuat token sesi yang berlangsung selama enam jam (21.600 detik) menggunakan permintaan PUT

- Menyimpan header token sesi dalam variabel bernama `TOKEN` (instance Linux) atau `token` (instance Windows)
- Meminta item metadata tingkat atas menggunakan token

Contoh Linux

Anda bisa menjalankan dua perintah terpisah, atau menggabungkannya.

Perintah terpisah

Pertama, hasilkan token menggunakan perintah berikut.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
```

Kemudian, gunakan token untuk menghasilkan item metadata tingkat atas dengan menggunakan perintah berikut.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Perintah gabungan

Anda dapat menyimpan token dan menggabungkan perintah. Contoh berikut menggabungkan dua perintah di atas dan menyimpan header token sesi dalam variabel bernama TOKEN.

> **Note**
>
> Jika ada kesalahan dalam membuat token, alih-alih token yang valid, pesan kesalahan akan disimpan dalam variabel, dan perintah tidak akan bekerja.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Setelah Anda membuat token, Anda dapat menggunakannya kembali hingga kedaluwarsa. Dalam contoh perintah berikut, yang mendapatkan ID AMI yang digunakan untuk meluncurkan instans, token yang disimpan di `$TOKEN` dalam contoh sebelumnya digunakan kembali.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Contoh Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Setelah Anda membuat token, Anda dapat menggunakannya kembali hingga kedaluwarsa. Dalam contoh perintah berikut, yang mendapatkan ID AMI yang digunakan untuk meluncurkan instans, token yang disimpan di `$token` dalam contoh sebelumnya digunakan kembali.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
 -Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Ketika Anda menggunakan IMDSv2 untuk meminta metadata instance, permintaan harus menyertakan yang berikut:

1. Gunakan permintaan PUT untuk memulai sesi ke layanan metadata instans. Permintaan PUT mengembalikan sebuah token yang harus disertakan dalam permintaan GET selanjutnya ke layanan metadata instans. Token diperlukan untuk mengakses metadata menggunakan. IMDSv2
2. Sertakan token di semua permintaan GET ke IMDS. Saat penggunaan token diatur ke `required`, permintaan tanpa token yang valid atau dengan token yang kedaluwarsa akan menerima kode kesalahan HTTP `401 - Unauthorized`.
   - Token adalah kunci untuk instans tertentu. Token tidak valid di instans EC2 lainnya dan akan ditolak jika Anda mencoba menggunakannya di luar instans tempatnya dibuat.
   - Permintaan PUT harus menyertakan header yang menentukan waktu hidup (TTL) untuk token, dalam detik, hingga maksimum enam jam (21.600 detik). Token tersebut mewakili sesi logis. TTL menentukan lamanya waktu token itu valid dan, oleh karena itu, merupakan durasi sesi.
   - Setelah token kedaluwarsa, untuk terus mengakses metadata instans, Anda harus membuat sesi baru menggunakan PUT yang lain.
   - Anda dapat memilih untuk menggunakan kembali token atau membuat token baru dengan setiap permintaan. Untuk sejumlah kecil permintaan, mungkin lebih mudah untuk membuat dan

langsung menggunakan token setiap kali Anda perlu mengakses IMDS. Namun, untuk efisiensi, Anda dapat menentukan durasi yang lebih lama untuk token dan menggunakannya kembali daripada harus menulis perimtaan PUT setiap kali Anda perlu meminta metadata instans. Tidak ada batasan praktis pada jumlah token bersamaan, masing-masing mewakili sesinya sendiri. IMDSv2 Namun, masih dibatasi oleh koneksi IMDS normal dan batas pelambatan. Untuk informasi selengkapnya, lihat Throttling kueri.

HTTP GET dan HEAD metode diperbolehkan dalam permintaan metadata IMDSv2 contoh. PUTpermintaan ditolak jika berisi X-Forwarded-For header.

Secara default, respons untuk permintaan PUT memiliki batas hop respons (waktu hidup) sebesar 1 di tingkat protokol IP. Jika Anda membutuhkan batas hop yang lebih besar, Anda dapat menyesuaikannya dengan menggunakan modify-instance-metadata-options AWS CLI perintah. Misalnya, Anda mungkin memerlukan batas hop yang lebih besar untuk kompatibilitas mundur dengan layanan container yang berjalan pada instans. Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans yang ada.

Menggunakan AWS SDK yang didukung

Untuk menggunakan IMDSv2, instans EC2 Anda harus menggunakan versi AWS SDK yang mendukung penggunaan. IMDSv2 Versi terbaru dari semua AWS SDKs dukungan menggunakan IMDSv2.

> **Important**
>
> Kami menyarankan Anda untuk tetap mengikuti kabar terbaru terkait perilisan SDK untuk mendapatkan fitur, pembaruan keamanan, dan dependensi dasar terbaru. Penggunaan berkelanjutan dari versi SDK yang tidak didukung tidak disarankan dan dilakukan sesuai kebijaksanaan Anda. Untuk informasi selengkapnya, lihat kebijakan pemeliharaan AWS SDKs dan Alat di Panduan Referensi Alat AWS SDKs dan.

Berikut ini adalah versi minimum yang mendukung penggunaan IMDSv2:

- AWS CLI – 1.16.289
- AWS Tools for Windows PowerShell – 4.0.1.0
- AWS SDK for .NET – 3.3.634.1
- AWS SDK for C++ – 1.7.229

- AWS SDK for Go – 1.25.38
- AWS SDK for Go v2 - 0.19.0
- AWS SDK for Java – 1.11.678
- AWS SDK for Java 2.x – 2.10.21
- AWS SDK untuk JavaScript di Node.js - 2.722.0
- AWS SDK for Kotlin— 1.1.4
- AWS SDK for PHP – 3.147.7
- AWS SDK untuk Python (Botocore) - 1.13.25
- AWS SDK for Python (Boto3) – 1.12.6
- AWS SDK for Ruby – 3.79.0

Contoh untuk IMDSv2

Jalankan contoh berikut di instans Amazon EC2 Anda untuk mengambil metadata instans. IMDSv2

Pada contoh Windows, Anda dapat menggunakan Windows PowerShell atau Anda dapat menginstal cURL atau wget. Jika Anda menginstal alat pihak ketiga pada instance Windows, pastikan Anda membaca dokumentasi yang menyertainya dengan cermat, karena panggilan dan outputnya mungkin berbeda dari yang dijelaskan di sini.

Contoh

- Dapatkan versi metadata instans yang tersedia
- Dapatkan item metadata tingkat atas
- Dapatkan nilai untuk item metadata
- Dapatkan daftar kunci publik yang tersedia
- Tunjukkan format di mana kunci publik 0 tersedia
- Dapatkan kunci publik 0 (dalam format kunci OpenSSH)
- Dapatkan ID subnet untuk instans
- Dapatkan tanda instans untuk sebuah instans

Dapatkan versi metadata instans yang tersedia

Contoh ini mendapatkan versi metadata instans yang tersedia. Setiap versi mengacu pada build metadata instans jika kategori metadata instans baru dirilis. Versi build metadata instans tidak

berkorelasi dengan versi API Amazon EC2. Versi sebelumnya tersedia untuk Anda jika Anda memiliki skrip yang mengandalkan struktur dan informasi yang ada di versi sebelumnya.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
```

```
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Dapatkan item metadata tingkat atas

Contoh ini mendapatkan item metadata tingkat atas. Untuk informasi selengkapnya tentang item dalam respons, lihatKategori metadata instans.

Perhatikan bahwa tag disertakan dalam output ini hanya jika Anda mengizinkan akses. Untuk informasi selengkapnya, lihat the section called “Aktifkan akses ke tag dalam metadata contoh”.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
```

```
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Dapatkan nilai untuk item metadata

Contoh-contoh ini mendapatkan nilai dari beberapa item metadata tingkat atas yang diperoleh pada contoh sebelumnya. Permintaan ini menggunakan token tersimpan yang dibuat menggunakan perintah dalam contoh sebelumnya. Token tidak boleh kedaluwarsa.

cURL

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Dapatkan daftar kunci publik yang tersedia

Contoh ini mendapatkan daftar kunci publik yang tersedia.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Tunjukkan format di mana kunci publik 0 tersedia

Contoh ini menunjukkan format di mana kunci publik 0 tersedia.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/
openssh-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Dapatkan kunci publik 0 (dalam format kunci OpenSSH)

Contoh ini mendapatkan kunci publik 0 (di format kunci OpenSSH).

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

```
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Dapatkan ID subnet untuk instans

Contoh ini mendapatkan ID subnet untuk sebuah instans.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -
Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Dapatkan tanda instans untuk sebuah instans

Jika akses ke tag instance dalam metadata instance diaktifkan, Anda bisa mendapatkan tag untuk instance dari metadata instance. Untuk informasi selengkapnya, lihat Mengambil tanda dari metadata instans.

Contoh untuk IMDSv1

Jalankan contoh berikut di instans Amazon EC2 Anda untuk mengambil metadata instans. IMDSv1

Pada contoh Windows, Anda dapat menggunakan Windows PowerShell atau Anda dapat menginstal cURL atau wget. Jika Anda menginstal alat pihak ketiga pada instance Windows, pastikan Anda membaca dokumentasi yang menyertainya dengan cermat, karena panggilan dan outputnya mungkin berbeda dari yang dijelaskan di sini.

Contoh

- Dapatkan versi metadata instans yang tersedia
- Dapatkan item metadata tingkat atas
- Dapatkan nilai untuk item metadata
- Dapatkan daftar kunci publik yang tersedia
- Tunjukkan format di mana kunci publik 0 tersedia
- Dapatkan kunci publik 0 (dalam format kunci OpenSSH)
- Dapatkan ID subnet untuk instans
- Dapatkan tanda instans untuk sebuah instans

Dapatkan versi metadata instans yang tersedia

Contoh ini mendapatkan versi metadata instans yang tersedia. Setiap versi mengacu pada build metadata instans jika kategori metadata instans baru dirilis. Versi build metadata instans tidak berkorelasi dengan versi API Amazon EC2. Versi sebelumnya tersedia untuk Anda jika Anda memiliki skrip yang mengandalkan struktur dan informasi yang ada di versi sebelumnya.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/
1.0
2007-01-19
2007-03-01
```

```
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Dapatkan item metadata tingkat atas

Contoh ini mendapatkan item metadata tingkat atas. Untuk informasi selengkapnya tentang item dalam respons, lihatKategori metadata instans.

Perhatikan bahwa tag disertakan dalam output ini hanya jika Anda mengizinkan akses. Untuk informasi selengkapnya, lihat the section called “Aktifkan akses ke tag dalam metadata contoh”.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
```

```
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Dapatkan nilai untuk item metadata

Contoh-contoh ini mendapatkan nilai dari beberapa item metadata tingkat atas yang diperoleh pada contoh sebelumnya.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-
id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-
hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Dapatkan daftar kunci publik yang tersedia

Contoh ini mendapatkan daftar kunci publik yang tersedia.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/ 0=my-public-key
```

Tunjukkan format di mana kunci publik 0 tersedia

Contoh ini menunjukkan format di mana kunci publik 0 tersedia.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
```

```
openssh-key
```

Dapatkan kunci publik 0 (dalam format kunci OpenSSH)

Contoh ini mendapatkan kunci publik 0 (di format kunci OpenSSH).

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Dapatkan ID subnet untuk instans

Contoh ini mendapatkan ID subnet untuk sebuah instans.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Dapatkan tanda instans untuk sebuah instans

Jika akses ke tag instance dalam metadata instance diaktifkan, Anda bisa mendapatkan tag untuk instance dari metadata instance. Untuk informasi selengkapnya, lihat Mengambil tanda dari metadata instans.

Transisi ke penggunaan Layanan Metadata Instans Versi 2

Jika Anda ingin mengonfigurasi instans agar hanya menerima panggilan Layanan Metadata Instans Versi 2 (IMDSv2), sebaiknya gunakan alat dan jalur transisi berikut.

Topik

- Alat untuk transisi ke IMDSv2
- Jalur yang direkomendasikan untuk membutuhkan IMDSv2

Alat untuk transisi ke IMDSv2

Alat-alat berikut dapat membantu Anda mengidentifikasi, memantau, dan mengelola transisi perangkat lunak Anda dari IMDSv1 ke IMDSv2. Untuk petunjuk tentang cara menggunakan alat ini, lihatJalur yang direkomendasikan untuk membutuhkan IMDSv2.

AWS perangkat lunak

Versi terbaru dari AWS CLI dan AWS SDK mendukung IMDSv2. Untuk menggunakan IMDSv2, perbarui instans EC2 Anda untuk menggunakan versi terbaru. Untuk versi AWS SDK minimum yang mendukung IMDSv2, lihatMenggunakan AWS SDK yang didukung.

Semua paket perangkat lunak Amazon Linux 2 dan Amazon Linux 2023 mendukung IMDSv2. Amazon Linux 2023 dinonaktifkan secara IMDSv1 default.

IMDS Package Analyzer

IMDS Packet Analyzer adalah alat sumber terbuka yang mengidentifikasi dan mencatat IMDSv1 panggilan selama fase boot dan operasi runtime instans Anda. Dengan menganalisis log ini, Anda dapat dengan tepat mengidentifikasi perangkat lunak yang membuat IMDSv1 panggilan pada instans Anda dan menentukan apa yang perlu diperbarui untuk mendukung IMDSv2 hanya pada instans Anda. Anda dapat menjalankan IMDS Packet Analyzer dari baris perintah atau menginstalnya sebagai layanan. Untuk informasi lebih lanjut, lihat AWS ImdsPacketAnalyzerdi GitHub.

CloudWatch

CloudWatch menyediakan dua metrik berikut untuk memantau instans Anda:

`MetadataNoToken`— IMDSv2 menggunakan sesi yang didukung token, sementara IMDSv1 tidak. `MetadataNoToken`Metrik melacak jumlah panggilan ke Layanan Metadata Instans (IMDS) yang digunakan. IMDSv1 Dengan melacak metrik ini ke nol, Anda dapat menentukan apakah dan kapan semua perangkat lunak Anda telah ditingkatkan untuk digunakanIMDSv2.

`MetadataNoTokenRejected`— Setelah Anda menonaktifkan IMDSv1, Anda dapat menggunakan `MetadataNoTokenRejected` metrik untuk melacak berapa kali IMDSv1 panggilan dicoba dan ditolak. Dengan melacak metrik ini, Anda dapat memastikan apakah perangkat lunak Anda perlu diperbarui untuk digunakan IMDSv2.

Untuk setiap instans EC2, metrik ini saling eksklusif. Ketika IMDSv1 diaktifkan (`httpTokens = optional`), hanya `MetadataNoToken` memancarkan. Ketika IMDSv1 dinonaktifkan (`httpTokens = required`), hanya `MetadataNoTokenRejected` memancarkan. Untuk kapan menggunakan metrik ini, lihatJalur yang direkomendasikan untuk membutuhkan IMDSv2.

Untuk informasi selengkapnya, lihat Metrik instans.

Peluncuran APIs

Instance baru: Gunakan RunInstancesAPI untuk meluncurkan instance baru yang memerlukan penggunaan. IMDSv2 Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans baru.

Instance yang ada: Gunakan ModifyInstanceMetadataOptionsAPI untuk meminta penggunaan IMDSv2 pada instance yang ada. Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans yang ada.

Instans baru yang diluncurkan oleh grup Auto Scaling: Untuk mewajibkan IMDSv2 penggunaan pada semua instans baru yang diluncurkan oleh grup Auto Scaling, grup Auto Scaling Anda dapat menggunakan templat peluncuran atau konfigurasi peluncuran. Saat Anda membuat template peluncuran atau membuat konfigurasi peluncuran, Anda harus mengonfigurasi `MetadataOptions` parameter agar memerlukan penggunaanIMDSv2. Grup Auto Scaling meluncurkan instans baru menggunakan templat peluncuran atau konfigurasi peluncuran baru, tetapi instans yang ada tidak terpengaruh.

Instance yang ada dalam grup Auto Scaling: Gunakan ModifyInstanceMetadataOptionsAPI untuk meminta penggunaan IMDSv2 pada instance yang ada, atau menghentikan instance dan grup Auto Scaling akan meluncurkan instance pengganti baru dengan setelan opsi metadata instans yang ditentukan dalam templat peluncuran baru atau konfigurasi peluncuran.

AMIs

AMIs dikonfigurasi dengan `ImdsSupport` parameter yang disetel ke `v2.0` akan meluncurkan instance yang membutuhkan secara IMDSv2 default. Amazon Linux 2023 dikonfigurasi dengan`ImdsSupport = v2.0`.

Baru AMIs: Gunakan perintah CLI register-image untuk mengatur parameter `ImdsSupport` `v2.0` saat membuat AMI baru.

AMIsExisting: Gunakan perintah modify-image-attributeCLI untuk mengatur `ImdsSupport` parameter `v2.0` saat memodifikasi AMI yang ada.

Untuk informasi selengkapnya, lihat Konfigurasikan AMI.

Kontrol tingkat akun

Anda dapat mengonfigurasi nilai default untuk semua opsi metadata instans di tingkat akun. Nilai default diterapkan secara otomatis saat Anda meluncurkan sebuah instance. Untuk informasi lebih lanjut. lihat. Tetapkan IMDSv2 sebagai default untuk akun

Anda juga dapat menerapkan persyaratan untuk digunakan IMDSv2 di tingkat akun. Saat IMDSv2 penegakan diaktifkan:

- Instance baru: Instans yang dikonfigurasi untuk diluncurkan dengan IMDSv1 diaktifkan akan gagal diluncurkan
- Instance yang ada dengan IMDSv1 dinonaktifkan: Upaya untuk IMDSv1 mengaktifkan instance yang ada akan dicegah.
- Instance yang ada dengan IMDSv1 diaktifkan: Instance yang ada dengan IMDSv1 sudah diaktifkan tidak akan terpengaruh.

Untuk informasi selengkapnya, lihat Menegakkan IMDSv2 di tingkat akun.

Kebijakan IAM dan SCPs

Anda dapat menggunakan kebijakan IAM atau kebijakan kontrol AWS Organizations layanan (SCP) untuk mengontrol pengguna sebagai berikut:

- Tidak dapat meluncurkan instance menggunakan RunInstancesAPI kecuali instance dikonfigurasi untuk digunakan IMDSv2.
- Tidak dapat memodifikasi instance yang ada menggunakan ModifyInstanceMetadataOptionsAPI untuk mengaktifkan kembaliIMDSv1.

Kebijakan IAM atau SCP harus berisi kunci syarat IAM berikut:

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Jika parameter dalam panggilan API atau CLI tidak cocok dengan status yang ditentukan dalam kebijakan yang berisi kunci kondisi, panggilan API atau CLI gagal dengan respons. `UnauthorizedOperation`

Selain itu, Anda dapat memilih lapisan perlindungan tambahan untuk menegakkan perubahan dari IMDSv1 ke IMDSv2. Pada lapisan manajemen akses sehubungan dengan API yang dipanggil melalui kredensil Peran EC2, Anda dapat menggunakan kunci kondisi baik dalam kebijakan IAM atau kebijakan kontrol AWS Organizations layanan (). SCPs Secara khusus, dengan menggunakan kunci kondisi `ec2:RoleDelivery` dengan nilai `2.0` dalam kebijakan IAM Anda, panggilan API yang dilakukan dengan kredenal Peran EC2 yang diperoleh dari IMDSv1 akan menerima respons. `UnauthorizedOperation` Hal yang sama dapat dicapai secara

lebih luas dengan kondisi yang disyaratkan oleh SCP. Ini memastikan bahwa kredensil yang dikirimkan melalui IMDSv1 tidak dapat benar-benar digunakan untuk memanggil APIs karena panggilan API apa pun yang tidak cocok dengan kondisi yang ditentukan akan menerima kesalahan`UnauthorizedOperation`.

Untuk contoh kebijakan IAM, lihat Cara menggunakan metadata instans. Untuk informasi selengkapnya SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.

Kebijakan Deklaratif

Gunakan Kebijakan Deklaratif (fitur AWS Organizations) untuk menetapkan default akun IMDS secara terpusat, termasuk IMDSv2 penegakan hukum, di seluruh organisasi Anda. Untuk kebijakan contoh, lihat tab Metadata Instans di bagian Kebijakan deklaratif yang didukung di Panduan Pengguna.AWS Organizations

Jalur yang direkomendasikan untuk membutuhkan IMDSv2

Dengan menggunakan alat di atas, kami merekomendasikan jalur berikut untuk transisi ke: IMDSv2

- Langkah 1: Identifikasi instance dengan IMDSv2 =opsional dan penggunaan audit IMDSv1
- Langkah 2: Perbarui perangkat lunak ke IMDSv2
- Langkah 3: Memerlukan IMDSv2 contoh
- Langkah 4: Set IMDSv2 = diperlukan sebagai default
- Langkah 5: Menerapkan instance untuk membutuhkan IMDSv2

Langkah 1: Identifikasi instance dengan IMDSv2 =opsional dan penggunaan audit IMDSv1

Untuk menilai cakupan IMDSv2 migrasi Anda, identifikasi instance yang dikonfigurasi untuk mengizinkan salah satu IMDSv1 atau IMDSv2, dan IMDSv1 panggilan audit.

1. Identifikasi instance yang dikonfigurasi untuk mengizinkan salah satu IMDSv1 atau IMDSv2:

   Amazon EC2 console

   1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
   2. Di panel navigasi, pilih Instans.
   3. Untuk melihat hanya instance yang dikonfigurasi untuk mengizinkan IMDSv1 atau IMDSv2, tambahkan filter IMDSv2 = opsional.

4. Atau, untuk melihat IMDSv2 apakah opsional atau wajib untuk semua instance, buka jendela Preferensi (ikon roda gigi), aktifkan IMDSv2, dan pilih Konfirmasi. Ini menambahkan IMDSv2kolom ke tabel Instances.

AWS CLI

Gunakan perintah describe-instance dan filter dengan`metadata-options.http-tokens = optional`, sebagai berikut:

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --
output text
```

2. IMDSv1 Panggilan audit pada setiap instance:

   Gunakan CloudWatch metrik`MetadataNoToken`. Metrik ini menunjukkan jumlah IMDSv1 panggilan ke IMDS pada instans Anda. Untuk informasi selengkapnya, lihat Metrik instans.

3. Identifikasi perangkat lunak pada instans Anda yang melakukan IMDSv1 panggilan:

   Gunakan IMDS Packet Analyzer open source untuk mengidentifikasi dan mencatat IMDSv1 panggilan selama fase boot dan operasi runtime instans Anda. Gunakan informasi ini untuk mengidentifikasi perangkat lunak yang akan diperbarui agar instance Anda siap digunakan IMDSv2 saja. Anda dapat menjalankan IMDS Packet Analyzer dari baris perintah atau menginstalnya sebagai layanan.

Langkah 2: Perbarui perangkat lunak ke IMDSv2

Perbarui semua SDKs, CLIs, dan perangkat lunak yang menggunakan kredensil Peran pada instans Anda ke IMDSv2 versi yang kompatibel. Untuk informasi selengkapnya tentang memperbarui CLI, lihat Menginstal atau memperbarui ke versi terbaru dari AWS CLIAWS Command Line Interface Panduan Pengguna.

Langkah 3: Memerlukan IMDSv2 contoh

Setelah mengonfirmasi nol IMDSv1 panggilan melalui `MetadataNoToken` metrik, konfigurasikan instans yang ada agar diperlukan IMDSv2. Juga, konfigurasikan semua instance baru untuk membutuhkan IMDSv2. Dengan kata lain, IMDSv1 nonaktifkan semua instance yang ada dan yang baru.

1. Konfigurasikan instance yang ada untuk membutuhkanIMDSv2:

   Amazon EC2 console

   1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
   2. Di panel navigasi, pilih Instans.
   3. Pilih instans Anda.
   4. Pilih Tindakan, Pengaturan instans, Ubah opsi metadata instans.
   5. Untuk IMDSv2, pilih Diperlukan.
   6. Pilih Simpan.

   AWS CLI

   Gunakan perintah modify-instance-metadata-optionsCLI untuk menentukan bahwa hanya IMDSv2 yang akan digunakan.

   > **Note**
   >
   > Anda dapat memodifikasi pengaturan ini pada instance yang sedang berjalan. Perubahan segera berlaku tanpa memerlukan instance restart.

   Untuk informasi selengkapnya, lihat Membutuhkan penggunaan IMDSv2.

2. Pantau masalah setelah menonaktifkanIMDSv1:

   1. Lacak berapa kali IMDSv1 panggilan dicoba dan ditolak dengan `MetadataNoTokenRejected` CloudWatch metrik.
   2. Jika catatan `MetadataNoTokenRejected` metrik IMDSv1 memanggil instance yang mengalami masalah perangkat lunak, ini menunjukkan bahwa perangkat lunak memerlukan pembaruan untuk digunakan IMDSv2.

3. Konfigurasikan instance baru untuk membutuhkanIMDSv2:

   Amazon EC2 console

   1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
   2. Ikuti langkah-langkah untuk meluncurkan instance.

3. Perluas Detail lanjutan, dan untuk versi Metadata, pilih V2 saja (diperlukan token).
4. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans.

   Untuk informasi selengkapnya, lihat Konfigurasikan instans saat peluncuran.

AWS CLI

AWS CLI: Gunakan perintah run-instance dan tentukan yang IMDSv2 diperlukan.

Langkah 4: Set IMDSv2 = diperlukan sebagai default

Anda dapat mengatur IMDSv2 =required sebagai konfigurasi default di tingkat akun atau organisasi. Ini memastikan bahwa semua instance yang baru diluncurkan dikonfigurasi secara otomatis untuk memerlukan IMDSv2.

1. Tetapkan default tingkat akun:

   Amazon EC2 console

   1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
   2. Di panel navigasi, pilih Dasbor.
   3. Pada kartu Atribut akun, di bawah Pengaturan, pilih Perlindungan dan keamanan data.
   4. Di bawah default IMDS, pilih Kelola.
   5. Untuk layanan metadata Instance, pilih Diaktifkan.
   6. Untuk versi Metadata, pilih V2 saja (diperlukan token).
   7. Pilih Perbarui.

   AWS CLI

   Gunakan perintah modify-instance-metadata-defaultsCLI dan tentukan `--http-tokens required` dan. `--http-put-response-hop-limit 2`

   Untuk informasi selengkapnya, lihat Tetapkan IMDSv2 sebagai default untuk akun.
2. Atau, tetapkan default tingkat organisasi menggunakan Kebijakan Deklaratif:

Gunakan Kebijakan Deklaratif untuk menyetel default organisasi IMDSv2 menjadi required. Untuk kebijakan contoh, lihat tab Metadata Instans di bagian Kebijakan deklaratif yang didukung di Panduan Pengguna.AWS Organizations

Langkah 5: Menerapkan instance untuk membutuhkan IMDSv2

Setelah Anda mengonfirmasi bahwa tidak ada ketergantungan IMDSv1 pada instans mana pun, kami sarankan Anda menerapkan IMDSv2 semua instans baru.

Gunakan salah satu opsi berikut untuk menegakkan IMDSv2:

1. Menegakkan IMDSv2 dengan properti akun

   Anda dapat menerapkan penggunaan IMDSv2 di tingkat akun untuk masing-masing AWS Region. Saat diberlakukan, instance hanya dapat diluncurkan jika dikonfigurasi untuk membutuhkan. IMDSv2 Penegakan ini berlaku terlepas dari bagaimana instans atau AMI dikonfigurasi. Untuk informasi selengkapnya, lihat Menegakkan IMDSv2 di tingkat akun. Untuk menerapkan setelan ini di tingkat organisasi, tetapkan Kebijakan Deklaratif. Untuk kebijakan contoh, lihat tab Metadata Instans di bagian Kebijakan deklaratif yang didukung di Panduan Pengguna.AWS Organizations

   Untuk mencegah pembalikan penegakan hukum, Anda harus menggunakan kebijakan IAM untuk mencegah akses ke API. ModifyInstanceMetadataDefaults Untuk informasi selengkapnya, lihat Gunakan kebijakan IAM.

   > **Note**
   >
   > Pengaturan ini tidak mengubah versi IMDS dari instans yang ada, tetapi memblokir pengaktifan IMDSv1 pada instance yang ada yang saat ini telah dinonaktifkan. IMDSv1

   > **Warning**
   >
   > Jika IMDSv2 penegakan `httpTokens` diaktifkan dan tidak disetel ke `required` konfigurasi instans saat peluncuran, pengaturan akun, atau konfigurasi AMI, peluncuran instance akan gagal. Untuk informasi pemecahan masalah, lihat Meluncurkan instance IMDSv1 -enabled gagal.

2. Atau, terapkan IMDSv2 dengan menggunakan kunci kondisi IAM atau SCP berikut:

- `ec2:MetadataHttpTokens`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpEndpoint`

Tombol kondisi ini mengontrol penggunaan RunInstancesdan ModifyInstanceMetadataOptions APIs dan yang sesuai CLIs. Jika kebijakan dibuat, dan parameter dalam panggilan API tidak cocok dengan status yang ditentukan dalam kebijakan menggunakan kunci syarat, panggilan API atau CLI akan gagal dengan tanggapan`UnauthorizedOperation`.

Misalnya kebijakan IAM, lihat .Cara menggunakan metadata instans

Batasi akses ke Layanan Metadata Instance

Anda dapat mempertimbangkan untuk menggunakan aturan firewall lokal untuk menonaktifkan akses dari beberapa atau semua proses ke Layanan Metadata Instans (IMDS).

Untuk instance berbasis NITRO, IMDS dapat dijangkau dari jaringan Anda sendiri ketika alat jaringan dalam VPC Anda, seperti router virtual, meneruskan paket ke alamat IMDS, dan pemeriksaan sumber/tujuan default pada instance dinonaktifkan. Untuk mencegah sumber dari luar VPC Anda mencapai IMDS, kami sarankan Anda memodifikasi konfigurasi alat jaringan untuk menjatuhkan paket dengan IPv4 alamat tujuan IMDS `169.254.169.254` dan, jika Anda mengaktifkan IPv6 titik akhir, alamat IMDS. IPv6 `[fd00:ec2::254]`

Batasi akses IMDS untuk instance Linux

Menggunakan iptables untuk membatasi akses

Contoh berikut menggunakan iptables Linux dan modul `owner` untuk mencegah server web Apache (berdasarkan ID pengguna instalasi default `apache`) mengakses 169.254.169.254. Ini menggunakan aturan penolakan untuk menolak semua permintaan metadata instance (apakah IMDSv1 atau IMDSv2) dari proses apa pun yang berjalan sebagai pengguna tersebut.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

Atau, Anda dapat mempertimbangkan untuk hanya mengizinkan akses ke pengguna atau grup tertentu, dengan menggunakan aturan izin. Aturan izinkan mungkin lebih mudah dikelola dari perspektif keamanan, karena aturan tersebut mengharuskan Anda membuat keputusan tentang

perangkat lunak apa yang memerlukan akses ke metadata instans. Jika Anda menggunakan aturan izin, kecil kemungkinannya Anda secara tidak sengaja mengizinkan perangkat lunak mengakses layanan metadata (yang tidak Anda inginkan untuk mempunyai akses) jika nanti Anda mengubah perangkat lunak atau konfigurasi pada sebuah instans. Anda juga dapat menggabungkan penggunaan grup dengan aturan izin, sehingga Anda dapat menambahkan dan menghapus pengguna dari grup yang diizinkan tanpa perlu mengubah aturan firewall.

Contoh berikut mencegah akses ke IMDS oleh semua proses, kecuali untuk proses yang berjalan di akun pengguna `trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Untuk menggunakan aturan firewall lokal, Anda perlu menyesuaikan perintah contoh sebelumnya agar sesuai dengan kebutuhan Anda.
> - Secara default, aturan iptables tidak persisten di seluruh boot ulang sistem. Aturan itu dapat dibuat persisten dengan menggunakan fitur OS, yang tidak dijelaskan di sini.
> - Modul `owner` iptables hanya cocok dengan keanggotaan grup jika grup tersebut adalah grup utama dari pengguna lokal tertentu. Grup lain tidak cocok.

Menggunakan PF atau IPFW untuk membatasi akses

Jika Anda menggunakanFreeBSD atauOpenBSD , Anda juga dapat mempertimbangkan untuk menggunakan PF atau IPFW. Contoh berikut membatasi akses ke IMDS hanya untuk pengguna root.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> Urutan perintah PF dan IPFW penting. PF default ke aturan pencocokan terakhir dan IPFW default ke aturan pencocokan pertama.

Batasi akses IMDS untuk instance Windows

Menggunakan firewall Windows untuk membatasi akses

PowerShell Contoh berikut menggunakan firewall Windows bawaan untuk mencegah server web Server Informasi Internet (berdasarkan ID pengguna instalasi defaultNT AUTHORITY\IUSR) mengakses 169.254.169.254. Ini menggunakan aturan penolakan untuk menolak semua permintaan metadata instance (apakah IMDSv1 atauIMDSv2) dari proses apa pun yang berjalan sebagai pengguna tersebut.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Atau, Anda dapat mempertimbangkan untuk hanya mengizinkan akses ke pengguna atau grup tertentu, dengan menggunakan aturan izin. Aturan izinkan mungkin lebih mudah dikelola dari perspektif keamanan, karena aturan tersebut mengharuskan Anda membuat keputusan tentang perangkat lunak apa yang memerlukan akses ke metadata instans. Jika Anda menggunakan aturan izin, kecil kemungkinannya Anda secara tidak sengaja mengizinkan perangkat lunak mengakses layanan metadata (yang tidak Anda inginkan untuk mempunyai akses) jika nanti Anda mengubah perangkat lunak atau konfigurasi pada sebuah instans. Anda juga dapat menggabungkan penggunaan grup dengan aturan izin, sehingga Anda dapat menambahkan dan menghapus pengguna dari grup yang diizinkan tanpa perlu mengubah aturan firewall.

Contoh berikut mencegah akses ke metadata instans oleh semua proses yang berjalan sebagai grup OS yang ditentukan dalam variabel `blockPrincipal` (dalam contoh ini, grup Windows `Everyone`),

kecuali untuk proses yang ditentukan dalam `exceptionPrincipal` (dalam contoh ini, grup yang bernama `trustworthy-users`). Anda harus menentukan baik menolak maupun mengizinkan pengguna utama karena Windows Firewall, tidak seperti aturan `! --uid-owner trustworthy-user` di iptables Linux, tidak menyediakan mekanisme pintasan untuk mengizinkan hanya pengguna utama (pengguna atau grup) tertentu dengan menolak semua yang lain.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Untuk menggunakan aturan firewall lokal, Anda perlu menyesuaikan perintah contoh sebelumnya agar sesuai dengan kebutuhan Anda.

Menggunakan aturan netsh untuk membatasi akses

Anda dapat mempertimbangkan untuk memblokir semua perangkat lunak menggunakan aturan `netsh`, tetapi itu sangat kurang fleksibel.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

> **Note**
>
> - Untuk menggunakan aturan firewall lokal, Anda perlu menyesuaikan perintah contoh sebelumnya agar sesuai dengan kebutuhan Anda.

- Aturan `netsh` harus disetel dari command prompt yang tinggi, dan tidak dapat diatur untuk menolak atau mengizinkan pengguna utama tertentu.

Konfigurasikan opsi Layanan Metadata Instance

Layanan Metadata Instance (IMDS) berjalan secara lokal pada setiap instans EC2. Opsi metadata instance mengacu pada sekumpulan konfigurasi yang mengontrol aksesibilitas dan perilaku IMDS pada instans EC2.

Anda dapat mengonfigurasi opsi metadata instance berikut pada setiap instance:

Layanan metadata instans (IMDS): | `enabled` `disabled`

Anda dapat mengaktifkan atau menonaktifkan IMDS pada sebuah instance. Saat dinonaktifkan, Anda atau kode apa pun tidak akan dapat mengakses metadata instance pada instance.

IMDS memiliki dua titik akhir pada sebuah instance: IPv4 (`169.254.169.254`) dan IPv6 (`[fd00:ec2::254]`). Saat Anda mengaktifkan IMDS, IPv4 titik akhir diaktifkan secara otomatis. Jika Anda ingin mengaktifkan IPv6 titik akhir, Anda perlu melakukannya secara eksplisit.

IPv6 Titik akhir IMDS: | `enabled` `disabled`

Anda dapat secara eksplisit mengaktifkan titik akhir IPv6 IMDS pada sebuah instance. Saat IPv6 titik akhir diaktifkan, IPv4 titik akhir tetap diaktifkan. IPv6Titik akhir hanya didukung pada instance berbasis Nitro di subnet yang IPv6 didukung (tumpukan ganda atau hanya). IPv6

Versi metadata: | `IMDSv1 or IMDSv2 (token optional)` `IMDSv2 only (token required)`

Saat meminta metadata instance, IMDSv2 panggilan memerlukan token. IMDSv1panggilan tidak memerlukan token. Anda dapat mengonfigurasi instance untuk mengizinkan salah satu IMDSv1 atau IMDSv2 panggilan (di mana token bersifat opsional), atau hanya mengizinkan IMDSv2 panggilan (di mana token diperlukan).

Batas hop respons metadata: — `1` `64`

Batas hop adalah jumlah hop jaringan yang diizinkan untuk dilakukan oleh respons PUT. Anda dapat mengatur batas hop ke minimum 1 dan maksimum64. Dalam lingkungan kontainer, batas lompatan 1 dapat menyebabkan masalah. Untuk informasi tentang cara mengurangi masalah ini, lihat informasi tentang lingkungan kontainer di bawah. Pertimbangan akses metadata instance

Akses ke tag dalam metadata contoh: | `enabled` `disabled`

Anda dapat mengaktifkan atau menonaktifkan akses ke tag instans dari metadata instans. Untuk informasi selengkapnya, lihat Lihat tag untuk instans EC2 Anda menggunakan metadata instans.

Untuk melihat konfigurasi instans saat ini, lihatMengueri opsi metadata instans untuk instans yang ada.

Tempat mengkonfigurasi opsi metadata instance

Opsi metadata instans dapat dikonfigurasi pada tingkat yang berbeda, sebagai berikut:

- Akun — Anda dapat menetapkan nilai default untuk opsi metadata instans di tingkat akun untuk masing-masing. AWS Region Saat instance diluncurkan, opsi metadata instance secara otomatis disetel ke nilai tingkat akun. Anda dapat mengubah nilai-nilai ini saat peluncuran. Nilai default tingkat akun tidak memengaruhi instance yang ada.
- AMI - Anda dapat mengatur `imds-support` parameter `v2.0` saat Anda mendaftar atau memodifikasi AMI. Ketika sebuah instance diluncurkan dengan AMI ini, versi metadata instance secara otomatis diatur ke IMDSv2 dan batas hop diatur ke 2.
- Instance - Anda dapat mengubah semua opsi metadata instance pada instance saat peluncuran, mengesampingkan pengaturan default. Anda juga dapat mengubah opsi metadata instans setelah diluncurkan pada instance yang sedang berjalan atau dihentikan. Perhatikan bahwa perubahan mungkin dibatasi oleh kebijakan IAM atau SCP.

Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans baru dan Mengonfigurasi opsi metadata instans untuk instans yang ada.

Urutan prioritas misalnya opsi metadata

Nilai untuk setiap opsi metadata instance ditentukan pada peluncuran instance, mengikuti urutan prioritas hierarkis. Hirarki, dengan prioritas tertinggi di atas, adalah sebagai berikut:

- Prioritas 1: Konfigurasi instans saat peluncuran - Nilai dapat ditentukan baik dalam template peluncuran atau dalam konfigurasi instance. Nilai apa pun yang ditentukan di sini mengesampingkan nilai yang ditentukan di tingkat akun atau di AMI.
- Prioritas 2: Pengaturan akun - Jika nilai tidak ditentukan pada peluncuran instance, maka itu ditentukan oleh pengaturan tingkat akun (yang ditetapkan untuk masing-masing). AWS Region

Pengaturan tingkat akun menyertakan nilai untuk setiap opsi metadata, atau menunjukkan tidak ada preferensi sama sekali.

- Prioritas 3: Konfigurasi AMI — Jika nilai tidak ditentukan pada peluncuran instance atau pada tingkat akun, maka nilai tersebut ditentukan oleh konfigurasi AMI. Ini hanya berlaku untuk `HttpTokens` dan`HttpPutResponseHopLimit`.

Setiap opsi metadata dievaluasi secara terpisah. Instance dapat dikonfigurasi dengan campuran konfigurasi instans langsung, default tingkat akun, dan konfigurasi dari AMI.

Anda dapat mengubah nilai opsi metadata apa pun setelah diluncurkan pada instance yang berjalan atau dihentikan, kecuali perubahan dibatasi oleh kebijakan IAM atau SCP.

> **Note**
>
> Pengaturan IMDSv2 penegakan tingkat akun dievaluasi setelah urutan prioritas telah menentukan pengaturan IMDS instans. Ketika IMDSv2 penegakan diaktifkan, instance yang diaktifkan dengan IMDSv1 akan gagal. Untuk informasi lebih lanjut tentang penegakan hukum, lihatMenegakkan IMDSv2 di tingkat akun.

> **Warning**
>
> Jika IMDSv2 penegakan diaktifkan dan `httpTokens` belum disetel ke `required` konfigurasi instans saat peluncuran, pengaturan akun, atau konfigurasi AMI, peluncuran Anda akan gagal.

Contoh 1 - Tentukan nilai untuk opsi metadata

Dalam contoh ini, instans EC2 diluncurkan ke Wilayah di mana `HttpPutResponseHopLimit` diatur ke 1 tingkat akun. AMI yang ditentukan telah `ImdsSupport` disetel ke`v2.0`. Tidak ada opsi metadata yang ditentukan langsung pada instance saat peluncuran. Instans diluncurkan dengan opsi metadata berikut:

```
"MetadataOptions": {
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
```

```
    ...
```

Nilai-nilai ini ditentukan sebagai berikut:

- Tidak ada opsi metadata yang ditentukan saat peluncuran: Selama peluncuran instance, nilai spesifik untuk opsi metadata tidak disediakan baik dalam parameter peluncuran instance atau dalam templat peluncuran.
- Pengaturan akun diutamakan berikutnya: Dengan tidak adanya nilai spesifik yang ditentukan saat peluncuran, pengaturan di tingkat akun dalam Wilayah diutamakan. Ini berarti bahwa nilai default yang dikonfigurasi pada tingkat akun diterapkan. Dalam hal ini, `HttpPutResponseHopLimit` diatur ke`1`.
- Pengaturan AMI diutamakan terakhir: Jika tidak ada nilai tertentu yang ditentukan saat peluncuran atau pada tingkat akun untuk `HttpTokens` (versi metadata instance), pengaturan AMI diterapkan. Dalam hal ini, pengaturan AMI `ImdsSupport: v2.0` menentukan yang `HttpTokens` disetel ke`required`. Perhatikan bahwa meskipun pengaturan AMI `ImdsSupport: v2.0` dirancang untuk disetel`HttpPutResponseHopLimit: 2`, pengaturan AMI diganti oleh pengaturan tingkat akun`HttpPutResponseHopLimit: 1`, yang memiliki prioritas lebih tinggi.

Contoh 2 - Tentukan nilai untuk opsi metadata

Dalam contoh ini, instans EC2 diluncurkan dengan pengaturan yang sama seperti pada Contoh 1 sebelumnya, tetapi dengan `HttpTokens` disetel ke `optional` langsung pada instance saat peluncuran. Instans diluncurkan dengan opsi metadata berikut:

```
"MetadataOptions": {
    ...
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

Nilai untuk `HttpPutResponseHopLimit` ditentukan dengan cara yang sama seperti pada Contoh 1. Namun, nilai untuk `HttpTokens` ditentukan sebagai berikut: Opsi metadata yang dikonfigurasi pada instance saat peluncuran diutamakan terlebih dahulu. Meskipun AMI dikonfigurasi dengan `ImdsSupport: v2.0` (dengan kata lain, `HttpTokens` disetel ke`required`), nilai yang ditentukan pada instance saat peluncuran (`HttpTokens`disetel ke`optional`) diutamakan.

Contoh 3 - Tentukan nilai untuk opsi metadata dengan diaktifkan HttpTokensEnforced

Dalam contoh ini, akun di Wilayah memiliki `HttpTokens = required` dan`HttpTokensEnforced = enabled`.

Pertimbangkan upaya peluncuran instans EC2 berikut:

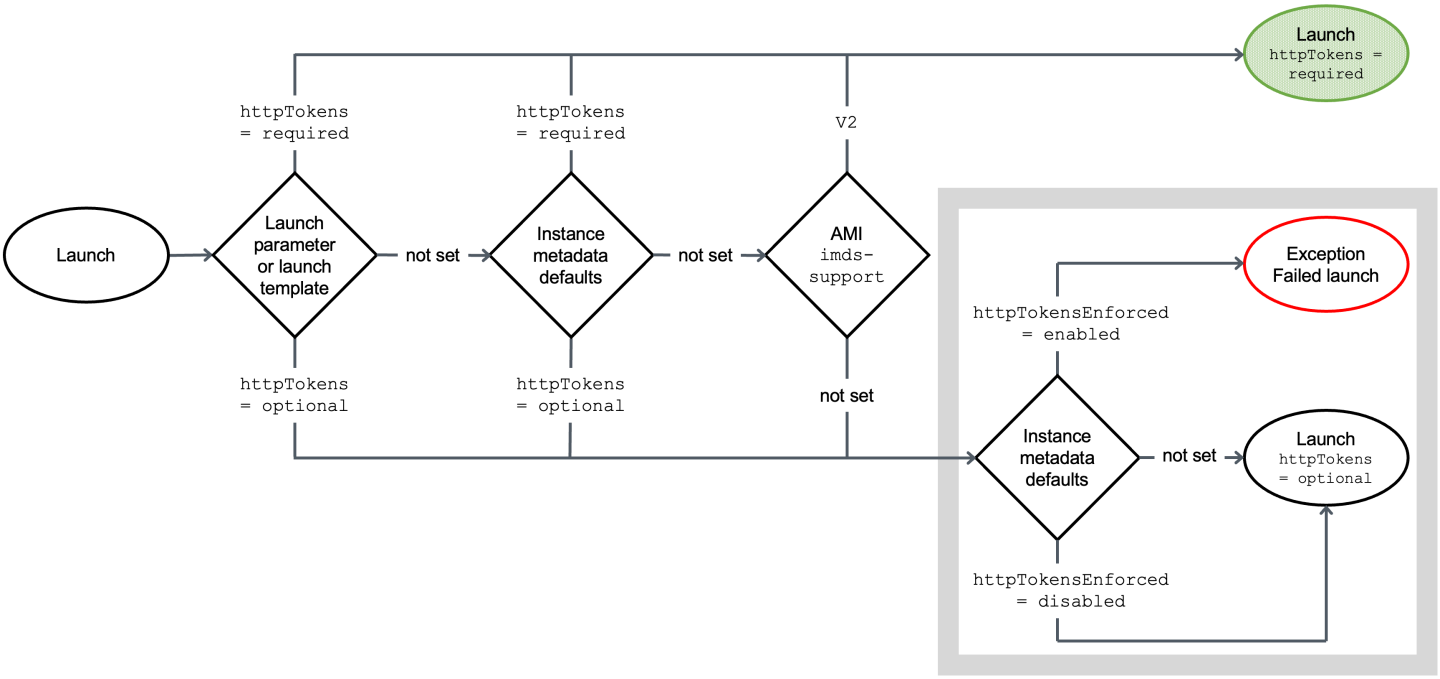
- Upaya peluncuran dengan `HttpTokens` set to `optional` — Peluncuran gagal karena penegakan tingkat akun diaktifkan (`HttpTokensEnforced = enabled`) dan parameter peluncuran lebih diutamakan daripada default akun.
- Upaya peluncuran dengan `HttpTokens` set to `required` — Peluncuran berhasil karena sesuai dengan penegakan tingkat akun.
- Upaya peluncuran tanpa `HttpTokens` nilai yang ditentukan - Peluncuran berhasil karena nilai defaultnya `required` berdasarkan pengaturan akun.

Mengatur versi metadata instance

Saat instance diluncurkan, nilai untuk versi metadata instance adalah IMDSv1 atau IMDSv2 (token optional) (**`httpTokens=optional`**) atau IMDSv2only (token required) (**`httpTokens=required`**).

Saat peluncuran instance, Anda dapat menentukan nilai untuk versi metadata secara manual, atau menggunakan nilai default. Jika Anda menentukan nilainya secara manual, itu akan mengganti default apa pun. Jika Anda memilih untuk tidak menentukan nilai secara manual, itu akan ditentukan oleh kombinasi pengaturan default.

Diagram alur berikut menunjukkan bagaimana versi metadata untuk instans saat peluncuran ditentukan oleh pengaturan pada tingkat konfigurasi yang berbeda dan di mana penegakan dievaluasi. Tabel berikut menyediakan pengaturan spesifik di setiap level.



Tabel menunjukkan bagaimana versi metadata untuk sebuah instance saat peluncuran (ditunjukkan oleh konfigurasi instans yang dihasilkan di kolom 4) ditentukan oleh pengaturan pada tingkat konfigurasi yang berbeda. Urutan prioritas adalah dari kiri ke kanan, di mana kolom pertama diutamakan, sebagai berikut:

- Kolom 1: Parameter peluncuran - Merupakan pengaturan pada instance yang Anda tentukan secara manual saat peluncuran.
- Kolom 2: Tingkat akun default - Merupakan pengaturan untuk akun.
- Kolom 3: AMI default - Merupakan pengaturan pada AMI.

Parameter peluncuran	Default tingkat akun	AMI standar	Konfigurasi instance yang dihasilkan
Hanya V2 (token diperlukan)	Tidak ada preferensi	Hanya V2	Hanya V2
Hanya V2 (token diperlukan)	Hanya V2	Hanya V2	Hanya V2
Hanya V2 (token diperlukan)	V1 atau V2	Hanya V2	Hanya V2

Parameter peluncuran	Default tingkat akun	AMI standar	Konfigurasi instance yang dihasilkan
V1 atau V2 (token opsional)	Tidak ada preferensi	Hanya V2	V1 atau V2
V1 atau V2 (token opsional)	Hanya V2	Hanya V2	V1 atau V2
V1 atau V2 (token opsional)	V1 atau V2	Hanya V2	V1 atau V2
Tidak diatur	Tidak ada preferensi	Hanya V2	Hanya V2
Tidak diatur	Hanya V2	Hanya V2	Hanya V2
Tidak diatur	V1 atau V2	Hanya V2	V1 atau V2
Hanya V2 (token diperlukan)	Tidak ada preferensi	null	Hanya V2
Hanya V2 (token diperlukan)	Hanya V2	null	Hanya V2
Hanya V2 (token diperlukan)	V1 atau V2	null	Hanya V2
V1 atau V2 (token opsional)	Tidak ada preferensi	null	V1 atau V2
V1 atau V2 (token opsional)	Hanya V2	null	V1 atau V2
V1 atau V2 (token opsional)	V1 atau V2	null	V1 atau V2
Tidak diatur	Tidak ada preferensi	null	V1 atau V2
Tidak diatur	Hanya V2	null	Hanya V2

Parameter peluncuran	Default tingkat akun	AMI standar	Konfigurasi instance yang dihasilkan
Tidak diatur	V1 atau V2	null	V1 atau V2

Gunakan kunci kondisi IAM untuk membatasi opsi metadata instans

Anda dapat menggunakan kunci kondisi IAM dalam kebijakan IAM atau SCP sebagai berikut:

- Izinkan instance untuk diluncurkan hanya jika dikonfigurasi untuk memerlukan penggunaan IMDSv2
- Batasi jumlah hop yang diizinkan
- Nonaktifkan akses untuk metadata instans

Tugas

- Mengonfigurasi opsi metadata instans untuk instans baru
- Mengonfigurasi opsi metadata instans untuk instans yang ada

> **Note**
>
> Anda harus melanjutkan dengan hati-hati dan melakukan pengujian yang cermat sebelum membuat perubahan apa pun. Perhatikan hal-hal berikut ini:
>
> - Jika Anda memaksakan penggunaan IMDSv2, aplikasi atau agen yang menggunakan IMDSv1 misalnya akses metadata akan rusak.
> - Jika Anda menonaktifkan semua akses ke metadata instans, aplikasi atau agen yang mengandalkan akses metadata instans ke fungsi akan rusak.
> - Untuk IMDSv2, Anda harus menggunakan `/latest/api/token` saat mengambil token.
> - (Hanya Windows) Jika PowerShell versi Anda lebih awal dari 4.0, Anda harus memperbarui ke Windows Management Framework 4.0 untuk meminta penggunaan IMDSv2.

Mengonfigurasi opsi metadata instans untuk instans baru

Anda dapat mengonfigurasi opsi metadata instance berikut untuk instance baru.

Opsi

- Membutuhkan penggunaan IMDSv2
- Aktifkan IMDS IPv4 dan titik akhir IPv6
- Nonaktifkan akses untuk metadata instans
- Mengizinkan akses ke tanda dalam metadata instans

> **Note**
>
> Pengaturan untuk opsi ini dikonfigurasi di tingkat akun, baik secara langsung di akun atau dengan menggunakan kebijakan deklaratif. Mereka harus dikonfigurasi di setiap AWS Region tempat Anda ingin mengkonfigurasi opsi metadata instance. Menggunakan kebijakan deklaratif memungkinkan Anda menerapkan pengaturan di beberapa Wilayah secara bersamaan, serta di beberapa akun secara bersamaan. Saat kebijakan deklaratif sedang digunakan, Anda tidak dapat mengubah pengaturan secara langsung di dalam akun. Topik ini menjelaskan cara mengonfigurasi pengaturan secara langsung di dalam akun. Untuk informasi tentang penggunaan kebijakan deklaratif, lihat Kebijakan deklaratif di AWS Organizations Panduan Pengguna.

Membutuhkan penggunaan IMDSv2

Anda dapat menggunakan metode berikut untuk meminta penggunaan IMDSv2 pada instance baru Anda.

Untuk membutuhkan IMDSv2

- Tetapkan IMDSv2 sebagai default untuk akun
- Menegakkan IMDSv2 di tingkat akun
- Konfigurasikan instans saat peluncuran
- Konfigurasikan AMI
- Gunakan kebijakan IAM

Tetapkan IMDSv2 sebagai default untuk akun

Anda dapat mengatur versi default untuk layanan metadata instans (IMDS) di tingkat akun untuk masing-masing. AWS Region Ini berarti bahwa ketika Anda meluncurkan instance baru, versi

metadata instans secara otomatis disetel ke default tingkat akun. Namun, Anda dapat mengganti nilai secara manual saat peluncuran atau setelah peluncuran. Untuk informasi selengkapnya tentang bagaimana pengaturan tingkat akun dan penggantian manual memengaruhi instance, lihat. Urutan prioritas misalnya opsi metadata

> **Note**
>
> Menyetel default tingkat akun tidak mengatur ulang instance yang ada. Misalnya, jika Anda menyetel default tingkat akun ke IMDSv2, semua instance yang ada yang disetel ke tidak IMDSv1 terpengaruh. Jika Anda ingin mengubah nilai pada instance yang ada, Anda harus secara manual mengubah nilai pada instance itu sendiri.

Anda dapat mengatur default akun untuk versi metadata instans IMDSv2 agar semua instance baru di akun diluncurkan dengan IMDSv2 required, dan IMDSv1 akan dinonaktifkan. Dengan default akun ini, saat Anda meluncurkan instance, berikut ini adalah nilai default untuk instance:

- Konsol: Versi metadata diatur ke V2 saja (diperlukan token) dan batas hop respons Metadata diatur ke 2.
- AWS CLI: `HttpTokens` diatur ke `required` dan `HttpPutResponseHopLimit` diatur ke2.

> **Note**
>
> Sebelum menyetel default akun IMDSv2, pastikan instans Anda tidak bergantung pada IMDSv1. Untuk informasi selengkapnya, lihat Jalur yang direkomendasikan untuk membutuhkan IMDSv2.

Console

Untuk menetapkan IMDSv2 sebagai default untuk akun untuk Wilayah yang ditentukan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Untuk mengubah AWS Region, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Di panel navigasi, pilih Dasbor.
4. Pada kartu Atribut akun, di bawah Pengaturan, pilih Perlindungan dan keamanan data.
5. Di samping default IMDS, pilih Kelola.

6. Pada halaman Kelola default IMDS, lakukan hal berikut:

   a. Untuk layanan metadata Instance, pilih Diaktifkan.

   b. Untuk Versi metadata, pilih V2 saja (token diperlukan).

   c. Untuk batas hop respons Metadata, tentukan 2 jika instance Anda akan meng-host container. Jika tidak, pilih Tidak ada preferensi. Ketika tidak ada preferensi yang ditentukan, saat peluncuran, nilai default ke 2 jika AMI memiliki pengaturan**`ImdsSupport: v2.0`**; jika tidak maka defaultnya ke 1.

   d. Pilih Perbarui.

AWS CLI

Untuk menetapkan IMDSv2 sebagai default untuk akun untuk Wilayah yang ditentukan

Gunakan modify-instance-metadata-defaultsperintah dan tentukan Wilayah untuk memodifikasi pengaturan tingkat akun IMDS. Sertakan `--http-tokens` set ke `required` dan `--http-put-response-hop-limit` atur ke 2 jika instance Anda akan meng-host kontainer. Jika tidak, tentukan `-1` untuk menunjukkan tidak ada preferensi. Ketika `-1` (tidak ada preferensi) ditentukan, saat peluncuran, nilai default jika AMI memiliki pengaturan`ImdsSupport: v2.0`; jika tidak maka default ke2. 1

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

Berikut ini adalah output contoh.

```
{
    "Return": true
}
```

Untuk melihat pengaturan akun default untuk opsi metadata instance untuk Wilayah yang ditentukan

Gunakan get-instance-metadata-defaultsperintah dan tentukan Wilayah.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Berikut ini adalah output contoh.

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    },
    "ManagedBy": "account"
}
```

`ManagedBy`Bidang menunjukkan entitas yang mengkonfigurasi pengaturan. Dalam contoh ini, `account` menunjukkan bahwa pengaturan dikonfigurasi langsung di akun. Nilai `declarative-policy` berarti pengaturan dikonfigurasi oleh kebijakan deklaratif. Untuk informasi selengkapnya, lihat Kebijakan deklaratif di Panduan AWS Organizations Pengguna.

Untuk menetapkan IMDSv2 sebagai default untuk akun untuk semua Wilayah

Gunakan modify-instance-metadata-defaultsperintah untuk mengubah pengaturan tingkat akun IMDS untuk semua Wilayah. Sertakan `--http-tokens` set ke `required` dan `--http-put-response-hop-limit` atur ke 2 jika instance Anda akan meng-host kontainer. Jika tidak, tentukan `-1` untuk menunjukkan tidak ada preferensi. Ketika `-1` (tidak ada preferensi) ditentukan, saat peluncuran, nilai default jika AMI memiliki pengaturan`ImdsSupport: v2.0`; jika tidak maka default ke2. 1

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
            --http-tokens required \
            --http-put-response-hop-limit 2 \
            --output text)
        echo -e "$region        \t $output"
    );
done
```

Berikut ini adalah output contoh.

```
Region                  Modified
--------------          ---------
ap-south-1              True
eu-north-1              True
eu-west-3               True
...
```

Untuk melihat pengaturan akun default untuk opsi metadata instans untuk semua Wilayah

Gunakan perintah get-instance-metadata-defaults.

```
echo -e "Region   \t Level          Hops    HttpTokens" ; \
echo -e "-------------- \t ------------   ----    ----------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-instance-metadata-defaults \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Berikut ini adalah output contoh.

```
Region           Level          Hops    HttpTokens
--------------   ------------   ----    ----------
ap-south-1       ACCOUNTLEVEL   2       required
eu-north-1       ACCOUNTLEVEL   2       required
eu-west-3        ACCOUNTLEVEL   2       required
...
```

PowerShell

Untuk menetapkan IMDSv2 sebagai default untuk akun untuk Wilayah yang ditentukan

Gunakan Edit-EC2InstanceMetadataDefaultcmdlet dan tentukan Wilayah untuk mengubah pengaturan tingkat akun IMDS. Sertakan `-HttpToken` set ke `required` dan `-HttpPutResponseHopLimit` atur ke 2 jika instance Anda akan meng-host kontainer. Jika tidak, tentukan `-1` untuk menunjukkan tidak ada preferensi. Ketika `-1` (tidak ada preferensi) ditentukan, saat peluncuran, nilai default jika AMI memiliki pengaturan`ImdsSupport: v2.0`; jika tidak maka default ke2. 1

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

Berikut ini adalah output contoh.

```
True
```

Untuk melihat pengaturan akun default untuk opsi metadata instance untuk Wilayah yang ditentukan

Gunakan Get-EC2InstanceMetadataDefaultcmdlet dan tentukan Region.

```
Get-EC2InstanceMetadataDefault -Region us-east-1 | Format-List
```

Berikut ini adalah output contoh.

```
HttpEndpoint            :
HttpPutResponseHopLimit : 2
HttpTokens              : required
InstanceMetadataTags    :
```

Untuk menetapkan IMDSv2 sebagai default untuk akun untuk semua Wilayah

Gunakan Edit-EC2InstanceMetadataDefaultcmdlet untuk mengubah pengaturan level akun IMDS untuk semua Wilayah. Sertakan `-HttpToken` set ke `required` dan `-HttpPutResponseHopLimit` atur ke 2 jika instance Anda akan meng-host kontainer. Jika tidak, tentukan `-1` untuk menunjukkan tidak ada preferensi. Ketika `-1` (tidak ada preferensi) ditentukan, saat peluncuran, nilai default jika AMI memiliki pengaturan`ImdsSupport: v2.0`; jika tidak maka default ke2. 1

```
(Get-EC2Region).RegionName | `
```

```
    ForEach-Object {
    [PSCustomObject]@{
        Region   = $_
        Modified = (Edit-EC2InstanceMetadataDefault `
                -Region $_ `
                -HttpToken required `
                -HttpPutResponseHopLimit 2)
    }
} | `
Format-Table Region, Modified -AutoSize
```

Output yang diharapkan

```
Region         Modified
------         --------
ap-south-1         True
eu-north-1         True
eu-west-3          True
...
```

Untuk melihat pengaturan akun default untuk opsi metadata instans untuk semua Wilayah

Gunakan Get-EC2InstanceMetadataDefaultcmdlet.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region = $_
        HttpPutResponseHopLimit = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpPutResponseHopLimit
        HttpTokens              = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpTokens
    }
} | `
Format-Table -AutoSize
```

Contoh Output

```
Region         HttpPutResponseHopLimit HttpTokens
------         ----------------------- ----------
ap-south-1                           2 required
eu-north-1                           2 required
eu-west-3                            2 required
```

```
...
```

Menegakkan IMDSv2 di tingkat akun

Anda dapat menerapkan penggunaan IMDSv2 di tingkat akun untuk masing-masing AWS Region. Saat diberlakukan, instance hanya dapat diluncurkan jika dikonfigurasi untuk membutuhkan. IMDSv2 Penegakan ini berlaku terlepas dari bagaimana instans atau AMI dikonfigurasi.

> **Note**
>
> Sebelum mengaktifkan IMDSv2 penegakan hukum di tingkat akun, pastikan aplikasi dan AMIs dukungan IMDSv2 Anda. Untuk informasi selengkapnya, lihat Jalur yang direkomendasikan untuk membutuhkan IMDSv2. Jika IMDSv2 penegakan `httpTokens` diaktifkan dan tidak disetel ke `required` konfigurasi instans saat peluncuran, pengaturan akun, atau konfigurasi AMI, peluncuran instance akan gagal. Untuk informasi pemecahan masalah, lihat Meluncurkan instance IMDSv1 -enabled gagal.

> **Note**
>
> Pengaturan ini tidak mengubah versi IMDS dari instans yang ada, tetapi memblokir pengaktifan IMDSv1 pada instance yang ada yang saat ini telah dinonaktifkan. IMDSv1

Console

IMDSv2 Untuk menegakkan akun di Wilayah yang ditentukan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Untuk mengubah AWS Region, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Di panel navigasi, pilih Dasbor.
4. Pada kartu Atribut akun, di bawah Pengaturan, pilih Perlindungan dan keamanan data.
5. Di samping default IMDS, pilih Kelola.
6. Pada halaman Kelola default IMDS, lakukan hal berikut:
   a. Untuk Versi metadata, pilih V2 saja (token diperlukan).
   b. Untuk Menegakkan IMDSv2, pilih Diaktifkan.

c. Pilih Perbarui.

AWS CLI

IMDSv2 Untuk menegakkan akun di Wilayah yang ditentukan

Gunakan modify-instance-metadata-defaultsperintah dan tentukan Wilayah yang akan ditegakkan IMDSv2.

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-tokens-enforced enabled
```

Berikut ini adalah output contoh.

```
{
"Return": true
}
```

Untuk melihat pengaturan IMDSv2 penegakan untuk akun di Wilayah tertentu

Gunakan get-instance-metadata-defaultsperintah dan tentukan Wilayah.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Berikut ini adalah output contoh.

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpTokensEnforced": "enabled"
    },
    "ManagedBy": "account"
}
```

`ManagedBy`Bidang menunjukkan entitas yang mengkonfigurasi pengaturan. Dalam contoh ini, `account` menunjukkan bahwa pengaturan dikonfigurasi langsung di akun. Nilai `declarative-policy` berarti pengaturan dikonfigurasi oleh kebijakan deklaratif. Untuk informasi selengkapnya, lihat Kebijakan deklaratif di Panduan Pengguna AWS Organizations.

Untuk menegakkan IMDSv2 akun untuk semua Wilayah

Gunakan modify-instance-metadata-defaultsperintah untuk menegakkan IMDSv2 di semua Wilayah.

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
            --http-tokens-enforced enabled \
            --output text)
        echo -e "$region        \t $output"
    );
done
```

Berikut ini adalah output contoh.

```
Region                  Modified
--------------          ---------
ap-south-1              True
eu-north-1              True
eu-west-3               True
...
```

Untuk melihat pengaturan IMDSv2 penegakan untuk akun di semua Wilayah

Gunakan perintah get-instance-metadata-defaults.

```
echo -e "Region   \t Level           HttpTokensEnforced" ; \
echo -e "-------------- \t ------------   ----------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
```

```
    do (output=$(
        aws ec2 get-instance-metadata-defaults \
            --region $region \
            --query 'AccountLevel.HttpTokensEnforced' \
            --output text)
        echo -e "$region \t ACCOUNTLEVEL $output"
    );
done
```

Berikut ini adalah output contoh.

```
Region           Level          HttpTokensEnforced
--------------   ------------   ------------------
ap-south-1       ACCOUNTLEVEL   enabled
eu-north-1       ACCOUNTLEVEL   enabled
eu-west-3        ACCOUNTLEVEL   enabled
...
```

PowerShell

IMDSv2 Untuk menegakkan akun di Wilayah yang ditentukan

Gunakan Edit-EC2InstanceMetadataDefaultcmdlet dan tentukan Wilayah yang akan ditegakkan. IMDSv2

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

Berikut ini adalah output contoh.

```
@{
    Return = $true
}
```

Untuk melihat pengaturan IMDSv2 penegakan untuk akun di Wilayah tertentu

Gunakan Get-EC2InstanceMetadataDefault perintah dan tentukan Wilayah.

```
Get-EC2InstanceMetadataDefault -Region us-east-1
```

Berikut ini adalah output contoh.

```
@{
    AccountLevel = @{
        HttpTokens = "required"
        HttpTokensEnforced = "enabled"
    }
    ManagedBy = "account"
}
```

`ManagedBy`Bidang menunjukkan entitas yang mengkonfigurasi pengaturan. Dalam contoh ini, `account` menunjukkan bahwa pengaturan dikonfigurasi langsung di akun. Nilai `declarative-policy` berarti pengaturan dikonfigurasi oleh kebijakan deklaratif. Untuk informasi selengkapnya, lihat Kebijakan deklaratif di Panduan Pengguna AWS Organizations.

Untuk menegakkan IMDSv2 akun untuk semua Wilayah

Gunakan modify-instance-metadata-defaultsperintah untuk menegakkan IMDSv2 di semua Wilayah.

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
            --http-tokens-enforced enabled \
            --output text)
        echo -e "$region        \t $output"
    );
done
```

Berikut ini adalah output contoh.

```
Region                  Modified
--------------          ---------
ap-south-1              True
```

```
eu-north-1                True
eu-west-3                 True
...
```

Untuk menetapkan IMDSv2 sebagai default untuk akun untuk semua Wilayah

Gunakan Edit-EC2InstanceMetadataDefaultcmdlet untuk mengubah pengaturan level akun IMDS untuk semua Wilayah. Sertakan `-HttpToken` set ke `required` dan `-HttpPutResponseHopLimit` atur ke 2 jika instance Anda akan meng-host kontainer. Jika tidak, tentukan `-1` untuk menunjukkan tidak ada preferensi. Ketika `-1` (tidak ada preferensi) ditentukan, saat peluncuran, nilai default jika AMI memiliki pengaturan`ImdsSupport: v2.0`; jika tidak maka default ke2. 1

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region   = $_
        Modified = (Edit-EC2InstanceMetadataDefault `
                -Region $_ `
                -HttpToken required `
                -HttpPutResponseHopLimit 2)
    }
} | `
Format-Table Region, Modified -AutoSize
```

Output yang diharapkan

```
Region         Modified
------         --------
ap-south-1         True
eu-north-1         True
eu-west-3          True
...
```

Untuk melihat pengaturan akun default untuk opsi metadata instans untuk semua Wilayah

Gunakan Get-EC2InstanceMetadataDefaultcmdlet.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region = $_
```

```
        HttpPutResponseHopLimit = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpPutResponseHopLimit
        HttpTokens              = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpTokens
    }
} | `
Format-Table -AutoSize
```

Contoh Output

```
Region         HttpPutResponseHopLimit HttpTokens
------         ----------------------- ----------
ap-south-1                           2 required
eu-north-1                           2 required
eu-west-3                            2 required
...
```

Konfigurasikan instans saat peluncuran

Saat meluncurkan instance, Anda dapat mengonfigurasi instance agar memerlukan penggunaan IMDSv2 dengan mengonfigurasi bidang berikut:

- Konsol Amazon EC2: Atur Versi metadata ke V2 saja (diperlukan token).
- AWS CLI: Atur `HttpTokens` ke `required`.

Bila Anda menentukan yang IMDSv2 diperlukan, Anda juga harus mengaktifkan titik akhir Layanan Metadata Instans (IMDS) dengan menyetel Metadata yang dapat diakses ke Enabled (console) atau to (). `HttpEndpoint` `enabled`AWS CLI

Dalam lingkungan kontainer, bila IMDSv2 diperlukan, kami sarankan untuk mengatur batas hop ke2. Untuk informasi selengkapnya, lihat Pertimbangan akses metadata instance.

Console

Untuk memerlukan penggunaan IMDSv2 pada instance baru

- Saat meluncurkan instans baru di konsol Amazon EC2, perluas Detail lanjutan, dan lakukan hal berikut:
  - Untuk Metadata yang dapat diakses, pilih Diaktifkan.

- Untuk Versi metadata, pilih V2 saja (token diperlukan).
- (Lingkungan kontainer) Untuk batas hop respons Metadata, pilih 2.

Untuk informasi selengkapnya, lihat Detail lanjutan.

AWS CLI

Untuk memerlukan penggunaan IMDSv2 pada instance baru

Contoh run-instances berikut meluncurkan instans `c6i.large` dengan `--metadata-options` yang diatur ke `HttpTokens=required`. Jika Anda menetapkan nilai untuk `HttpTokens`, maka Anda juga harus mengatur `HttpEndpoint` ke `enabled`. Karena header token aman disetel ke `required` untuk permintaan pengambilan metadata, ini memerlukan instance untuk digunakan IMDSv2 saat meminta metadata instance.

Dalam lingkungan kontainer, bila IMDSv2 diperlukan, kami sarankan untuk mengatur batas hop ke 2 with`HttpPutResponseHopLimit=2`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Untuk memerlukan penggunaan IMDSv2 pada instance baru

Contoh New-EC2Instancecmdlet berikut meluncurkan `c6i.large` instance dengan `MetadataOptions_HttpEndpoint` set to `enabled` dan parameter ke. `MetadataOptions_HttpTokens` `required` Jika Anda menetapkan nilai untuk `HttpTokens`, maka Anda juga harus mengatur `HttpEndpoint` ke `enabled`. Karena header token aman disetel ke `required` untuk permintaan pengambilan metadata, ini memerlukan instance untuk digunakan IMDSv2 saat meminta metadata instance.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
```

```
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

CloudFormation

Untuk menentukan opsi metadata untuk instance yang digunakan CloudFormation, lihat AWS::EC2::LaunchTemplate MetadataOptionsproperti di AWS CloudFormation Panduan Pengguna.

Konfigurasikan AMI

Saat Anda mendaftarkan AMI baru atau memodifikasi AMI yang ada, Anda dapat mengatur parameter `imds-support` ke `v2.0`. Instans yang diluncurkan dari AMI ini akan memiliki versi Metadata yang disetel ke V2 saja (diperlukan token) (konsol) atau `HttpTokens` disetel ke `required` ().AWS CLI Dengan pengaturan ini, instance mengharuskan yang IMDSv2 digunakan saat meminta metadata instance.

Perhatikan bahwa jika Anda mengatur `imds-support` ke `v2.0`, instans yang diluncurkan dari AMI ini juga akan memiliki Batas hop tanggapan Metadata (konsol) atau `http-put-response-hop-limit` (AWS CLI) diatur ke 2.

Important

Jangan gunakan parameter ini kecuali perangkat lunak AMI Anda mendukungIMDSv2. Setelah Anda mengatur nilainya ke `v2.0`, Anda tidak dapat membatalkannya. Satu-satunya cara untuk “mengatur ulang” AMI Anda adalah dengan membuat AMI baru dari snapshot dasar.

Untuk mengkonfigurasi AMI baru untuk IMDSv2

Gunakan salah satu metode berikut untuk mengonfigurasi AMI baru untukIMDSv2.

AWS CLI

Contoh register-image berikut mendaftarkan AMI menggunakan snapshot yang ditentukan dari volume root EBS sebagai perangkat `/dev/xvda`. Tentukan `v2.0` `imds-support` parameter sehingga instance yang diluncurkan dari AMI ini akan memerlukan yang IMDSv2 digunakan saat meminta metadata instance.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

Contoh Register-EC2Imagecmdlet berikut mendaftarkan AMI menggunakan snapshot yang ditentukan dari volume root EBS sebagai perangkat. `/dev/xvda` Tentukan `v2.0` `ImdsSupport` parameter sehingga instance yang diluncurkan dari AMI ini akan memerlukan yang IMDSv2 digunakan saat meminta metadata instance.

```
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example'
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

Untuk mengonfigurasi AMI yang ada untuk IMDSv2

Gunakan salah satu metode berikut untuk mengonfigurasi AMI yang ada untukIMDSv2.

AWS CLI

modify-image-attributeContoh berikut memodifikasi AMI yang ada IMDSv2 hanya untuk. Tentukan `v2.0` `imds-support` parameter sehingga instance yang diluncurkan dari AMI ini akan memerlukan yang IMDSv2 digunakan saat meminta metadata instance.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --imds-support v2.0
```

PowerShell

Contoh Edit-EC2ImageAttributecmdlet berikut memodifikasi AMI yang ada hanya untuk. IMDSv2 Tentukan `v2.0` `imds-support` parameter sehingga instance yang diluncurkan dari AMI ini akan memerlukan yang IMDSv2 digunakan saat meminta metadata instance.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Gunakan kebijakan IAM

Anda dapat membuat kebijakan IAM yang melakukan salah satu hal berikut:

- Mencegah pengguna meluncurkan instance baru kecuali mereka membutuhkan IMDSv2 instance baru.
- Mencegah pengguna memanggil ModifyInstanceMetadataOptions API untuk mengubah opsi metadata dari instance yang sedang berjalan. Batasi akses ke properti ModifyInstanceMetadataOptions HttpTokens untuk mencegah pembaruan yang tidak diinginkan dari instance yang sedang berjalan.
- Cegah pengguna memanggil ModifyInstanceMetadataDefaults API untuk mengubah pengaturan default akun dari HttpTokens dan. httpTokensEnforced Membatasi akses ke dua properti ini akan memastikan bahwa hanya peran resmi yang dapat mengubah default akun.

Untuk menegakkan penggunaan IMDSv2 pada semua instans baru dengan menggunakan kebijakan IAM

Untuk memastikan bahwa pengguna hanya dapat meluncurkan instance yang memerlukan penggunaan IMDSv2 saat meminta metadata instance, lakukan hal berikut:

- Batasi akses ke keduanya `ModifyInstanceMetadataOptions` dan `ModifyInstanceMetadataDefaults` API, dan lebih khusus lagi `httpTokensEnforced` properti `httpTokens` dan properti.

- Kemudian, atur default akun ke `httpTokens = required` dan`httpTokensEnforced = enabled`.

  Untuk contoh kebijakan IAM, lihat Cara menggunakan metadata instans.

Aktifkan IMDS IPv4 dan titik akhir IPv6

IMDS memiliki dua titik akhir pada sebuah instance: IPv4 (`169.254.169.254`) dan IPv6 (`[fd00:ec2::254]`). Saat Anda mengaktifkan IMDS, IPv4 titik akhir diaktifkan secara otomatis. IPv6 Titik akhir tetap dinonaktifkan bahkan jika Anda meluncurkan instance ke subnet IPv6 - only. Untuk mengaktifkan IPv6 titik akhir, Anda perlu melakukannya secara eksplisit. Saat Anda mengaktifkan titik IPv6 akhir, IPv4 titik akhir tetap diaktifkan.

Anda dapat mengaktifkan IPv6 titik akhir saat peluncuran instance atau setelahnya.

Persyaratan untuk mengaktifkan titik akhir IPv6

- Jenis instance yang dipilih adalah instance berbasis Nitro.
- Subnet yang dipilih mendukung IPv6, di mana subnet adalah tumpukan ganda atau IPv6 hanya.

Gunakan salah satu metode berikut untuk meluncurkan instance dengan IPv6 titik akhir IMDS diaktifkan.

Console

Untuk mengaktifkan IPv6 titik akhir IMDS saat peluncuran instans

- Luncurkan instans di konsol Amazon EC2 dengan menentukan hal-hal berikut ini pada Detail lanjutan:
  - Untuk IPv6 titik akhir Metadata, pilih Diaktifkan.

Untuk informasi selengkapnya, lihat Detail lanjutan.

AWS CLI

Untuk mengaktifkan IPv6 titik akhir IMDS saat peluncuran instans

Contoh run-instance berikut meluncurkan `c6i.large` instance dengan IPv6 titik akhir diaktifkan untuk IMDS. Untuk mengaktifkan IPv6 titik akhir, untuk `--metadata-options`

parameter, tentukan`HttpProtocolIpv6=enabled`. Jika Anda menetapkan nilai untuk `HttpProtocolIpv6`, maka Anda juga harus mengatur `HttpEndpoint` ke `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Untuk mengaktifkan IPv6 titik akhir IMDS saat peluncuran instans

Contoh New-EC2Instancecmdlet berikut meluncurkan `c6i.large` instance dengan IPv6 titik akhir diaktifkan untuk IMDS. Untuk mengaktifkan IPv6 titik akhir, tentukan `MetadataOptions_HttpProtocolIpv6` sebagai`enabled`. Jika Anda menetapkan nilai untuk `MetadataOptions_HttpProtocolIpv6`, maka Anda juga harus mengatur `MetadataOptions_HttpEndpoint` ke `enabled`.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Nonaktifkan akses untuk metadata instans

Anda dapat menonaktifkan akses ke metadata instans dengan menonaktifkan IMDS saat Anda meluncurkan instans. Anda dapat mengaktifkan akses nanti dengan mengaktifkan kembali IMDS. Untuk informasi selengkapnya, lihat Aktifkan akses ke metadata instans.

Important

Anda dapat memilih untuk menonaktifkan IMDS saat peluncuran atau setelah peluncuran. Jika Anda menonaktifkan IMDS saat peluncuran, hal-hal berikut ini mungkin tidak berfungsi:

- Anda mungkin tidak memiliki akses SSH ke instans Anda. `public-keys/0/openssh-key`, yang merupakan kunci SSH publik instans Anda, tidak akan dapat diakses karena kunci biasanya disediakan dan diakses dari metadata instans EC2.

- Data pengguna EC2 tidak akan tersedia dan tidak akan berjalan saat instans dimulai. Data pengguna EC2 di-host di IMDS. Jika Anda menonaktifkan IMDS, Anda secara efektif mematikan akses ke data pengguna.

Untuk mengakses fungsionalitas ini, Anda dapat mengaktifkan kembali IMDS setelah peluncuran.

Console

Untuk menonaktifkan akses ke metadata instans saat peluncuran

- Luncurkan instans di konsol Amazon EC2 dengan menentukan hal-hal berikut ini pada Detail lanjutan:
  - Untuk Metadata yang dapat diakses, pilih Diaktifkan.

Untuk informasi selengkapnya, lihat Detail lanjutan.

AWS CLI

Untuk menonaktifkan akses ke metadata instans saat peluncuran

Luncurkan instans dengan `--metadata-options` diatur ke `HttpEndpoint=disabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

Untuk menonaktifkan akses ke metadata instans saat peluncuran

Contoh New-EC2Instancecmdlet berikut meluncurkan instance dengan `MetadataOptions_HttpEndpoint` set ke. `disabled`

```
New-EC2Instance `
```

```
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

CloudFormation

Untuk menentukan opsi metadata untuk instance yang digunakan CloudFormation, lihat AWS::EC2::LaunchTemplate MetadataOptionsproperti di CloudFormation Panduan Pengguna.

Mengizinkan akses ke tanda dalam metadata instans

Secara default, tag instance tidak dapat diakses dalam metadata instance. Untuk setiap contoh, Anda harus secara eksplisit mengizinkan akses. Jika akses diizinkan, kunci tag instance harus mematuhi batasan karakter tertentu, jika tidak, peluncuran instance akan gagal. Untuk informasi selengkapnya, lihat Aktifkan akses ke tag dalam metadata contoh.

Mengonfigurasi opsi metadata instans untuk instans yang ada

Anda dapat mengonfigurasi opsi metadata instans untuk instans yang ada

Anda juga dapat membuat kebijakan IAM yang mencegah pengguna mengubah opsi metadata instans pada instans yang ada. Untuk mengontrol pengguna mana yang dapat memodifikasi opsi metadata instance, tentukan kebijakan yang mencegah semua pengguna selain pengguna dengan peran tertentu untuk menggunakan API. ModifyInstanceMetadataOptions Untuk contoh kebijakan IAM, lihat Cara menggunakan metadata instans.

> **Note**
>
> Jika kebijakan deklaratif digunakan untuk mengonfigurasi opsi metadata instance, Anda tidak dapat memodifikasinya secara langsung di dalam akun. Untuk informasi selengkapnya, lihat Kebijakan deklaratif di Panduan AWS Organizations Pengguna.

Membutuhkan penggunaan IMDSv2

Gunakan salah satu metode berikut untuk memodifikasi opsi metadata instance pada instance yang ada untuk meminta yang IMDSv2 digunakan saat meminta metadata instance. Ketika IMDSv2 diperlukan, IMDSv1 tidak dapat digunakan.

> **Note**
>
> Sebelum mengharuskan yang IMDSv2 digunakan, pastikan bahwa instance tidak melakukan IMDSv1 panggilan. `MetadataNoToken`CloudWatch Metrik melacak IMDSv1 panggilan. Ketika `MetadataNoToken` mencatat IMDSv1 penggunaan nol untuk sebuah instance, instance kemudian siap untuk membutuhkan IMDSv2.

Console

Untuk memerlukan penggunaan IMDSv2 pada instance yang ada

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans Anda.
4. Pilih Tindakan, Pengaturan instans, Ubah opsi metadata instans.
5. Di kotak dialog Ubah opsi metadata instans, lakukan hal berikut:
   a. Untuk Layanan metadata instans, pilih Diaktifkan.
   b. Untuk IMDSv2, pilih Diperlukan.
   c. Pilih Simpan.

AWS CLI

Untuk memerlukan penggunaan IMDSv2 pada instance yang ada

Gunakan perintah modify-instance-metadata-optionsCLI dan atur `http-tokens` parameternya ke. `required` Jika Anda menetapkan nilai untuk `http-tokens`, maka Anda juga harus mengatur `http-endpoint` ke `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

Untuk memerlukan penggunaan IMDSv2 pada instance yang ada

Gunakan Edit-EC2InstanceMetadataOptioncmdlet dan atur `HttpTokens` parameternya ke. `required` Jika Anda menetapkan nilai untuk `HttpTokens`, maka Anda juga harus mengatur `HttpEndpoint` ke `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Kembalikan penggunaan IMDSv1

Ketika IMDSv2 diperlukan pada sebuah instance, menggunakan IMDSv1 permintaan akan gagal. IMDSv2 Kapan opsional, maka keduanya IMDSv2 dan IMDSv1 akan berfungsi. Oleh karena itu, untuk mengembalikan IMDSv1, atur IMDSv2 ke opsional (`httpTokens = optional`) menggunakan salah satu metode berikut.

Properti `httpTokensEnforced` IMDS juga mencegah upaya untuk IMDSv1 mengaktifkan instance yang ada. Saat diaktifkan untuk akun di Wilayah, upaya `httpTokens` untuk menyetel `optional` akan menghasilkan `UnsupportedOperation` pengecualian. Untuk informasi lebih lanjut, lihatPemecahan masalah.

Important

Jika peluncuran instans Anda gagal karena IMDSv2 penegakan hukum, Anda memiliki dua opsi untuk mengaktifkan peluncuran agar berhasil:

- Luncurkan instance sebagai IMDSv2 -only - Jika perangkat lunak yang berjalan pada instance IMDSv2 hanya menggunakan (tidak ada ketergantungan pada IMDSv1), maka Anda dapat meluncurkan instance sebagai saja. IMDSv2 Untuk melakukan ini, konfigurasikan IMDSv2 hanya dengan mengatur `httpTokens = required` baik dalam parameter peluncuran atau dalam default metadata untuk akun di Wilayah.
- Nonaktifkan penegakan hukum — Jika perangkat lunak Anda masih bergantung IMDSv1, atur `httpTokensEnforced` ke `disabled` akun di Wilayah. Untuk informasi selengkapnya, lihat Menegakkan IMDSv2 di tingkat akun.

Console

Untuk mengembalikan penggunaan IMDSv1 pada sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans Anda.
4. Pilih Tindakan, Pengaturan instans, Ubah opsi metadata instans.
5. Di kotak dialog Ubah opsi metadata instans, lakukan hal berikut:
   a. Untuk Layanan metadata instans, pastikan Aktifkan telah dipilih.
   b. Untuk IMDSv2, pilih Opsional.
   c. Pilih Simpan.

AWS CLI

Untuk mengembalikan penggunaan IMDSv1 pada sebuah instance

Anda dapat menggunakan perintah modify-instance-metadata-optionsCLI dengan `http-tokens` set to `optional` untuk mengembalikan penggunaan IMDSv1 saat meminta metadata instance.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

Untuk mengembalikan penggunaan IMDSv1 pada sebuah instance

Anda dapat menggunakan Edit-EC2InstanceMetadataOptioncmdlet dengan `HttpTokens` set to `optional` untuk mengembalikan penggunaan IMDSv1 saat meminta metadata instance.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Mengubah batas hop respons PUT

Untuk instans yang ada, Anda dapat mengubah pengaturan batas hop respons PUT.

Saat ini hanya AWS CLI dan AWS SDKs mendukung perubahan batas hop respons PUT.

AWS CLI

Mengubah batas hop respons PUT

Gunakan perintah modify-instance-metadata-optionsCLI dan atur `http-put-response-hop-limit` parameter ke jumlah hop yang diperlukan. Pada instans berikut, batas hop diatur ke `3`. Perhatikan bahwa saat Anda menetapkan nilai untuk `http-put-response-hop-limit`, maka Anda juga harus mengatur `http-endpoint` ke `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

Mengubah batas hop respons PUT

Gunakan Edit-EC2InstanceMetadataOptioncmdlet dan atur `HttpPutResponseHopLimit` parameter ke jumlah hop yang diperlukan. Pada instans berikut, batas hop diatur ke `3`. Perhatikan bahwa saat Anda menetapkan nilai untuk `HttpPutResponseHopLimit`, maka Anda juga harus mengatur `HttpEndpoint` ke `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Aktifkan IMDS IPv4 dan titik akhir IPv6

IMDS memiliki dua titik akhir pada sebuah instance: IPv4 (`169.254.169.254`) dan IPv6 (`[fd00:ec2::254]`). Saat Anda mengaktifkan IMDS, IPv4 titik akhir diaktifkan secara otomatis. IPv6 Titik akhir tetap dinonaktifkan bahkan jika Anda meluncurkan instance ke subnet IPv6 -

only. Untuk mengaktifkan IPv6 titik akhir, Anda perlu melakukannya secara eksplisit. Saat Anda mengaktifkan titik IPv6 akhir, IPv4 titik akhir tetap diaktifkan.

Anda dapat mengaktifkan IPv6 titik akhir saat peluncuran instance atau setelahnya.

Persyaratan untuk mengaktifkan titik akhir IPv6

- Jenis instance yang dipilih adalah instance berbasis Nitro.
- Subnet yang dipilih mendukung IPv6, di mana subnet adalah tumpukan ganda atau IPv6 hanya.

Saat ini hanya AWS SDKs dukungan AWS CLI dan yang mengaktifkan IPv6 titik akhir IMDS setelah peluncuran instance.

AWS CLI

Untuk mengaktifkan IPv6 titik akhir IMDS untuk instans Anda

Gunakan perintah modify-instance-metadata-optionsCLI dan atur `http-protocol-ipv6` parameternya ke. `enabled` Perhatikan bahwa saat Anda menetapkan nilai untuk `http-protocol-ipv6`, maka Anda juga harus mengatur `http-endpoint` ke `enabled`.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567890abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Untuk mengaktifkan IPv6 titik akhir IMDS untuk instans Anda

Gunakan Edit-EC2InstanceMetadataOptioncmdlet dan atur `HttpProtocolIpv6` parameternya ke. `enabled` Perhatikan bahwa saat Anda menetapkan nilai untuk `HttpProtocolIpv6`, maka Anda juga harus mengatur `HttpEndpoint` ke `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Aktifkan akses ke metadata instans

Anda dapat mengaktifkan akses ke metadata instans dengan mengaktifkan titik akhir HTTP IMDS pada instans Anda, apa pun versi IMDS yang Anda gunakan. Anda dapat megembalikan perubahan ini kapan saja dengan menonaktifkan titik akhir HTTP.

Gunakan salah satu metode berikut untuk menonaktifkan akses ke metadata instans pada instans.

Console

Untuk mengaktifkan akses ke metadata instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans Anda.
4. Pilih Tindakan, Pengaturan instans, Ubah opsi metadata instans.
5. Di kotak dialog Ubah opsi metadata instans, lakukan hal berikut:
   a. Untuk Layanan metadata instans, pilih Diaktifkan.
   b. Pilih Simpan.

AWS CLI

Untuk mengaktifkan akses ke metadata instans

Gunakan perintah modify-instance-metadata-optionsCLI dan atur `http-endpoint` parameternya ke. `enabled`

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-endpoint enabled
```

PowerShell

Untuk mengaktifkan akses ke metadata instans

Gunakan Edit-EC2InstanceMetadataOptioncmdlet dan atur `HttpEndpoint` parameternya ke. `enabled`

```
(Edit-EC2InstanceMetadataOption `
```

```
    -InstanceId i-1234567890abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Nonaktifkan akses untuk metadata instans

Anda dapat menonaktifkan akses ke metadata instans dengan menonaktifkan titik akhir HTTP IMDS pada instans Anda, apa pun versi IMDS yang Anda gunakan. Anda dapat megembalikan perubahan ini kapan saja dengan mengaktifkan titik akhir HTTP.

Gunakan salah satu metode berikut untuk menonaktifkan akses ke metadata instans pada instans.

Console

Untuk menonaktifkan akses untuk metadata instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans Anda.
4. Pilih Tindakan, Pengaturan instans, Ubah opsi metadata instans.
5. Di kotak dialog Ubah opsi metadata instans, lakukan hal berikut:
   a. Untuk Layanan metadata instans, hapus Aktifkan.
   b. Pilih Simpan.

AWS CLI

Untuk menonaktifkan akses untuk metadata instans

Gunakan perintah modify-instance-metadata-optionsCLI dan atur `http-endpoint` parameternya ke. `disabled`

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-endpoint disabled
```

PowerShell

Untuk menonaktifkan akses untuk metadata instans

Gunakan Edit-EC2InstanceMetadataOptioncmdlet dan atur `HttpEndpoint` parameternya ke. `disabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Mengizinkan akses ke tanda dalam metadata instans

Anda dapat mengizinkan akses ke tag dalam metadata instance pada instance yang sedang berjalan atau dihentikan. Untuk setiap contoh, Anda harus secara eksplisit mengizinkan akses. Jika akses diizinkan, kunci tag instance harus mematuhi batasan karakter tertentu, jika tidak, Anda akan mendapatkan kesalahan. Untuk informasi selengkapnya, lihat Aktifkan akses ke tag dalam metadata contoh.

Pemecahan masalah

Gagal memodifikasi instance IMDSv1 -enabled

Deskripsi

Anda mendapatkan pesan galat berikut:

```
You can't launch instances with IMDSv1 because httpTokensEnforced
is enabled for this account. Either launch the instance with
httpTokens=required or contact your account owner to disable
httpTokensEnforced using the ModifyInstanceMetadataDefaults API or the
account settings in the EC2 console.
```

Penyebab

Kesalahan ini muncul saat Anda mencoba mengubah instance yang ada untuk IMDSv1 diaktifkan (`httpTokens = optional`) di akun tempat pengaturan akun EC2 atau kebijakan deklaratif AWS Organisasi memberlakukan penggunaan IMDSv2 (). `httpTokensEnforced = enabled`

Solusi

Jika Anda memerlukan IMDSv1 dukungan pada instans yang ada, Anda harus menonaktifkan IMDSv2 penegakan hukum untuk akun di Wilayah. Untuk menonaktifkan IMDSv2

penegakan, atur `HttpTokensEnforced` ke`disabled`. Untuk informasi selengkapnya, lihat ModifyInstanceMetadataDefaultsdi Referensi API Amazon EC2. Jika Anda lebih suka mengonfigurasi pengaturan ini menggunakan konsol, lihatMenegakkan IMDSv2 di tingkat akun.

Kami menyarankan Anda IMDSv2 hanya menggunakan (`httpTokens=required`). Untuk informasi selengkapnya, lihat Transisi ke penggunaan Layanan Metadata Instans Versi 2.

Jalankan perintah saat Anda meluncurkan instans EC2 dengan input data pengguna

Saat meluncurkan instans Amazon EC2, Anda dapat meneruskan data pengguna ke instans yang digunakan untuk melakukan tugas konfigurasi otomatis, atau menjalankan skrip setelah instance dimulai.

Jika Anda tertarik dengan skenario otomatisasi yang lebih kompleks, Anda dapat mempertimbangkannya CloudFormation. Untuk informasi selengkapnya, lihat Menerapkan aplikasi di Amazon EC2 CloudFormation dengan di Panduan Pengguna AWS CloudFormation .

Pada instance Linux, Anda dapat meneruskan dua jenis data pengguna ke Amazon EC2: skrip shell dan direktif cloud-init. Anda juga dapat meneruskan data ini ke wizard instance peluncuran sebagai teks biasa, sebagai file (ini berguna untuk meluncurkan instance dengan alat baris perintah), atau sebagai teks yang disandikan base64 (untuk panggilan API).

Pada instance Windows, agen peluncuran menangani skrip data pengguna Anda.

Pertimbangan-pertimbangan

- Data pengguna diperlakukan sebagai data buram: apa yang Anda berikan adalah apa yang Anda dapatkan kembali. Terserah instans untuk menafsirkannya.
- Data pengguna harus dienkode base64. Konsol Amazon EC2 dapat melakukan pengkodean base64 untuk input yang disandikan base64 atau menerima input yang disandikan base64. Jika Anda mengambil data pengguna menggunakan metadata instans atau konsol, data base64 diterjemahkan untuk Anda secara otomatis.
- Data pengguna dibatasi hingga 16 KB, dalam bentuk mentah, sebelum dienkode base64. Ukuran string dengan panjang n setelah enkode base64 adalah ceil(n/3)*4.
- Data pengguna adalah atribut instans. Jika Anda membuat AMI dari instans, data pengguna instans tidak disertakan dalam AMI.

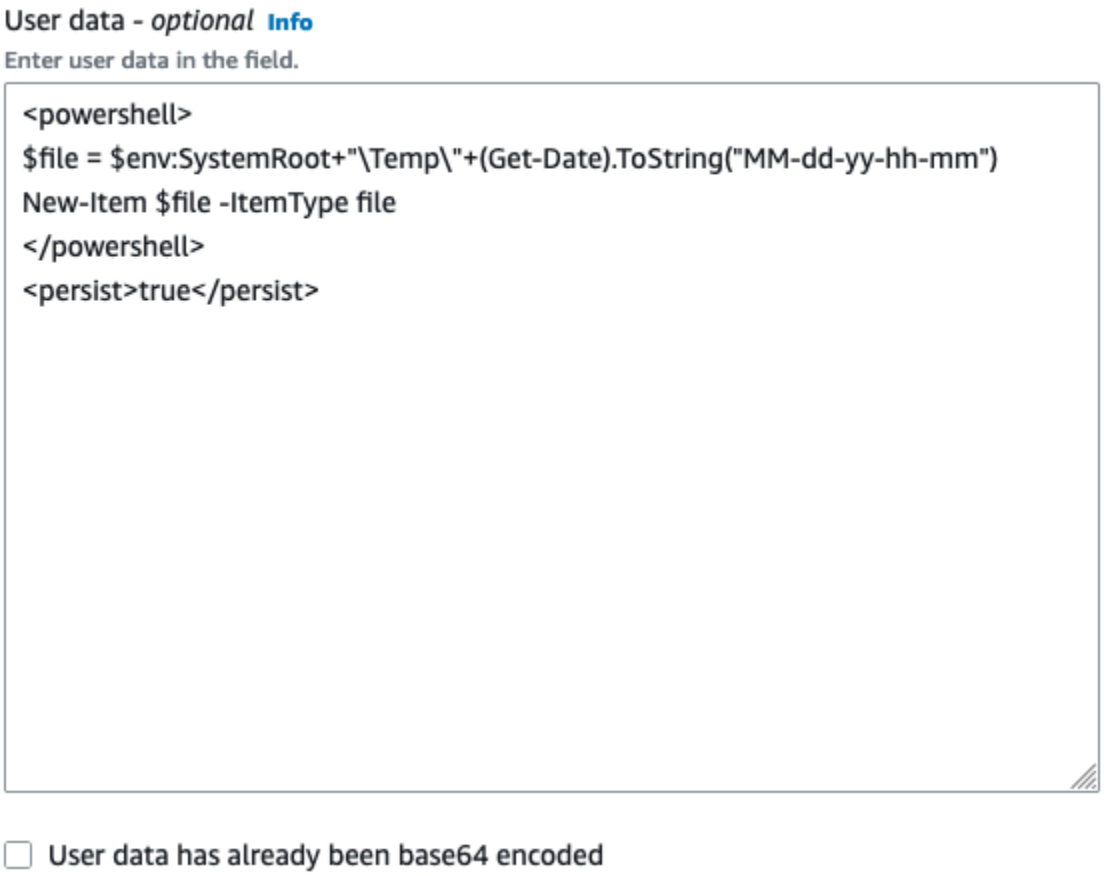
Data pengguna di Konsol Manajemen AWS

Anda dapat menentukan data pengguna instans saat Anda meluncurkan instans. Jika volume root dari instans adalah volume EBS, Anda juga dapat menghentikan instans dan memperbarui data penggunanya.

Tentukan data pengguna instance saat peluncuran dengan Launch Wizard

Anda dapat menentukan data pengguna saat meluncurkan instance dengan Launch Wizard di konsol EC2. Untuk menentukan data pengguna saat peluncuran, ikuti prosedur untuk meluncurkan instance. Bidang Data pengguna terletak di bagian Detail lanjutan wizard peluncuran instans. Masukkan PowerShell skrip Anda di bidang Data pengguna, dan kemudian selesaikan prosedur peluncuran instance.

Pada tangkapan layar dari bidang Data pengguna berikut, skrip contoh membuat file di folder sementara Windows, dengan menggunakan tanggal dan waktu saat ini di nama file. Saat Anda memasukkan `<persist>true</persist>`, skrip akan dijalankan setiap kali Anda melakukan boot ulang atau memulai instans. Jika Anda membiarkan kotak centang data Pengguna telah dikodekan base64 kosong, konsol Amazon EC2 melakukan pengkodean base64 untuk Anda.



Untuk informasi selengkapnya, lihat Tentukan data pengguna instance saat peluncuran dengan Launch Wizard. Untuk contoh Linux yang menggunakan AWS CLI, lihatthe section called “Data pengguna dan AWS CLI”. Untuk contoh Windows yang menggunakan Alat untuk Windows PowerShell, lihatthe section called “Data pengguna dan Alat untuk Windows PowerShell”.

Lihat dan perbarui data pengguna instans

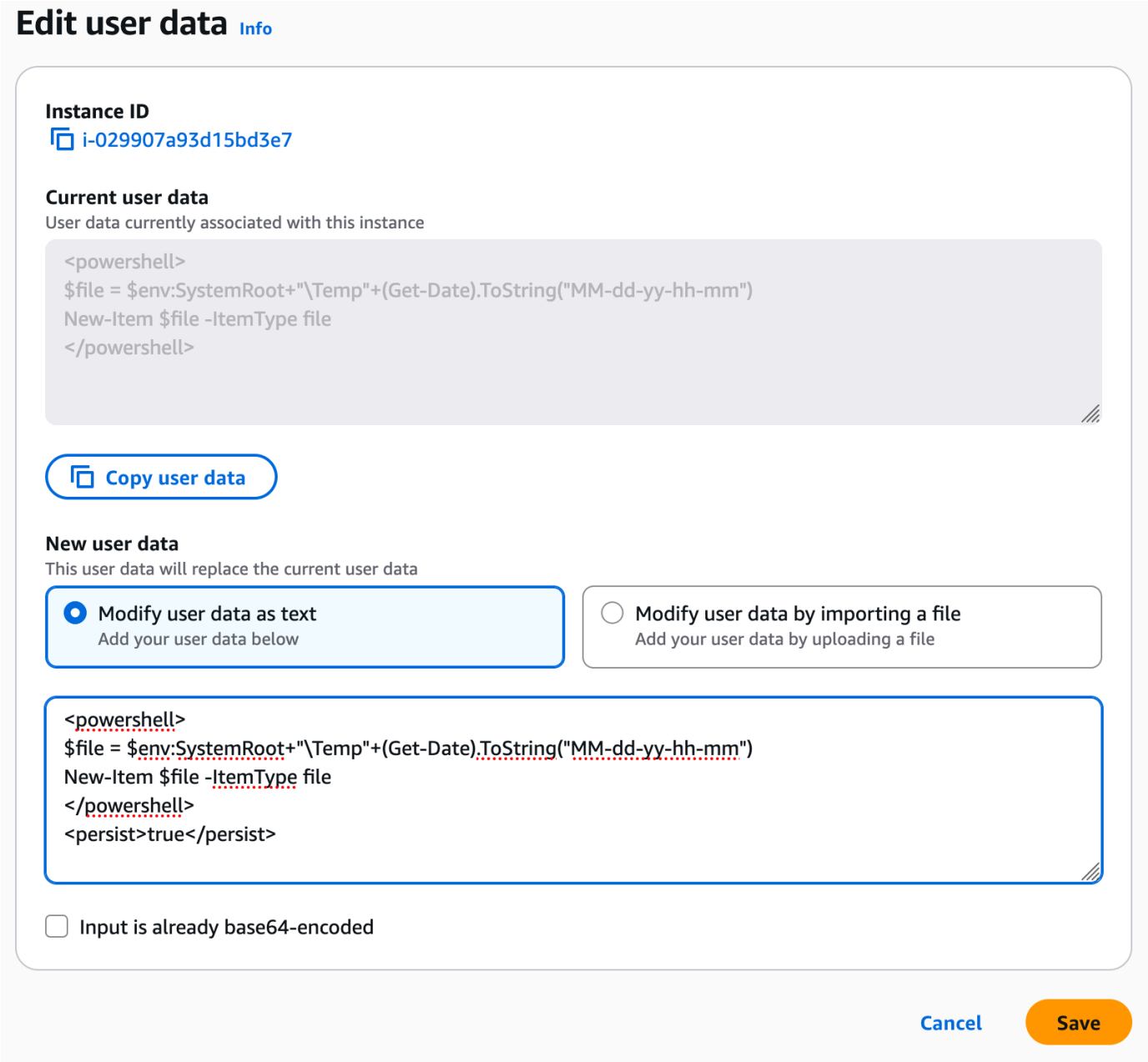
Anda dapat melihat data pengguna instans untuk semua instans, dan Anda dapat memperbarui data pengguna instans untuk instans yang dihentikan.

Untuk memperbarui data pengguna untuk sebuah instans dengan menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans dan pilih Tindakan, status instans, Hentikan instans.

> **Warning**
>
> Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instans akan hilang. Untuk menyimpan data ini, buat cadangan ke penyimpanan persisten.

4. Ketika diminta konfirmasi, pilih Berhenti. Hal ini dapat memerlukan waktu beberapa menit sampai instans berhenti.
5. Dengan instans yang masih dipilih, pilih Tindakan, Pengaturan instans, Edit data pengguna. Anda tidak dapat mengubah data pengguna jika instans sedang berjalan, tetapi Anda dapat melihatnya.
6. Dalam kotak dialog Edit data pengguna, perbarui data pengguna, lalu pilih Simpan. Untuk menjalankan skrip data pengguna setiap kali Anda melakukan boot ulang atau memulai instans, tambahkan `<persist>true</persist>`, seperti yang ditunjukkan pada contoh berikut:



7. Mulai instans. Jika Anda mengaktifkan eksekusi data pengguna untuk boot ulang atau permulaan berikutnya, skrip data pengguna yang diperbarui akan dijalankan sebagai bagian dari proses mulai instans.

Cara Amazon EC2 menangani data pengguna untuk instans Linux

Contoh berikut menggunakan data pengguna untuk menjalankan perintah yang mengatur server LAMP saat instance diluncurkan. Dalam setiap contoh, tugas-tugas berikut dilakukan:

- Paket perangkat lunak distribusi diperbarui.

- Server web,`php`, dan `mariadb` paket diinstal.
- `httpd`Layanan dimulai dan dihidupkan.
- Pengguna `ec2-user` ditambahkan ke grup apache.
- Kepemilikan yang sesuai dan izin file ditetapkan untuk direktori web dan file yang ada di dalamnya.
- Halaman web sederhana dibuat untuk menguji server web dan mesin PHP.

Daftar Isi

- Prasyarat
- Data pengguna dan skrip shell
- Perbarui data pengguna instance
- Data pengguna dan arahan cloud-init
- Data pengguna dan AWS CLI
- Menggabungkan skrip shell dan arahan cloud-init

Prasyarat

Contoh-contoh dalam topik ini mengasumsikan hal berikut:

- Instans Anda memiliki nama DNS publik yang dapat dijangkau dari internet.
- Grup keamanan yang terkait dengan instans Anda dikonfigurasi untuk mengizinkan lalu lintas SSH (port 22) sehingga Anda dapat terhubung ke instans untuk melihat file log keluaran.
- Instans Anda diluncurkan menggunakan AMI Amazon Linux. Perintah dan arahan mungkin tidak berfungsi untuk distribusi Linux lainnya. Untuk informasi selengkapnya tentang distribusi lain, seperti dukungannya untuk cloud-init, lihat dokumentasi untuk distribusi tertentu.

Data pengguna dan skrip shell

Jika Anda terbiasa dengan skrip shell, ini adalah cara termudah dan terlengkap untuk mengirim instruksi ke sebuah instans saat peluncuran. Menambahkan tugas ini pada waktu boot akan menambah jumlah waktu yang dibutuhkan untuk booting sebuah instans. Anda harus memberikan waktu tambahan beberapa menit untuk penyelesaian tugas sebelum menguji apakah skrip pengguna telah berhasil diselesaikan.

> **Important**
>
> Secara default, skrip data pengguna dan arahan cloud-init hanya berjalan selama siklus boot saat Anda pertama kali meluncurkan sebuah instans. Anda dapat memperbarui konfigurasi untuk memastikan bahwa skrip data pengguna dan arahan cloud-init Anda berjalan setiap kali Anda memulai ulang instans. Untuk informasi selengkapnya, lihat Bagaimana cara menggunakan data pengguna untuk menjalankan skrip secara otomatis dengan setiap restart instans Amazon EC2 Linux saya? di pusat AWS pengetahuan.

Skrip shell data pengguna harus dimulai dengan `#!` karakter dan jalur ke penerjemah yang ingin Anda baca skrip (umumnya. /bin/bash) Untuk pengenalan tentang skrip shell, lihat Manual Referensi Bash di situs web Sistem Operasi GNU.

Skrip yang dimasukkan sebagai data pengguna dijalankan sebagai pengguna root pengguna, jadi jangan gunakan perintah sudo dalam skrip. Ingatlah bahwa file apa pun yang Anda buat akan menjadi milik pengguna root; jika Anda membutuhkan pengguna non-root untuk memiliki akses file, Anda harus mengubah izin yang sesuai dalam skrip. Selain itu, karena skrip tidak dijalankan secara interaktif, Anda tidak dapat menyertakan perintah yang memerlukan umpan balik pengguna (seperti yum update tanpa bendera `-y`).

Jika Anda menggunakan AWS API, termasuk AWS CLI, dalam skrip data pengguna, Anda harus menggunakan profil instance saat meluncurkan instance. Profil instance menyediakan AWS kredensi yang sesuai yang diperlukan oleh skrip data pengguna untuk mengeluarkan panggilan API. Untuk informasi selengkapnya, lihat Menggunakan profil instans di Panduan Pengguna IAM. Izin yang Anda tetapkan ke peran IAM bergantung pada layanan mana yang Anda panggil dengan API. Untuk informasi selengkapnya, lihat IAM role untuk Amazon EC2.

File log keluaran cloud-init () menangkap keluaran konsol sehingga mudah untuk men-debug skrip Anda setelah peluncuran jika instans tidak berperilaku seperti yang Anda inginkan. Untuk melihat file log, hubungkan ke instans dan buka `/var/log/cloud-init-output.log`.

Ketika skrip data pengguna diproses, skrip itu akan disalin dan dijalankan dari `/var/lib/cloud/instances/`*`instance-id`*`/`. Skrip tidak dihapus setelah dijalankan. Pastikan untuk menghapus skrip data pengguna dari `/var/lib/cloud/instances/`*`instance-id`*`/` sebelum Anda membuat AMI dari instans. Jika tidak, skrip akan ada di direktori ini pada setiap instans yang diluncurkan dari AMI.

Perbarui data pengguna instance

Untuk memperbarui data pengguna instans, Anda harus menghentikan instans tersebut terlebih dahulu. Jika instans sedang berjalan, Anda dapat melihat data pengguna tetapi Anda tidak dapat mengubahnya.

> **Warning**
>
> Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instans akan hilang. Untuk menyimpan data ini, buat cadangan ke penyimpanan persisten.

Untuk mengubah data pengguna instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans dan pilih Status instans, Hentikan instans. Jika opsi ini dinonaktifkan, instance sudah dihentikan atau volume rootnya adalah volume penyimpanan instance.
4. Ketika diminta konfirmasi, pilih Berhenti. Hal ini dapat memerlukan waktu beberapa menit sampai instans berhenti.
5. Dengan instans yang masih dipilih, pilih Tindakan, Pengaturan instans, Edit data pengguna.
6. Ubah data pengguna sesuai kebutuhan, lalu pilih Simpan.
7. Mulai instans. Data pengguna baru terlihat di instans Anda setelah Anda memulainya; namun, skrip data pengguna tidak dijalankan.

Data pengguna dan arahan cloud-init

Paket cloud-init mengonfigurasi aspek spesifik dari instans Amazon Linux baru saat diluncurkan; paket ini terutama mengonfigurasi file `.ssh/authorized_keys` untuk ec2-user sehingga Anda dapat masuk dengan kunci privat Anda sendiri. Untuk informasi selengkapnya tentang tugas konfigurasi yang dilakukan paket cloud-init untuk instans Amazon Linux, lihat dokumentasi berikut:

- Amazon Linux 2023 - Cloud-init yang disesuaikan
- Amazon Linux 2 - Menggunakan cloud-init di Amazon Linux 2

Arahan pengguna cloud-init dapat diteruskan ke instans saat peluncuran dengan cara yang sama seperti skrip diteruskan, meskipun sintaksnya berbeda. Untuk informasi selengkapnya tentang cloud-init, lihat. https://cloudinit.readthedocs.org/en/latest/index.html

> **Important**
>
> Secara default, skrip data pengguna dan arahan cloud-init hanya berjalan selama siklus boot saat Anda pertama kali meluncurkan sebuah instans. Anda dapat memperbarui konfigurasi untuk memastikan bahwa skrip data pengguna dan arahan cloud-init Anda berjalan setiap kali Anda memulai ulang instans. Untuk informasi selengkapnya, lihat Bagaimana cara menggunakan data pengguna untuk menjalankan skrip secara otomatis dengan setiap restart instans Amazon EC2 Linux saya? di pusat AWS pengetahuan.

Menambahkan tugas ini pada waktu boot akan menambah jumlah waktu yang dibutuhkan untuk booting sebuah instans. Anda harus memberikan waktu tambahan beberapa menit untuk penyelesaian tugas sebelum menguji apakah arahan data pengguna Anda telah selesai.

Untuk meneruskan arahan cloud-init ke instans Amazon Linux

1. Ikuti prosedur untuk meluncurkan instans. Bidang Data pengguna terletak di bagian Detail lanjutan wizard peluncuran instans. Masukkan teks arahan cloud-init Anda di bidang Data pengguna, lalu selesaikan prosedur peluncuran instans.

   Dalam contoh di bawah ini, arahan membuat dan mengkonfigurasi server web di Amazon Linux. Baris `#cloud-config` di atas diperlukan untuk mengidentifikasi perintah sebagai arahan cloud-init.

   AL2023

   ```
   #cloud-config
   package_update: true
   package_upgrade: all

   packages:
   - httpd
   - mariadb105-server
   - php8.1
   - php8.1-mysqlnd
   ```

```
runcmd:
- systemctl start httpd
- systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

AL2

```
#cloud-config
package_update: true
package_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

2. Berikan waktu yang cukup bagi instans untuk meluncurkan dan menjalankan arahan di data pengguna Anda, lalu periksa untuk melihat apakah arahan Anda telah menyelesaikan tugas yang Anda maksudkan.

   Misalnya, di peramban web, masukkan URL file pengujian PHP yang dibuat arahan tersebut. URL ini adalah alamat DNS publik dari instans Anda yang diikuti dengan garis miring ke depan dan nama file.

   ```
   http://my.public.dns.amazonaws.com/phpinfo.php
   ```

Anda akan melihat halaman informasi PHP: Jika Anda tidak dapat melihat halaman informasi PHP, periksa apakah grup keamanan yang Anda gunakan berisi aturan yang mengizinkan lalu lintas HTTP (port 80). Untuk informasi selengkapnya, lihat Mengonfigurasi aturan grup keamanan.

3. (Opsional) Jika arahan Anda tidak menyelesaikan tugas yang Anda harapkan, atau jika Anda hanya ingin memverifikasi bahwa arahan Anda selesai tanpa kesalahan, hubungkan ke instans, periksa file log output (`/var/log/cloud-init-output.log`), dan cari pesan kesalahan di output. Untuk informasi debugging tambahan, Anda dapat menambahkan baris berikut ke arahan Anda:

   ```
   output : { all : '| tee -a /var/log/cloud-init-output.log' }
   ```

   Arahan ini mengirimkan output runcmd ke `/var/log/cloud-init-output.log`.

Data pengguna dan AWS CLI

Anda dapat menggunakan AWS CLI untuk menentukan, memodifikasi, dan melihat data pengguna untuk instance Anda. Untuk informasi tentang melihat data pengguna dari instans Anda menggunakan metadata instans, lihat Akses metadata instans untuk instans EC2.

Di Windows, Anda dapat menggunakan AWS Tools for Windows PowerShell alih-alih menggunakan file AWS CLI. Untuk informasi selengkapnya, lihat Data pengguna dan Alat untuk Windows PowerShell.

Contoh: Tentukan data pengguna saat peluncuran

Untuk menentukan data pengguna saat Anda meluncurkan instans, gunakan perintah run-instances dengan parameter `--user-data`. Denganrun-instances, AWS CLI melakukan pengkodean base64 dari data pengguna untuk Anda.

Contoh berikut menunjukkan cara menentukan skrip sebagai string pada baris perintah:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data echo user data
```

Contoh berikut menunjukkan cara menentukan skrip menggunakan file teks. Pastikan untuk menggunakan awalan `file://` untuk menentukan file.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data file://my_script.txt
```

Berikut ini adalah contoh file teks dengan skrip shell.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Contoh: Modifikasi data pengguna dari instans yang dihentikan

Anda dapat memodifikasi data pengguna dari instance yang dihentikan menggunakan modify-instance-attributeperintah. Denganmodify-instance-attribute, AWS CLI tidak melakukan pengkodean base64 dari data pengguna untuk Anda.

- Di komputer Linux, gunakan perintah base64 untuk mengenkode data pengguna.

  ```
  base64 my_script.txt >my_script_base64.txt
  ```

- Di komputer Windows, gunakan perintah certutil untuk mengenkode data pengguna. Sebelum Anda dapat menggunakan file ini dengan AWS CLI, Anda harus menghapus baris pertama (BEGIN CERTIFICATE) dan terakhir (END CERTIFICATE).

  ```
  certutil -encode my_script.txt my_script_base64.txt
  notepad my_script_base64.txt
  ```

Menggunakan parameter `--attribute` dan `--value` untuk menggunakan file teks yang dienkode untuk menentukan data pengguna. Pastikan untuk menggunakan awalan `file://` untuk menentukan file.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Contoh: Hapus data pengguna dari instans yang dihentikan

Untuk menghapus data pengguna yang ada, gunakan modify-instance-attributeperintah sebagai berikut:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Contoh: Lihat data pengguna

Untuk mengambil data pengguna untuk sebuah contoh, gunakan describe-instance-attributeperintah. Dengandescribe-instance-attribute, AWS CLI tidak melakukan decoding base64 dari data pengguna untuk Anda.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

Berikut ini adalah contoh output dengan data pengguna berenkode base64.

```
{
    "UserData": {
        "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
    "InstanceId": "i-1234567890abcdef0"
}
```

- Di komputer Linux, gunakan`--query` opsi untuk mendapatkan data pengguna yang disandikan dan perintah base64 untuk mendekodekannya.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" | base64 --decode
  ```

- Di komputer Windows, gunakan`--query` opsi untuk mendapatkan data pengguna yang dikodekan dan perintah certutil untuk mendekodekannya. Perhatikan bahwa output dienkode disimpan dalam suatu file dan output yang didekode disimpan di file lain.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" >my_output.txt
  certutil -decode my_output.txt my_output_decoded.txt
  type my_output_decoded.txt
  ```

Berikut ini adalah output contoh.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Menggabungkan skrip shell dan arahan cloud-init

Secara default, Anda hanya dapat menyertakan satu tipe konten dalam data pengguna pada satu waktu. Namun, Anda dapat menggunakan tipe konten `text/cloud-config` dan `text/x-shellscript` dalam file bagian mime-multi untuk menyertakan skrip shell dan arahan cloud-init dalam data pengguna Anda.

Berikut ini menunjukkan format bagian mime-multi.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
--//--
```

Misalnya, data pengguna berikut menyertakan arahan cloud-init dan skrip bash shell. Arahan cloud-init membuat file (`/test-cloudinit/cloud-init.txt`), dan menulis `Created by cloud-init` ke file itu. Skrip bash shell membuat file (`/test-userscript/userscript.txt`) dan menulis `Created by bash shell script` ke file itu.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
- [ mkdir, /test-cloudinit ]
write_files:
- path: /test-cloudinit/cloud-init.txt
content: Created by cloud-init

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
mkdir test-userscript
touch /test-userscript/userscript.txt
echo "Created by bash shell script" >> /test-userscript/userscript.txt
--//--
```

Bagaimana Amazon EC2 menangani data pengguna untuk instans Windows

Pada instance Windows, agen peluncuran melakukan tugas yang terkait dengan data pengguna. Untuk informasi selengkapnya, lihat berikut ini:

- EC2Luncurkan v2
- EC2Peluncuran
- EC2Layanan Config

Untuk contoh perakitan `UserData` properti dalam CloudFormation template, lihat Base64 Encoded Property dan Base64 Encoded UserData Property dengan dan. UserData AccessKey SecretKey

Untuk contoh menjalankan perintah pada instance dalam grup Auto Scaling yang bekerja dengan kait siklus hidup, lihat Tutorial: Mengonfigurasi data pengguna untuk mengambil status siklus hidup target melalui metadata instans di Panduan Pengguna Amazon EC2 Auto Scaling.

Daftar Isi

- Skrip data pengguna
- Data pengguna terkompresi
- Eksekusi data pengguna
- Data pengguna dan Alat untuk Windows PowerShell

Skrip data pengguna

Untuk `EC2Config` atau `EC2Launch` untuk menjalankan skrip, Anda harus melampirkan skrip dalam tag khusus saat Anda menambahkannya ke data pengguna. Tag yang Anda gunakan tergantung pada apakah perintah berjalan di jendela Command Prompt (perintah batch) atau menggunakan WindowsPowerShell.

Jika Anda menentukan skrip batch dan skrip Windows, PowerShell skrip batch berjalan terlebih dahulu dan PowerShell skrip Windows berjalan berikutnya, terlepas dari urutan kemunculannya dalam data pengguna instance.

Jika Anda menggunakan AWS API, termasuk AWS CLI, dalam skrip data pengguna, Anda harus menggunakan profil instance saat meluncurkan instance. Profil instance menyediakan AWS kredensi yang sesuai yang diperlukan oleh skrip data pengguna untuk melakukan panggilan API. Untuk informasi selengkapnya, lihat Profil instans. Izin yang Anda tetapkan ke peran IAM bergantung pada layanan mana yang Anda panggil dengan API. Untuk informasi selengkapnya, lihat IAM role untuk Amazon EC2.

Tipe skrip

- Sintaks untuk skrip batch
- Sintaks untuk skrip Windows PowerShell
- Sintaks untuk skrip konfigurasi YAML
- Enkode Base64

Sintaks untuk skrip batch

Tentukan skrip batch menggunakan tanda `script`. Pisahkan perintah menggunakan jeda baris seperti yang ditunjukkan dalam contoh berikut.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

Secara default, skrip data pengguna dijalankan satu kali saat Anda meluncurkan instans. Untuk menjalankan skrip data pengguna setiap kali Anda melakukan boot ulang atau memulai instans, tambahkan `<persist>true</persist>` ke data pengguna.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<persist>true</persist>
```

EC2Luncurkan agen v2

Untuk menjalankan skrip data pengguna XMLsebagai proses terpisah dengan executeScript tugas EC2 Launch v2 di `UserData` panggung, tambahkan `<detach>true</detach>` ke data pengguna.

> **Note**
>
> detachTag tidak didukung oleh agen peluncuran sebelumnya.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<detach>true</detach>
```

Sintaks untuk skrip Windows PowerShell

AWS Windows AMIs menyertakan AWS Tools for Windows PowerShell, sehingga Anda dapat menentukan cmdlet ini dalam data pengguna. Jika Anda mengaitkan peran IAM dengan instans,

Anda tidak perlu menentukan kredensil ke cmdlet, karena aplikasi yang berjalan pada instance menggunakan kredenal peran untuk mengakses sumber daya (AWS misalnya, bucket Amazon S3).

Tentukan PowerShell skrip Windows menggunakan `<powershell>` tag. Pisahkan perintah menggunakan jeda baris. Tag `<powershell>` tidak peka huruf besar/kecil.

Contoh:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

Secara default, skrip data pengguna berjalan satu kali saat Anda meluncurkan instance. Untuk menjalankan skrip data pengguna setiap kali Anda melakukan boot ulang atau memulai instans, tambahkan `<persist>true</persist>` ke data pengguna.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Anda dapat menentukan satu atau lebih PowerShell argumen dengan `<powershellArguments>` tag. Jika tidak ada argumen yang diteruskan, EC2 EC2 Launch dan Launch v2 tambahkan argumen berikut secara default:`-ExecutionPolicy Unrestricted`.

Contoh:

```
<powershell>
    $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

EC2Luncurkan agen v2

Untuk menjalankan skrip data pengguna XMLsebagai proses terpisah dengan executeScript tugas EC2 Launch v2 di `UserData` panggung, tambahkan `<detach>true</detach>` ke data pengguna.

> **Note**
>
> detachTag tidak didukung oleh agen peluncuran sebelumnya.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

Sintaks untuk skrip konfigurasi YAML

Jika Anda menggunakan EC2 Launch v2 untuk menjalankan skrip, Anda dapat menggunakan format YAMAL. Untuk melihat tugas konfigurasi, detail, dan contoh untuk EC2 Launch v2, lihatEC2Luncurkan konfigurasi tugas v2.

Tentukan skrip YAML dengan tugas `executeScript`.

Contoh sintaks YAMG untuk menjalankan skrip PowerShell

```
version: 1.0
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
      New-Item $file -ItemType file
```

Contoh sintaks YAML untuk menjalankan skrip batch

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: batch
```

```
    runAs: localSystem
    content: |-
      echo Current date and time >> %SystemRoot%\Temp\test.log
      echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Enkode Base64

Jika Anda menggunakan API Amazon EC2 atau alat yang tidak melakukan enkode base64 pada data pengguna, Anda harus mengenkode sendiri data pengguna. Jika tidak, kesalahan akan dicatat tentang tidak dapat menemukan tanda `script` atau `powershell` yang akan dijalankan. Berikut ini adalah contoh yang menyandikan menggunakan Windows PowerShell .

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Berikut ini adalah contoh yang menerjemahkan menggunakan PowerShell .

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Untuk informasi lebih lanjut tentang pengkodean base64, lihat https://www.ietf. org/rfc/rfc4648.txt.

Data pengguna terkompresi

EC2Launch v2 mendukung data pengguna zip sebagai metode untuk mengirimkan data pengguna yang lebih besar dari batas 16 KB yang diberlakukan oleh IMDS. Untuk menggunakan fitur ini, kompres skrip data pengguna Anda ke dalam `.zip` arsip dan teruskan ke instans EC2 Anda. Ketika EC2 Launch v2 mendeteksi data pengguna terkompresi, secara otomatis membuka ritsleting skrip data pengguna terkompresi dan menjalankannya.

Seperti halnya data pengguna standar, jika Anda menggunakan Amazon EC2 API atau alat yang tidak melakukan pengkodean base64 data pengguna, Anda harus menyandikan sendiri data pengguna yang dikompresi. Untuk informasi selengkapnya tentang batas ukuran data pengguna dan pengkodean base64, lihat. Akses metadata instans untuk instans EC2

Eksekusi data pengguna

Secara default, semua AWS Windows AMIs memiliki eksekusi data pengguna yang diaktifkan untuk peluncuran awal. Anda dapat menentukan bahwa skrip data pengguna dijalankan setiap kali

instans di-boot ulang atau dimulai ulang. Atau, Anda dapat menentukan bahwa skrip data pengguna dijalankan setiap kali instans di-boot ulang atau dimulai ulang.

> **Note**
>
> Data pengguna tidak diaktifkan untuk dijalankan secara default setelah peluncuran awal. Agar data pengguna dapat dijalankan saat Anda melakukan boot ulang atau memulai instans, lihat Jalankan skrip selama reboot atau mulai berikutnya.

Skrip data pengguna dijalankan dari akun administrator lokal ketika kata sandi acak dibuat. Jika tidak, skrip data pengguna dijalankan dari akun Sistem.

Skrip peluncuran instance

Skrip dalam data pengguna instans dijalankan selama peluncuran awal instans. Jika tanda `persist` ditemukan, eksekusi data pengguna diaktifkan untuk boot ulang atau pemulaian berikutnya. File log untuk EC2 Launch v2, EC2 Launch, dan EC2 Config berisi output dari output standar dan aliran kesalahan standar.

EC2Luncurkan v2

File log untuk EC2 Launch v2 adalah`C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Folder `C:\ProgramData` mungkin tersembunyi. Untuk melihat folder, Anda harus menampilkan file dan folder yang tersembunyi.

Informasi berikut dicatat ketika data pengguna dijalankan:

- `Info: Converting user-data to yaml format` – Jika data pengguna disediakan dalam format XML
- `Info: Initialize user-data state` – Awal eksekusi data pengguna
- `Info: Frequency is: always` – Jika tugas data pengguna berjalan di setiap boot
- `Info: Frequency is: once` – Jika tugas data pengguna berjalan hanya sekali
- `Stage: postReadyUserData execution completed` – Akhir eksekusi data pengguna

EC2Peluncuran

File log untuk EC2 Launch adalah`C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

Folder `C:\ProgramData` mungkin tersembunyi. Untuk melihat folder, Anda harus menampilkan file dan folder yang tersembunyi.

Informasi berikut dicatat ketika data pengguna dijalankan:

- `Userdata execution begins` – Awal eksekusi data pengguna
- `<persist> tag was provided: true` – Jika tanda yang masih ada ditemukan
- `Running userdata on every boot` – Jika tanda yang masih ada ditemukan
- `<powershell> tag was provided.. running powershell content` – Jika tanda powershell ditemukan
- `<script> tag was provided.. running script content` – Jika tanda skrip ditemukan
- `Message: The output from user scripts` – Jika skrip data pengguna dijalankan, maka outputnya dicatat

EC2Config

File log untuk EC2 Config adalah. `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log` Informasi berikut dicatat ketika data pengguna dijalankan:

- `Ec2HandleUserData: Message: Start running user scripts` – Awal eksekusi data pengguna
- `Ec2HandleUserData: Message: Re-enabled userdata execution` – Jika tanda yang masih ada ditemukan
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>` – Jika tanda yang masih ada tidak ditemukan
- `Ec2HandleUserData: Message: The output from user scripts` – Jika skrip data pengguna dijalankan, maka outputnya dicatat

Jalankan skrip selama reboot atau mulai berikutnya

Saat Anda memperbarui data pengguna instans, konten data pengguna yang diperbarui secara otomatis tercermin dalam metadata instans saat berikutnya Anda me-reboot atau memulai instance.

Namun, tergantung pada agen peluncuran yang diinstal, konfigurasi tambahan mungkin diperlukan untuk mengonfigurasi skrip data pengguna agar berjalan pada reboot atau mulai berikutnya.

Jika Anda memilih opsi Shutdown with Sysprep, skrip data pengguna berjalan saat instance dimulai atau reboot berikutnya, bahkan jika Anda tidak mengaktifkan eksekusi data pengguna untuk reboot atau memulai berikutnya.

Untuk instruksi untuk mengaktifkan eksekusi data pengguna, pilih tab yang cocok dengan agen peluncuran Anda.

EC2Launch v2

Tidak seperti EC2 Launch v1, EC2 Launch v2 mengevaluasi tugas data pengguna pada setiap boot. Tidak perlu menjadwalkan tugas data pengguna secara manual. Data pengguna berjalan berdasarkan frekuensi yang disertakan atau opsi bertahan.

Untuk skrip data pengguna XHTML

Untuk menjalankan skrip data pengguna pada setiap boot, tambahkan `<persist>true</persist>` bendera ke data pengguna. Jika flag persisten tidak disertakan, skrip data pengguna hanya berjalan pada boot awal.

Untuk data pengguna YAMG

- Untuk menjalankan tugas dalam data pengguna pada boot awal, atur tugas `frequency` ke`once`.
- Untuk menjalankan tugas dalam data pengguna pada setiap boot, atur tugas `frequency` ke`always`.

EC2Launch

1. Hubungkan ke instans Windows Anda.
2. Buka jendela PowerShell perintah dan jalankan salah satu perintah berikut:

   Jalankan sekali

   Untuk menjalankan data pengguna sekali pada boot berikutnya, gunakan `-Schedule` bendera.

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
   Schedule
   ```

Jalankan pada semua sepatu bot berikutnya

Untuk menjalankan data pengguna pada semua boot berikutnya, gunakan `-SchedulePerBoot` bendera.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

3. Putuskan sambungan dari instans Windows Anda. Untuk menjalankan skrip yang diperbarui saat instans dimulai lagi nanti, hentikan instans dan perbarui data pengguna.

EC2Config

1. Hubungkan ke instans Windows Anda.
2. Buka `C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe`.
3. Untuk Data Pengguna , pilih Aktifkan UserData eksekusi untuk layanan berikutnya dimulai .
4. Putuskan sambungan dari instans Windows Anda. Untuk menjalankan skrip yang diperbarui saat instans dimulai lagi nanti, hentikan instans dan perbarui data pengguna.

Data pengguna dan Alat untuk Windows PowerShell

Anda dapat menggunakan Alat untuk Windows PowerShell untuk menentukan, memodifikasi, dan melihat data pengguna untuk instance Anda. Untuk informasi tentang melihat data pengguna dari instans Anda menggunakan metadata instans, lihat Akses metadata instans untuk instans EC2. Untuk informasi tentang data pengguna dan AWS CLI, lihatData pengguna dan AWS CLI.

Contoh: Tentukan data pengguna instans saat peluncuran

Buat file teks dengan data pengguna instans. Untuk menjalankan skrip data pengguna setiap kali Anda melakukan boot ulang atau memulai instans, tambahkan `<persist>true</persist>`, seperti yang ditunjukkan pada contoh berikut.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Untuk menentukan data pengguna instance saat Anda meluncurkan instance Anda, gunakan New-EC2Instanceperintah. Perintah ini tidak melakukan enkode base64 pada data pengguna untuk Anda. Gunakan perintah berikut untuk menyandikan data pengguna dalam file teks bernama.`script.txt`

```
PS C:\> $Script = Get-Content -Raw script.txt
PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Gunakan parameter `-UserData` untuk meneruskan data pengguna ke perintah New-EC2Instance.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
    -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
    -UserData $UserData
```

Contoh: Perbarui data pengguna instans untuk instans yang dihentikan

Anda dapat memodifikasi data pengguna dari instance yang dihentikan menggunakan Edit-EC2InstanceAttributeperintah.

Buat file teks dengan skrip baru. Gunakan perintah berikut untuk menyandikan data pengguna dalam file teks bernama.`new-script.txt`

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Gunakan parameter `-UserData` dan `-Value` untuk menentukan data pengguna.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Contoh: Lihat data pengguna instans

Untuk mengambil data pengguna untuk sebuah contoh, gunakan Get-EC2InstanceAttributeperintah.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

Berikut ini adalah output contoh. Perhatikan bahwa data pengguna dienkode.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Gunakan perintah berikut untuk menyimpan data pengguna yang dienkode dalam variabel dan kemudian mendekodekannya.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

Berikut ini adalah contoh output.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Contoh: Ubah nama instans agar sesuai dengan nilai tanda

Anda dapat menggunakan Get-EC2Tagperintah untuk membaca nilai tag, mengganti nama instance pada boot pertama agar sesuai dengan nilai tag, dan reboot. Untuk menjalankan perintah ini dengan sukses, Anda harus memiliki peran dengan izin `ec2:DescribeTags` yang dilampirkan ke instans karena informasi tag diambil dengan panggilan API. Untuk informasi selengkapnya tentang izin pengaturan menggunakan peran IAM, lihat. Melampirkan IAM role ke instans

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
    $instanceId = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" =
 $token} -Method GET -Uri 'http://169.254.169.254/latest/meta-data/instance-id' -
UseBasicParsing
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
```

```
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
 $instanceId = (Invoke-WebRequest http://169.254.169.254/latest/meta-data/instance-
id -UseBasicParsing).content
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Anda juga dapat mengganti nama instans menggunakan tanda dalam metadata instans, jika instans Anda dikonfigurasi untuk mengakses tanda dari metadata instans. Lihat informasi yang lebih lengkap di Lihat tag untuk instans EC2 Anda menggunakan metadata instans.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
```

```
 $nameValue = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri 'http://169.254.169.254/latest/meta-data/tags/instance/Name' -
UseBasicParsing
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Identifikasi setiap instance yang diluncurkan dalam satu permintaan

Contoh ini menunjukkan bagaimana Anda dapat menggunakan data pengguna dan metadata instans untuk mengonfigurasi instans Amazon EC2 Anda.

> **Note**
>
> Contoh di bagian ini menggunakan IPv4 alamat IMDS:`169.254.169.254`. Jika Anda mengambil metadata instans untuk instans EC2 melalui IPv6 alamat, pastikan Anda mengaktifkan dan menggunakan alamat sebagai gantinya:. IPv6 `[fd00:ec2::254]` IPv6 Alamat IMDS kompatibel dengan IMDSv2 perintah. IPv6 Alamat hanya dapat diakses pada instance berbasis Nitro di subnet yang IPv6 didukung (tumpukan ganda atau hanya). IPv6

Alice ingin meluncurkan empat instans AMI basis data favoritnya, di mana instans pertama bertindak sebagai instans asli dan tiga instans lainnya bertindak sebagai replika. Saat meluncurkannya, dia ingin menambahkan data pengguna tentang strategi replikasi untuk setiap replika. Dia sadar bahwa data ini akan tersedia untuk keempat instans, jadi dia perlu menyusun data pengguna dengan cara yang memungkinkan setiap instans untuk mengenali bagian mana yang dapat diterapkan padanya. Dia bisa melakukan ini dengan menggunakan nilai metadata instans `ami-launch-index`, yang akan unik untuk setiap instans. Jika ia memulai lebih dari satu instans secara bersamaan, maka `ami-launch-index` menunjukkan urutan peluncuran instans tersebut. Nilai instans pertama yang diluncurkan adalah `0`.

Berikut adalah data pengguna yang telah dibuat oleh Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

Data `replicate-every=1min` menentukan konfigurasi replika pertama, `replicate-every=5min` menentukan konfigurasi replika kedua, dan seterusnya. Alice memutuskan untuk memberikan data ini sebagai string ASCII dengan simbol pipa (`|`) yang membatasi data untuk instans terpisah.

Alice meluncurkan empat instans menggunakan perintah run-instances, dengan menentukan data pengguna.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Setelah diluncurkan, semua instans memiliki salinan data pengguna dan metadata umum yang ditampilkan di sini:

- ID AMI: ami-0abcdef1234567890
- ID Reservasi: r-1234567890abcabc0
- Kunci publik: tidak ada
- Nama grup keamanan: default
- Tipe instans: t2.micro

Namun, setiap instance memiliki metadata unik, seperti yang ditunjukkan pada tabel berikut.

Metadata	Nilai
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

Metadata	Nilai
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

Metadata	Nilai
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

Metadata	Nilai
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice bisa menggunakan nilai `ami-launch-index` untuk menentukan bagian mana dari data pengguna yang berlaku untuk instans tertentu.

1. Dia terhubung salah satu instans, dan mengambil `ami-launch-index` untuk instans tersebut agar dapat memastikan bahwa instans itu adalah salah satu replika:

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/
   token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   ```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-launch-index
2
```

Untuk langkah-langkah berikut, IMDSv2 permintaan menggunakan token yang disimpan dari IMDSv2 perintah sebelumnya, dengan asumsi token belum kedaluwarsa.

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
2
```

2. Dia menyimpan `ami-launch-index` sebagai variabel.

   IMDSv2

   ```
   [ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

3. Dia menyimpan data pengguna sebagai variabel.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. Akhirnya, Alice menggunakan perintah cut untuk mengekstrak bagian dari data pengguna yang berlaku untuk instans itu.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

IMDSv1

```
[ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
replicate-every=5min
```

Mendeteksi apakah host adalah sebuah EC2 instance

Anda mungkin perlu tahu apakah aplikasi atau situs web Anda berjalan pada sebuah EC2 instance, terutama jika Anda memiliki lingkungan komputasi campuran. Anda dapat menggunakan salah satu opsi berikut untuk menentukan apakah host untuk aplikasi atau situs web Anda adalah sebuah EC2 instance.

Opsi

- Memeriksa dokumen identitas instans
- Periksa sistem UUID
- Periksa pengenal pembuatan mesin virtual sistem

Memeriksa dokumen identitas instans

Setiap instance memiliki dokumen identitas instance yang ditandatangani yang dapat Anda verifikasi secara kriptografi. Anda dapat menemukan dokumen-dokumen ini menggunakan Layanan Metadata Instance (IMDS).

Untuk informasi selengkapnya, lihat Dokumen identitas instans.

Periksa sistem UUID

Anda bisa mendapatkan UUID sistem dan melihat oktet awal UUID untuk `EC2` (di Linux, ini mungkin huruf kecil). `ec2` Metode ini cepat, tetapi berpotensi tidak akurat karena ada kemungkinan kecil bahwa sistem yang bukan EC2 instance dapat memiliki UUID yang dimulai dengan karakter ini. Selain itu, beberapa versi SMBIOS menggunakan format endian kecil, yang tidak termasuk `EC2` di awal UUID. Ini mungkin terjadi pada EC2 contoh yang menggunakan SMBIOS 2.4 untuk Windows, atau untuk distribusi Linux selain Amazon Linux yang memiliki implementasi SMBIOS sendiri.

Contoh Linux: Dapatkan UUID dari DMI (hanya HVM) AMIs

Gunakan perintah berikut untuk mendapatkan UUID menggunakan Desktop Management Interface (DMI):

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Dalam contoh output berikut, UUID dimulai dengan "EC2“, yang menunjukkan bahwa sistem mungkin sebuah EC2 instance.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

Dalam contoh output berikut, UUID direpresentasikan dalam format little-endian.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Atau, untuk instans yang dibangun di sistem Nitro, Anda dapat menggunakan perintah berikut:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Jika output adalah ID instance, sebagai contoh output berikut, sistem adalah sebuah EC2 instance:

```
i-0af01c0123456789a
```

Contoh Linux: Dapatkan UUID dari hypervisor (hanya PV) AMIs

Gunakan perintah berikut untuk mendapatkan UUID dari hypervisor:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

Dalam contoh output berikut, UUID dimulai dengan “ec2", yang menunjukkan bahwa sistem mungkin sebuah instance. EC2

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Contoh Windows: Dapatkan UUID menggunakan WMI atau Windows PowerShell

Gunakan baris perintah Instrumentasi Manajemen Windows (WMIC) sebagai berikut:

```
wmic path win32_computersystemproduct get uuid
```

Atau, jika Anda menggunakan Windows PowerShell, gunakan Get-WmiObject cmdlet sebagai berikut:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

Dalam contoh output berikut, UUID dimulai dengan "EC2“, yang menunjukkan bahwa sistem mungkin sebuah EC2 instance.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Untuk instans yang menggunakan SMBIOS 2.4, UUID mungkin direpresentasikan dalam format little-endian; misalnya:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Periksa pengenal pembuatan mesin virtual sistem

Pengidentifikasi generasi mesin virtual terdiri dari buffer unik 128-bit yang diartikan sebagai pengidentifikasi integer acak kriptografi. Anda dapat mengambil pengenal pembuatan mesin virtual untuk mengidentifikasi instans Amazon Elastic Compute Cloud Anda. Pengidentifikasi generasi diekspos dalam sistem operasi tamu instans melalui entri tabel ACPI. Nilai akan berubah jika mesin Anda diklona, disalin, atau diimpor ke AWS, seperti dengan VM Import/Export.

Contoh: Ambil pengenal generasi mesin virtual dari Linux

Anda dapat menggunakan perintah berikut untuk mengambil pengenal pembuatan mesin virtual dari instans Anda yang menjalankan Linux.

Amazon Linux 2

1. Perbarui paket perangkat lunak yang ada, jika perlu, menggunakan perintah berikut:

   ```
   sudo yum update
   ```

2. Jika perlu, sumber paket busybox dengan perintah berikut ini:

```
sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
```

3. Jika perlu, instal paket prasyarat menggunakan perintah berikut:

```
sudo yum install busybox.rpm iasl -y
```

4. Jalankan `iasl` perintah berikut untuk menghasilkan output dari tabel ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

5. Jalankan perintah berikut untuk meninjau output dari `iasl` perintah:

```
cat SSDT2.dsl
```

Output harus menghasilkan ruang alamat yang diperlukan untuk mengambil pengenal pembuatan mesin virtual:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
```

```
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

6. (Opsional) Tingkatkan izin terminal Anda untuk langkah-langkah yang tersisa dengan perintah berikut:

```
sudo -s
```

7. Gunakan perintah berikut untuk menyimpan ruang alamat yang dikumpulkan sebelumnya:

```
VMGN_ADDR=0xFED01000
```

8. Gunakan perintah berikut untuk melakukan iterasi melalui ruang alamat dan membuat pengidentifikasi pembuatan mesin virtual:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Ambil pengidentifikasi pembuatan mesin virtual dari file output dengan perintah berikut:

```
cat vmgenid ; echo
```

Output Anda harus serupa dengan berikut:

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Perbarui paket perangkat lunak yang ada, jika perlu, menggunakan perintah berikut:

```
sudo apt update
```

2. Jika perlu, instal paket prasyarat menggunakan perintah berikut:

```
sudo apt install busybox iasl -y
```

3. Jalankan `iasl` perintah berikut untuk menghasilkan output dari tabel ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Jalankan perintah berikut untuk meninjau output dari `iasl` perintah:

```
cat SSDT2.dsl
```

Output harus menghasilkan ruang alamat yang diperlukan untuk mengambil pengenal pembuatan mesin virtual:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
```

```
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
```

```
        })
    }
}
}
```

5. (Opsional) Tingkatkan izin terminal Anda untuk langkah-langkah yang tersisa dengan perintah berikut:

```
sudo -s
```

6. Gunakan perintah berikut untuk menyimpan ruang alamat yang dikumpulkan sebelumnya:

```
VMGN_ADDR=0xFED01000
```

7. Gunakan perintah berikut untuk melakukan iterasi melalui ruang alamat dan membuat pengidentifikasi pembuatan mesin virtual:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Ambil pengidentifikasi pembuatan mesin virtual dari file output dengan perintah berikut:

```
cat vmgenid ; echo
```

   Output Anda harus serupa dengan berikut:

```
EC2F335D979132C4165896753E72BD1C
```

Contoh: Ambil pengenal generasi mesin virtual dari Windows

Anda dapat membuat sampel aplikasi untuk mengambil pengidentifikasi pembuatan mesin virtual dari instans Anda yang menjalankan Windows. Untuk informasi selengkapnya, lihat Mendapatkan pengidentifikasi pembuatan mesin virtual di dokumentasi Microsoft.

Dokumen identitas instans untuk EC2 instans Amazon

Setiap instans yang Anda luncurkan memiliki dokumen identitas instans yang memberikan informasi tentang instans tersebut. Anda dapat menggunakan dokumen identitas instans untuk memvalidasi atribut instans.

Dokumen identitas instans dibuat saat instans dihentikan dan dimulai, dimulai ulang, atau diluncurkan. Anda dapat mengakses dokumen identitas instance untuk sebuah instance melalui Layanan Metadata Instans (IMDS). Untuk instruksinya, lihatAmbil dokumen identitas instance.

Dokumen identitas instance menggunakan format JSON plaintext. Ini termasuk informasi berikut.

Data	Deskripsi
`accountId`	ID AWS akun yang meluncurkan instance.
`architecture`	Arsitektur AMI yang digunakan untuk meluncurkan instans (i386 | x86_64 | arm64).
`availabilityZone`	Nama Availability Zone di mana instance berjalan. Misalnya, `us-east-1` . Perlu diingat bahwa nama Availability Zone mungkin berbeda di seluruh AWS akun.
`billingProducts`	Produk penagihan instans.
`devpayProductCodes`	Telah usang.
`imageId`	ID AMI yang digunakan untuk meluncurkan instans.
`instanceId`	ID instans.
`instanceType`	Tipe instans dari instans tersebut.
`kernelId`	ID kernel yang terkait dengan instans, jika ada.
`marketplaceProductCodes`	Kode AWS Marketplace produk AMI digunakan untuk meluncurkan instance.
`pendingTime`	Tanggal dan waktu instans diluncurkan.
`privateIp`	Alamat IP pribadi dari instance. Untuk instance IPv4 -only dan dual-stack, ini berisi alamat. IPv4 Untuk instance IPv6 -only, ini berisi alamat. IPv6
`ramdiskId`	ID dari RAM disk yang terkait dengan instans, jika ada.
`region`	Wilayah tempat instans berjalan.

Data	Deskripsi
`version`	Versi format dokumen identitas instans.

Mengambil dokumen identitas instance untuk sebuah instance EC2

Dokumen identitas instance untuk EC2 instans Amazon menggunakan format JSON plaintext. Untuk deskripsi isi dokumen identitas instance, lihatthe section called “Dokumen identitas instans”.

Dokumen identitas instance disimpan dalam metadata instance untuk instance, dalam kategori data `instance-identity/document` dinamis. Anda mengakses dokumen identitas instance untuk sebuah instance dengan menghubungkan ke instance dan mengambilnya dari metadata instance.

Anda dapat mengakses metadata instance menggunakan IPv4 alamat 169.254.169.254 atau alamat. IPv6 fd00:ec2::254 Ini adalahAlamat link-lokal, artinya Anda dapat mengaksesnya hanya dari instance. Contoh di halaman ini menggunakan IPv4 alamat IMDS:169.254.169.254. Untuk mengambil metadata instance untuk EC2 instance di atas, gunakan. IPv6 fd00:ec2::254

Untuk memverifikasi keaslian dokumen identitas instance setelah Anda mengambilnya, lihat. Verifikasi dokumen identitas instance

IMDSv2

Linux

Jalankan perintah berikut dari instance Linux Anda untuk mengambil dokumen identitas instance.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda untuk mengambil dokumen identitas instance.

```
[string]$token = (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} `
```

```
    -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing).Content
```

```
(Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $token} `
    -Uri 'http://169.254.169.254/latest/dynamic/instance-identity/document' -
UseBasicParsing).Content
```

IMDSv1

Linux

Jalankan perintah berikut dari instance Linux Anda untuk mengambil dokumen identitas instance.

```
curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda untuk mengambil dokumen identitas instance.

```
(Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/
document).Content
```

Berikut ini adalah output contoh.

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
```

```
}
```

Verifikasi dokumen identitas instans untuk EC2 instans Amazon

Jika Anda bermaksud menggunakan konten dokumen identitas instans untuk tujuan penting, Anda harus memverifikasi konten dan keaslian sebelum menggunakannya.

Dokumen identitas instans plaintext disertai dengan tiga tanda tangan yang di-hash dan dienkripsi. Anda dapat menggunakan tanda tangan ini untuk memverifikasi asal dan keaslian dokumen identitas instans serta informasi yang disertakan. Tanda tangan berikut disediakan:

- Base64-Encoded Signature—Ini adalah SHA256 hash berenkode base64 dari dokumen identitas instance yang dienkripsi menggunakan key pair RSA.
- PKCS7 Signature—ini adalah SHA1 hash dari dokumen identitas instance yang dienkripsi menggunakan key pair DSA.
- Tanda tangan RSA-2048 — Ini adalah SHA256 hash dari dokumen identitas instance yang dienkripsi menggunakan key pair RSA-2048.

Setiap tanda tangan tersedia di titik akhir yang berbeda dalam metadata instans. Anda dapat menggunakan salah satu dari tanda tangan ini, tergantung persyaratan hashing dan enkripsi Anda. Untuk memverifikasi tanda tangan, Anda harus menggunakan sertifikat AWS publik yang sesuai.

Opsi

- Opsi 1: Verifikasi dokumen identitas contoh menggunakan PKCS7 tanda tangan
- Opsi 2: Verifikasi dokumen identitas instance menggunakan tanda tangan yang disandikan base64
- Opsi 3: Verifikasi dokumen identitas instance menggunakan tanda tangan RSA-2048

Opsi 1: Verifikasi dokumen identitas contoh menggunakan PKCS7 tanda tangan

Topik ini menjelaskan cara memverifikasi dokumen identitas instance menggunakan PKCS7 tanda tangan dan sertifikat publik AWS DSA.

Instans Linux

Untuk memverifikasi dokumen identitas instance menggunakan PKCS7 tanda tangan dan sertifikat publik AWS DSA

1. Hubungkan dengan instans.

2. Ambil PKCS7 tanda tangan dari metadata instance dan tambahkan ke file baru bernama `pkcs7` bersama dengan header dan footer yang diperlukan. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7 >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
    >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

3. Temukan sertifikat publik DSA untuk Wilayah Anda di AWS sertifikat publik misalnya tanda tangan dokumen identitas dan tambahkan konten ke file baru yang bernama `certificate`.

4. Gunakan perintah OpenSSL smime untuk memverifikasi tanda tangan. Masukkan opsi `-verify` untuk menunjukkan bahwa tanda tangan perlu diverifikasi, dan opsi `-noverify` untuk menunjukkan bahwa sertifikat tidak perlu diverifikasi.

   ```
   $ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
    document
   ```

   Jika tanda tangan valid, pesan `Verification successful` muncul.

   Perintah tersebut juga menulis konten dokumen identitas instans ke file baru bernama `document`. Anda dapat membandingkan konten dokumen identitas instans dari metadata instans dengan konten file ini menggunakan perintah berikut.

   ```
   $ openssl dgst -sha256 < document
   ```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Jika tanda tangan tidak dapat diverifikasi, kontak Dukungan.

Instans Windows

Prasyarat

Prosedur ini membutuhkan kelas `System.Security` Microsoft.NET Core. Untuk menambahkan kelas ke PowerShell sesi Anda, jalankan perintah berikut.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Perintah menambahkan kelas ke PowerShell sesi saat ini saja. Jika Anda memulai sesi baru, Anda harus menjalankan perintah lagi.

Untuk memverifikasi dokumen identitas instance menggunakan PKCS7 tanda tangan dan sertifikat publik AWS DSA

1. Hubungkan dengan instans.
2. Ambil PKCS7 tanda tangan dari metadata instance, ubah menjadi array byte, dan tambahkan ke variabel bernama. `$Signature` Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-
   metadata-token-ttl-seconds' = '21600'} -Uri http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} -Uri http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7).Content)
   ```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Uri
 http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

3. Ambil dokumen identitas instans plaintext dari metadata instans, ubah menjadi array byte, dan tambahkan ke variabel bernama `$Document`. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} -Uri http://169.254.169.254/latest/
   dynamic/instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Temukan sertifikat publik DSA untuk Wilayah Anda di AWS sertifikat publik misalnya tanda tangan dokumen identitas dan tambahkan konten ke file baru yang bernama `certificate.pem`.
5. Ekstrak sertifikat dari file sertifikat dan simpan dalam variabel bernama `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifikasi tanda tangan.

   ```
   PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
   ```

   ```
   PS C:\> $SignatureDocument.Decode($Signature)
   ```

   ```
   PS C:\> $SignatureDocument.CheckSignature($Store, $true)
   ```

Jika tanda tangan valid, perintah tidak mengembalikan keluaran. Jika tanda tangan tidak dapat diverifikasi, perintah menampilkan `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Jika tanda tangan tidak dapat diverifikasi, hubungi AWS Dukungan.

7. Validasi konten dokumen identitas instans.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Jika konten dokumen identitas instans valid, perintah mengembalikan `True`. Jika dokumen identitas instance tidak dapat divalidasi, hubungi AWS Dukungan.

Opsi 2: Verifikasi dokumen identitas instance menggunakan tanda tangan yang disandikan base64

Topik ini menjelaskan cara memverifikasi dokumen identitas instance menggunakan tanda tangan berenkode base64 dan sertifikat publik RSA AWS .

Instans Linux

Untuk memvalidasi dokumen identitas instance menggunakan tanda tangan berenkode base64 dan sertifikat publik RSA AWS

1. Hubungkan dengan instans.
2. Ambil tanda tangan berenkode base64 dari metadata instans, konversikan ke biner, dan tambahkan tanda tangan tersebut ke file bernama `signature`. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

   IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/signature | base64 -d >> signature
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
 base64 -d >> signature
```

3. Ambil dokumen identitas instans plaintext dari metadata instans dan tambahkan ke file bernama `document`. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```

4. Tambahkan sertifikat publik RSA untuk Wilayah Anda di AWS sertifikat publik misalnya tanda tangan dokumen identitas dan tambahkan konten ke file baru yang bernama `certificate`.
5. Ekstrak kunci publik dari sertifikat publik AWS RSA dan simpan ke file bernama`key`.

   ```
   $ openssl x509 -pubkey -noout -in certificate >> key
   ```

6. Gunakan perintah OpenSSL dgst untuk memverifikasi dokumen identitas instans.

   ```
   $ openssl dgst -sha256 -verify key -signature signature document
   ```

   Jika tanda tangannya valid, file`Verification successful` pesan muncul.

   Perintah tersebut juga menulis konten dokumen identitas instans ke file baru bernama `document`. Anda dapat membandingkan konten dokumen identitas instans dari metadata instans dengan konten file ini menggunakan perintah berikut.

   ```
   $ openssl dgst -sha256 < document
   ```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Jika tanda tangan tidak dapat diverifikasi, kontak Dukungan.

Instans Windows

Untuk memvalidasi dokumen identitas instance menggunakan tanda tangan berenkode base64 dan sertifikat publik RSA AWS

1. Hubungkan dengan instans.
2. Ambil tanda tangan berenkode base64 dari metadata instans, konversikan ke array bita, dan tambahkan tanda tangan tersebut ke variabel bernama `$Signature`. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/signature).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
   ```

3. Ambil dokumen identitas instans plaintext dari metadata instans, ubah menjadi array byte, dan tambahkan ke variabel bernama `$Document`. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Tambahkan sertifikat publik RSA untuk Wilayah Anda di AWS sertifikat publik misalnya tanda tangan dokumen identitas dan tambahkan konten ke file baru yang bernama `certificate.pem`.
5. Verifikasi dokumen identitas instans.

```
PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
```

Jika tanda tangan valid, perintah mengembalikan `True`. Jika tanda tangan tidak dapat diverifikasi, kontak Dukungan.

Opsi 3: Verifikasi dokumen identitas instance menggunakan tanda tangan RSA-2048

Topik ini menjelaskan cara memverifikasi dokumen identitas instance menggunakan tanda tangan RSA-2048 dan sertifikat publik RSA-2048. AWS

Instans Linux

Untuk memverifikasi dokumen identitas instance menggunakan tanda tangan RSA-2048 dan sertifikat publik RSA-2048 AWS

1. Hubungkan dengan instans.
2. Ambil tanda tangan RSA-2048 dari metadata instans dan tambahkan ke file bernama `rsa2048` beserta header dan footer yang diperlukan. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
 && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/rsa2048 >> rsa2048 \
 && echo "" >> rsa2048 \
 && echo "-----END PKCS7-----" >> rsa2048
```

IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
 && curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
 >> rsa2048 \
 && echo "" >> rsa2048 \
 && echo "-----END PKCS7-----" >> rsa2048
```

3. Tambahkan sertifikat publik RSA-2048 untuk Wilayah Anda di AWS sertifikat publik misalnya tanda tangan dokumen identitas dan tambahkan konten ke file baru yang bernama `certificate`.
4. Gunakan perintah OpenSSL smime untuk memverifikasi tanda tangan. Masukkan opsi `-verify` untuk menunjukkan bahwa tanda tangan perlu diverifikasi, dan opsi `-noverify` untuk menunjukkan bahwa sertifikat tidak perlu diverifikasi.

   ```
   $ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
    tee document
   ```

   Jika tanda tangan valid, pesan `Verification successful` muncul. Jika tanda tangan tidak dapat diverifikasi, kontak Dukungan.

Instans Windows

Prasyarat

Prosedur ini membutuhkan kelas `System.Security` Microsoft.NET Core. Untuk menambahkan kelas ke PowerShell sesi Anda, jalankan perintah berikut.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Perintah menambahkan kelas ke PowerShell sesi saat ini saja. Jika Anda memulai sesi baru, Anda harus menjalankan perintah lagi.

Untuk memverifikasi dokumen identitas instance menggunakan tanda tangan RSA-2048 dan sertifikat publik RSA-2048 AWS

1. Hubungkan dengan instans.
2. Ambil tanda tangan RSA-2048 dari metadata instans, ubah ke byte array, dan tambahkan ke variabel bernama `$Signature`. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/rsa2048).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
   ```

3. Ambil dokumen identitas instans plaintext dari metadata instans, ubah menjadi array byte, dan tambahkan ke variabel bernama `$Document`. Gunakan salah satu perintah berikut, tergantung pada versi IMDS yang digunakan oleh instans.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Tambahkan sertifikat publik RSA-2048 untuk Wilayah Anda di AWS sertifikat publik misalnya tanda tangan dokumen identitas dan tambahkan konten ke file baru yang bernama `certificate.pem`.
5. Ekstrak sertifikat dari file sertifikat dan simpan dalam variabel bernama `$Store`.

```
PS C:\> $Store =
 [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
Path certificate.pem)))
```

6. Verifikasi tanda tangan.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Jika tanda tangan valid, perintah tidak mengembalikan keluaran. Jika tanda tangan tidak dapat diverifikasi, perintah menampilkan `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Jika tanda tangan tidak dapat diverifikasi, hubungi AWS Dukungan.

7. Validasi konten dokumen identitas instans.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Jika konten dokumen identitas instans valid, perintah mengembalikan `True`. Jika dokumen identitas instance tidak dapat divalidasi, hubungi AWS Dukungan.

AWS sertifikat publik misalnya tanda tangan dokumen identitas

Sertifikat AWS publik berikut dapat digunakan untuk memverifikasi isi dokumen identitas instans seperti yang dijelaskan dalamVerifikasi dokumen identitas instance.

Pastikan bahwa Anda menggunakan sertifikat yang benar untuk Wilayah Anda dan untuk prosedur verifikasi yang Anda gunakan. Jika Anda memverifikasi PKCS7 tanda tangan, gunakan sertifikat DSA. Jika Anda memverifikasi tanda tangan yang dikodekan base64, gunakan sertifikat RSA. Jika Anda memverifikasi tanda tangan RSA-2048, gunakan sertifikat RSA-2048.

Perluas setiap Wilayah di bawah ini untuk melihat sertifikat khusus Wilayah.

AS Timur (Virginia N.) — us-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
```

```
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

AS Timur (Ohio) — us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
```

```
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

AS Barat (California Utara) — us-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
```

```
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

AS Barat (Oregon) — us-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
```

```
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

Afrika (Cape Town) — af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
```

```
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Asia Pasifik (Hong Kong) – ap-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
```

```
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
```

```
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----
```

Asia Pasifik (Hyderabad) — ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLj9CMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+sFcobrjvcAYm0PNRD8f4R1jAzvoLt2+qGeOTAyO1Httj6cmsYN3AP1hN5iYuppFiYsl2eNPa/
CD0Vg0BAfDFlV5rzjpA0j7TJabVh4kj7JvtD+xYMi6wEQA4x6SPONY4OeZ2+8o/
HS8nucpWDVdPRO6ciWUlMhjmDmwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAy6sgTdRkTqELHBeWj69q60xHyUmsWqHAQ
TGGbYP0yP2qfMl0cCImzRI5W0gn8gogdervfeT7nH5ih0TWEy/QDWfkQ601L4erm4yh4YQq8vcqAPSkf04N
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Asia Pasifik (Jakarta) — ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhvO/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b
+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV
+OkP9ab5wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs
+87w/g9lNwUnUt0ZHYyh2tuBG6hVJuUEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyyc Gt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
-----END CERTIFICATE-----
```

Asia Pasifik (Malaysia) - ap-tenggara - 5

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQC5X6U+vgoLEDAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMxMjU3NTRaGA8y
```

```
MDUwMDEwMzEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAIzEMPCIPFfOYCg4
BCjKGyl60wOfmwHPzSOXZ3Z2wS/LYNHUtHGwtVNePSTyCu/CuZF6gC9n/wBORtQp
+SSkn+weGc/BmUA1mp/vrN7v+aSCgKJoO+sgpa1PPOgNvUaMw6O5odsZWQCMSjkU
6RTo/PL2v/tMfiCocF4ghvyRC6hvAhUA0VoObKC2IXzXgVvRRupo4qHbcm8CgYAe
bbNuawh3rAxkFvUs9FPzW5E+xllG16Z//61PENKqonmk+zBiBdiIlS1F6ZqmTqkI
z5+qfSt1m3pb3j2W0NT7lEDFvy8Gr6Y2vohCHmL+T1u1Yy4PeqbgrFwcen7y7WoO
/KCV7Y9/ODQMMyuAzT3h5wJNweT7L5MUN8JYpZSi3QOBhAACgYBqaDuG2u6V91Qj
K2wEAElxaaRaNo/ewg/wWDmHYqoeHOR0HfuFCYgASE9f7ULqYtX1VURcgcjw9XN4
BDmPilXvfi04INPTnw4IxFJKDzzC0kVH7esVas982Po8v3megH32H9Rl87r7UG1c
ZEbkSkKVX6YKYg1PR3rfjXgdwVZv/zAJBgcqhkjOOAQDAzAAMC0CFFWeRe2fYW2i
6mMd26Wzbx87Y0DXAhUAoPCnF+5hGJw0jT9aL7QsgcfLi9Y=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMuBl6rhZCJKMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFuKydxZsordNH7bLwIluEGOkX7/CdLdpeqkDKEhQkFwzpRxaX4EAlkGh2/o7D
8qneC9cGQhqSG5WVVBrmZG7sfkFOM4m1AtY++kfv+MYto1VFgLk1xJbkpq1r4YeQ
Ul+ZsJYsZpyX/t+g8s7rW0OVcBsYx4L75bf34z38mwK8PQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBADD9C4pWL8RUvF1CJW8kExj35xmozlFlmrKs8Zpi8+Eg6q+W9dgd
xMdH95tgZtmVMDqlvVR+DK0iO1BNpqPjrqWkk2tTLivpS+sGzCE/jCl18Q28Rk71
/A3gLD7Rtbq5TKNvuFCHwYMjrTDHI6aBjIaAlDm4e2/j/OxVtHyZGTre
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANC3xtbPhQ2GMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAt3aMy7Hsp4ySG3mlfi+pdTcZw6H6XNU1Y36fNdi4c+MzinQQbnqMPyt7
QLgU+XCWmcWsVo7GQF6n9N01Rh+UXXUZU4jcXlFocQPCWf9O+IIIIPXkd67kFMUV
```

```
HAxCELjfxHbC+I8e7dwOJhmdF4Bfi52Ty8zz0HdE8JDypPkTDlXuGvTgDyW7NP56
I/vlQaXLoYSbcQe5pv2a9gyBaaCM1QoeqwAHAeCNXb9Nuj9ZX3GHGJb3TuqAeKCD
5i9TscCB9XjY6Fx+zfSAobjBZwgLEtLOwJhbZnKmx4gJMaaNFipAjVT2FSS3+yev
eTYBoa1dvhk0ivQyQIPpHmihrmkWuwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBC
fdgyI8GjmCqiHAlh+L1bj0LdNql9zl7RXmOEzsuRdtdMumkxYXX88UtROy3fdi1i
VaEwHdAK8ThzRkesgHza/cXzqCMewaYxujSI6p6G7x99FFeGif1x0FJdj8AoeTL7
4h9bmS/6l4/NL7DJI9G7ovES/hoUA9v9TDhv+vauxXlgfrp0MPecprxBYlrc+DH2
adGCdKCp2lQ2YDKOD9TCEjYIli8XSoyevoWHUjfDYrCrCp8l4s/p7HOgYr8fJBAs
EuVy8211LVz1/X4EMBRNtNjXK9sklsxAOX14NDfBFSS0toxl3K6Tf9t/PviBl95d
hncyDAcFgDCK4w8LLlVW
-----END CERTIFICATE-----
```

Asia Pasifik (Melbourne) — ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSh40SMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+qWTGAbGsPeMX4hBMjAJUKys2NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt
+wV6MRtfOjh0Dvj/veJe88aEZJMozNgkJFRS
+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAF7vpPghH0FRo5gu49EArRNPrIvW1egM
wcgkqIwwuXYj+1rhlL+/
iMpQWjdVGEqIZSeXn5fLmdx50eegFCwND837r9e8XYTiQS143Sxt9+Yi6BZ7U7YD8kK9NBWoJxFqUeHdpRCs0O7COjT3
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Asia Pasifik (Mumbai) - ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
```

```
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
```

```
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Asia Pasifik (Selandia Baru) - ap-tenggara - 6

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCcP+D4eLFOajAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMxMjEzMDZaGA8y
MDUwMTIwNDEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBANBMmM/LbAX13IeB
3yr2pMMpiTW1b1go/axNLfcxEmj0fThKk8y0FAT1frN/UPdI9qRInsyBdEZQLiIH
4WHCXk8IidQLh4DED3G9DvSFFC4Gb8ax+UIQY11wfHPWO4+wA9q8liYTg/FxdJMM
tZS9tZAZxjH6+8yfV8Bt0wUd2Y+lAhUAwg0CxCmZPinHtKbFnpMQfKnzjCMCgYAf
i+D7nGVFOWJ8EYOpRYbG0pHkrpwNy+h01csn6IAwQbIfeOG+SF4N3LeuOAC9vXGY
VGh9XNxuasvqkRAzgRmJ/EYM5Xa/YN62EhddRuN8wCOg66MeczUDh3RTb+Tu6HK0
UR6oTSOQ6rxA5aA1qTc7TqI0+pRZv+QYIZK/ozsZzgOBhAACgYAbVm+rOX8J38cG
LxKjUXVM0KB69SksGLEqjO4ps80EcZ/0W3g1hGLnSX/RjYfAS60hbKK1GX9PpcaO
4mDzCTm3dZ6shbae5t8bBU+mUi8BmaK+Pdu3z5J77y4zv22/yXte8ulZ5J0zKP9K
QP3p3pa7XI9NaXpKGT3yZsJ0BWY2xTAJBgcqhkjOOAQDAzAAMC0CFBs4KQmrxHjQ
OHh0r8JqB8UiwlutAhUAwgxid7wT6FNm8Zwq9hioQ2v2K0A=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMwLuv2/tk9eMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMx
MjEzMDZaGA8yMjA0MDUwOTEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
```

```
gQC9AsBNOUfT8QpguHqMa9KIXP/YgZOmfRAgEmnLawXTC+40bXUq/fwkx+cebv3x
CvUx6d07/iDlD0dm2Hf2HhPFi3OaCI7vc8c3lqVBvcn6yzmwv35aSEvtVm2NHC3j
4/q6vN2tR2d4a1Mf1QhmOVOJ7XiTEbCy2Yv+pmDbk29V6QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAHatyQIy612kio8neI4r5VBg8pgKwW+mFGpAzOQ2NOyLCNoOeD1D
lPRaSipBN7WW6jpIozbz7JG7Kqc3N+piPGGzfjH9gZjqUqfOGrNHB5nsxvMHI2iL
e+DwsOcV7qnEVRgYbmLYOVKJv25wCsM/Tcn/6f6scEX2x+H0hAh7rwiP
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAI/xUfWwSQOtMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMx
MjEzMDZaGA8yMjA0MDUwOTEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArbid9Tnunu0pWCQUqZCkGeiF8hWixi+LBS1AOew2UsT9keAt2rXXGlU/
wSMriKHsvcrfKtuVKj5chArsOyFvagszH5lIKhI+GfWVQEd2aZiOvAJ+iRUQq1+R
gOr2gyjWlf3znZXTcyhHcJoXDhbn5e+kEa3pwS4yKNRpM3P61V4M2702xis08hjP
qMDxwXMa1Fiy4b7nAyNQifgrwb3bCA5k5prmkl/iajaWa1zMMFgLI9vA6UwUSbTK
H9iOuL/xNfMX+Xzq4CCaQYiJ8zdi56kqnB/lrA05NSjOPLskg6sUGkyiDxGK4gzC
DFrO6oygcdlBaxnyAECGdJcOM6TOmwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBg
8yVPNpctrvSvTazf/Ij8qC6+q6df1SptdYKQkOYWeUVZR7+3uTZ9Yiyq+Bh8Hbyf
NcR0eR6UqhgiB3p5slYNhTvLkpuMuqTpVJFvQtzZycnmKXAQ35G5zCYV0+pkF59L
ch26SukWk0+VP3kIM9VmaIZQKJEBlBLcnbDZyXlHUDnZAYPcxxKQ8uFPkW0GOFMr
ekFCGOUmFSItFXOHy5hD2xmctKNk3l12m6cKydYvONtk/3DovKNnw3c5k40WHQW/
Zdh/LWd4/Jrkan+kQnqm4rkrXF+x3aF0qrKTtHMICvpkZ8g7/588hBs4mZnCmFLa
q/g9WqIcd9SMmBkT6KZ8
-----END CERTIFICATE-----
```

Asia Pasifik (Osaka) — ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
```

```
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----
```

Asia Pasifik (Seoul) — ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
```

```
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Asia Pasifik (Singapura) — ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2Rerilrq5VvppHtbATVNY2qecXDA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Asia Pasifik (Sydney) — ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
```

```
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
-----END CERTIFICATE-----
```

Asia Pasifik (Taipei) — ap-timur-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQDrb+HArMxssTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQxNDU2MDZaGA8y
MDUwMDUyNTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAPFb5R5TBUs2N0YW
aJcOjxr4UCDrpVT3x6EeqoGFNAc1yiZw9iv++ff6wsXm0VG5XV1QkWMQcjPfK/2I
TvXh9XEOhsG7vaBHoWkb2gmIxE6C2u8TfoZu0ZmiMceFK7aYz5w/q2J9CmRs38dT
I9qgTq0LYX+VkiNYOQnn7sQXQ8CjAhUAp2Lue9SfYTmubbpH+3j91Sivc+cCgYAi
DiyGU5R5VgiNV3mhuAyiHCft3LEmTIxos/hx/rHzgm+vCMH55tYejIrv9n7YGrIZ
MejOt8bGYxqSf0Ir/aoj3ZfHihxUzwyfyzwH7D8kAodXJNsPUTKi0O0pGl/e+nVD
JhTIFV3AwC8Tt0r2hljbjhOiyhdYy5hxWHa/WokLAQOBhAACgYAkGGHXbFr/JXol
itpS1qfiETWSRkXGHrdSmUkRumgti2y7c57TgXPwCyNlP1sTr1duy/kYDpwSwyqi
qEYfko0b/xWpDEQQPsWBgolpEYP7RIT85IxrTCrC9ohz85n7v6m9oF6BiBQGtZdk
GBN7iqemg85UaF6mXfHvl3tUYjsB2jAJBgcqhkjOOAQDAy8AMCwCFED9Ybn6fEVF
wLNjDvULmki5bPBWAhR64pxsHFRHz0ZQi+SYMWdIpEs5RQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIICNjCCAZ+gAwIBAgIJAJp99iy2CTXhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQx
NDU2MDZaGA8yMjAzMTAyOTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDVdclgpcIIsyGG51ag8srK1UMfZ+Ioh9E4PLP+cIWQcdh31fv2kV/whKaqfmif
NefBIuHrTPl6L+mJQbsfeA+TiEx1Jamg4lwQfhgQKQCmjZVMaHtK+AY57TVN6FBf
HXxT2MXzktsKxAQRGeSTFQYrHRzSYvu+GkA+37lqyWRfcwIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBABM+WL9MSb7z3bNOTMkM7ufPucvj+LQ+zEAJiuG0rcB8GI2DhGB5
8ohDPUGlq1cP7vYmDkWG/FrLqx7qgIzkbE3zfb62JpdOuX73oHgCmikMfq8ifoS1
CUxMQ36PDZBFNPzGZxv5kEORqhmGBkYCoIUCQ43jh3aALR/A/rfzfij8
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJt5hgMuWbpMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQx
NDU2MDZaGA8yMjAzMTAyOTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA91FXs9Wk9kMI3lkNhjC69C6RTBpSvdLWSohPDlJKXFoaGYIDtyW1ViwO
FORAKz0koarVBx1D4fNKCxf+mhYAf//4Pxt31GzjehHNs2YVGimwhq/SNr+3AuIO
PibA+qScXamaiknE1Pxb4jisbBu2PMAG9OxU2dESNwiqBMvdJvg30YNTUITZ6r0e
MPjR1Y/EFVx/SLHW6wdvwqhNi9hz8HHdThzjCbCQPvmoLBJIKXIfosKqvauSezt1
KJSoS2jMx1OjJB2bBlQTZC8vF0WFNPoiH4jXyJ6+wMUMNSSd5b3uL5stVTMzuIz4
39Hd5YW41rmAy+6jmpGp2eXn6Td0rQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAs
gcgv+Xr67Cj08jKdAUT4GuCoGxveOFAjSDjs5y0cD+kXIT/Yj/+HKFOx5cwThT8F
TxNQ/oVuo3bGeuFEX799H0rT9Jupy0WiE1Vx81mk2M/1EDtns437edM4ofiWR8tR
Q1VNiRgz6Crr0nFgNoQa9HmR6/M+bImxevHJkWB3skvnxtA+lpKGwJs8jo6fA7AW
jr00opK0r731iBd1z/5hjIjkHn5NizAdiJEh3lVY/A3WS82aygW8LvYnKZeaBfZJ
J4NgxeflxocLFKBJD+hyf5u1hhvl7Mn/aGr5VI8/0F2oUqYo+xsHLT3keNghywO4
NNcyLcD9u16HVXhRhGvo
-----END CERTIFICATE-----
```

Asia Pasifik (Thailand) - ap-tenggara - 7

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC8TCCAq8CCQCOEEMWiJIJpTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIxNTI4NTZaGA8y
MDUwMDQxMzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASsGByqGSM44BAEwggEeAoGBAJWKfrIlz9+/U4wm
NDJPX00avUTdksBKX5RwHkY4o0///2G2HWwiBbxw8F1U+RzCXr80gSoe4+/SCSg3
uDuhJyzN5r4jr7c590CAgsiGdWERs7l4gLQCP504feU4TEjJoq9A8MfRZeqMj7Ug
fT5InTUW7S1/r98ddG/rBHMsJwEbAhUAneIckZ1YeyGcCeL32lujMhj+g68CgYA+
RsyTXCy3Tug5aHun51IfcG2d+pn5K/tv/N3WUR18RplVctrLhwIOUoAsDWPWtxNV
sODetezAyo759CK43JAmYGzXKbRFUHm3n46jP88tSdhuSeJhc/D4l5/0+2L7ndXp
L3+W4N05NdiKSGI8e8t452wTZv/RODivPZ3RtuCDywOBhQACgYEAjVS1Huwzdn1J
+kpd2Rcbe1BAGkmvk5sUu0KhyttqIB1kxTxeWZgsdO8REZSC5gJOwkcGFvXnb3DY
+Ms45r0e0s0rx2FFYjqMLwyRpK9wUjJfSXeJMa9iLQEXuyzBz6zPgfemXbS3zNq/
eoJ9ztIwjB9DMoKL+E1vSLsTGhehqRowCQYHKoZIzjgEAwMxADAuAhUAmljDM3c9
hf0j4XbMjjpnzrx1xhkCFQCASR9pgFNgLK8y6Kojj+P1KJkrSQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAIuIHAhL0xWcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIx
NTI4NTZaGA8yMjAzMDkxNzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCajgAeOauwvqGDLrHvxujnZ1BnkMzwjrycMUTkj8jqNtWoDQWUJVNPZJILosEU
VwK2I3oNkEsx/ryl9XfXcNNceoYfVEPzkTzozrZyuOG66FWtUU1LKeJ7h9/rX0Zd
9lZEokrdr6dLPt9FsHWaK5ExlUnWBjNltcQLkkKqoeYaFwIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAE4G5G+FvKTsX3T7BEcId7f5LSCc2J9gZRDiWn2oTr40CrBMOzJT
KsWr9W89YXW3gaGWltzc0WCwYQbJZgAkuEAZItJjbhdnns87ZbsFO+NZhc6gDtjA
WC3dPlSB9b6rfVoVW9O6Xwa7iNXZo8ddYVJ/ZOIv/totUz9qJt4DmmKk
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANaQIrYcijxaMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIx
NTI4NTZaGA8yMjAzMDkxNzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
```

```
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAxtMGK4r6WerVtMfpRRCY3DMP9Q/s4jnRIqolPaxeT99BAFp03HXyOrTz
WjggEHArRGGeDowFkL7Vj+QNY7ran2lnYVlAQ7Ow6OLl6WttT6lMsgsLUIcsED6G
eJ1Ko+ovT1qvmuush1U5R2pHkcCJ1IT2s6uQff85l066K7dCFpaoA1QHUk9zACHj
i0DtWuTAWBXirAZSGlmtP6uj1Aw6y5kACDTjIvZJeW/kmswfApTKaJ56eNkJsUBU
NpKwt3um1BMZduy0cjUv0Sc3dIbLNyfOdyPn8tX5u5ck0EPdtBB5WjEh71IXdZJD
oaBREV7AHg5ERPQsm0BqSvMQt09KiwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
qJyZbv/GUQnm8dEyVYgilQr3Yu35n8sfTwwZ1OJzIVce7NBPWePMfYii/tvGoKNp
KwFa/Vugbn1EwqpTEKqkPE1dOZvnUa97XxhYkoW5U7sgdKCANi1KWjywn7MiJ3Eg
j4gdqYK8wxvHi21ppqr572UO77ZuA8YMBoBT/CyQzWYUSmbqwKnnzaQBAZeO2iAk
VHuNU+9UsntNB676gRl9ag3Wfxq3yx5Ee1CeQf+US3HJn/pKk1H8dExXmBHvHwO6
GKUVNPN1rxfjTiaSt8wuO80uElAnyHIM3VOR8rJO7PKsobyEeJV0WI1hURO+wxpL
h3IsW7iBrFVvhX5xx7ZU
-----END CERTIFICATE-----
```

Asia Pasifik (Tokyo) — ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
```

```
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
```

```
-----END CERTIFICATE-----
```

Kanada (Pusat) — ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
```

```
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Kanada Barat (Calgary) — ca-barat-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
```

```
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAYPou9weMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ieYvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW
+w9lMQjFHkJ7Jy/
PHCJ69EzebQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGe9Snkz1A6rHBH6/5kDtYvtPYwhx2sXNxztbhkXErFk40Nw5l4
gvDVtWG7qyb6fAqgoisyAbk8K9LzxSim2S1nmT9vD84B/t/VvwQBylc
+ej8kRxMH7fquZLp7IXfmtBzyUqu6Dpbne+chG2
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

Tiongkok (Beijing) – cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
```

```
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

Tiongkok (Ningxia) – cn-northwest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
```

```
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
```

```
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

Eropa (Frankfurt) — eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
```

```
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Eropa (Irlandia) — eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Eropa (London) — eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
```

```
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Eropa (Milan) — eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Eropa (Paris) — eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
```

```
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
-----END CERTIFICATE-----
```

Eropa (Spanyol) — eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdH
+3m/
rxIUZ2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
```

```
iMMzcFucmLMl5BxEblrFXOz7IIuOeiGkndmrqUeDCykztLku45s7hxdNy4ltTuVAaE5aNBdw5J8U1mRvsKvHLy2ThH6h
+hBgiphYp84DUbWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Eropa (Stockholm) — eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
```

```
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
-----END CERTIFICATE-----
```

Eropa (Zürich) — eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
opKZAUusJx2hpgU3pUHhlp9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAILlpoE3k9o7KdALAxsFJNit
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBElvPCDKFvTJl4QQhToy056llO5GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczRO0YSm3OjkqbydU7DFlmkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6Owyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israel (Tel Aviv) — il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
```

```
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+S8vOy5hpLoRe4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM
+t1K4S0xsqjXxxS716uGYh7eWtkxrCihj8AbXN/6pa095h
+7TZyl2n83keiNUzM2KoqQVMwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADwA6VVEIIZD2YL00F12po40xDLzIc9XvqFPS
FmU7H8s62/jD6cOR1A1cClIyZUe1yT1ZbPySCs43J+Thr8i8FSRxzDBSZZi5foW
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

Meksiko (Tengah) — mx-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq8CCQD4QwfTExrgxTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDExMTQwOTQ4MjRaGA8y
MDUwMTExNTA5NDgyNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASwGByqGSM44BAEwggEfAoGBAK+pJEOtD2RFlCbf
oAzONffZa42FB8G6OA/30DT81xWvB2Hnmgw7LfiELYqgfuck3YSDffNDcmiFTJuX
AU9u0NtbbxcOytcdUq4HInpHiB85I6WWWKYB66aGbvYowUPpqBZkASb1i/pYAh5W
nNYvx408008tTzqpMfZDchJHzWqBAhUA0ogoJzTw2/4pKhz9aqTsRCzRVPsCgYEA
qklRUcuU0du/bT/M6kWxYvrTGhO9KXQe+7RtbaIq4dWRsCBnO4smDY/GmI9H8ew1
LRJ9AcLGmxDm795CvVZkHNcht7PDAREagWmz2YvhLA+ev6U0RpfdlBXCck2p1CxQ
LMtoFO7DThksHIQBtnlQdHDvguKEZQz/Iobhne6Kb3wDgYQAAoGAQSTlOqFq6RtR
Jvp406XhGl+eO9SQUpevpzG3Dzbdy6EQ8PBJDOHHJvxbebvpnQssh0CnQfTkSw26
jwPy9V5zRC0ZezwnRTyGSJwiErUKDGeVekEAoNJL1USy8jKkgBajlskZrR+0JHDN
Jv3UwYIPplc4ZS2f2E7btrtlaWt/P70wCQYHKoZIzjgEAwMvADAsAhRXljPWKWYf
61DkDVdgPPHsS2/LuwIUejcGV9WuS3uPvJ6lmn4opxUGBZw=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICPzCCAaigAwIBAgIUCmzpTTMBQYItpMC2VDYsZfIAS7IwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcMB1NlYXR0bGUxIDAeBgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQwMjEyNTAzNloXDTI5MDQwMTEyNTAzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAe
BgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDfvOnCzm1iN58Nm7k6ehoy6v0lnnFI617D6CY3bfuq01RCdEQL
96+pYawJieTH8JAQKj02CAa3AeaqdXTE/pDhI/YKLreeMb4K68WMn24Wjjs6oxjB
bAmsKXtt9ihKHGBFNUhgFrNFYyA2i7ieJviwpHjQ/XgXiG2u1/t/4VydUwIDAQAB
MA0GCSqGSIb3DQEBCwUAA4GBAL5+vvj4lhaE+J5tuCqV3XJzDd97lsD4le2O2uGw
P0sGdUcRAdxzU3Bwq/hhtzNWnfwo0aCEQKmLM7xyd3nUa0VvKXLq+DDuayipWINr
OATnNxFRe99d38qHTR1dgkjZdKbbtnl6O4fgM57tVEuQJd/N4ILl9jaRcJ5Ip+9t
3y5t
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALxuE00HoJomMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMzEx
MTE0MzNaGA8yMjA0MDQwNjExMTQzM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13xWucALo8M/TXbZJgHrqFqFON91dSLPE/eLbmeIJbP1pb9ICd33qKAx
HlKSrXI9b9YS3U1Pl0bF3ZgfeE/x4Y0KDDZwzpf07H8IgRittULJoNLYVKCJXWPq
Ky1qvDJX3653dUbUu9eAdVCTRgk7eKpPBLAmW27+pgAGzEYrVV3u2AvqNTonvfTU
sPgEVnAL1J490pNM85KtFynxFTWGigHkd3BHidxmLrTH4I4eRxNZ9q/3gsDW+zKt
jQlpM7JzZa2OqxsF5YQDh1fF52Emqsr+ufLeGqDLOgT1QWcqpz57AX8GqZpgZULo
itCRNXbQDzZY9FxIgpiFJv3y/qYYDQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCt
MTeH4EgqjJEjb1qm5tzXYurLprVrEVQ+PhGXJFJd3xAZyeaDVYy7kio08E2xhmHd
HtkBDty2KnOHsTQmeAJCci7d4tYXZ/1qe341wwm9OoFcO8jhIndx6FXJCgQUY4dL
AAr9HQJFWG5dMZgbi1Zuhxdio3sSoOBjL2p7QIsGNkITvCDIs/H0/szpJnyyyIqu
wmUhSel5hdy5MwOsyUKVGnAdaS5Vd9oL4kLszS9nBZ7ny6BC9odIkFAdGqQ5vM4z
vcbfOq14hjatQmJgJhksN/0Dpl78Gheq0pIhP8LTkAOEG2832nQLzCa3oxSk8otG
GJXkzzyQjse+13r8+yNJ
-----END CERTIFICATE-----
```

Timur Tengah (Bahrain) — me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
```

```
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
```

```
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Timur Tengah (UEA) — me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8moOhqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
```

```
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

Amerika Selatan (Sao Paulo) — sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
```

```
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
```

```
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

AWS GovCloud (AS-Timur) — -1 us-gov-east

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
```

```
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

AWS GovCloud (AS-Barat) — -1 us-gov-west

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
```

```
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
```

```
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

AWS Awan Berdaulat Eropa — -1 eusc-de-east

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq8CCQDyckpYH0omIDAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMTgwOTM5MzdaGA8y
MDUwMTAxOTA5MzkzN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASsGByqGSM44BAEwggEeAoGBAJR1zx7FzSGhXd3m
U1PfwH33QEK4CHnFSnp/DUse0SdLwsvLkHw7Tq3M7IX4E+TZ6OzYZZeoVZttqbyq
OZ8ROUS7CzDWcQ0503de/ya51cTs4BiO4nv2awm1WEoV9XtQyA2JLn0Jv7g2uja0
317krS+Dk3kjs9RpWvkmiyTMu1YhAhUA69U+A26BWLVpNIZZ0uWMZJSNlIkCgYBw
w1cgrHFGEqJNhqN7Sjs2YwTP+jpp1GvhxKyce5aOh5ErVvufb5gVVoKahrrHEBms
TrBXxnfcPaTupwdmEZ9eM8a+9RS2vye//KU1kGIOMgafPEzBEXs9m7okmAQpYXnG
cVOTtx2gd/E/VfKRiMSAmam178qwvcbcijNqRdLjRQOBhQACgYEAiEFVGYVCntmy
va8c2oU5/owdMws+NZ6u9blat0ymPr/8Q+DR77CgUPJW+K0k41GdgWpVlrsjiiPw
iygzw4DW7Vsl018KcIFUTiSwpzv2in+tKNUkO5Ly0q6arbSxrXZffYe7aOZKtCCH
XWDMKOH2iCvZptMpG7fDDSc7Be8v4AgwCQYHKoZIzjgEAwMwADAtAhQyvCF3q437
RvdPXMFcMc6qrD0svAIVAMvsN3NwOY4KRYlFv9Dnok8D/ixI
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAPybReXZqUSNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMTgw
OTM5MzdaGA8yMjA0MDMyNDA5MzkzN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDShbskmohorgcjN7gfApw89CEsg7praCDggaUVXF6gy9JdJ5INcv7+DkwKaAxd
NQWDsWZnxIOqPuPfyAYVP3D2/exP3Rfxj31UomLduu7S83zgiJ8VVL/GzlDELv5/
K2rTcd+580NjLSa6FYDcXDip2ir6TXxRYBYHP65dwniE+wIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAKu9t3CAtZt7c+k4bCZlmxrwgps1668p24x7QRmLxgXnwj5A2MOM
qEtxA9Q3q3WxUc0nWKaCTvRrTfWW917xsLcvVL8rI6xCjg2bb5FJ73xzcfSxHr9I
Q1mThJgLaWVIblllGJK7+EogR7gfqlPhc0Ql5bYuaozdt+r69xNuJlyR
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAODRxRi5VXBbMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNTAyMjEx
MjQ0MTRaGA8yMjA0MDcyODEyNDQxNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAr24OkDrpRU1ffx1PAcHZbKu7fZkhfT/e/PDhSkp2FvOzJEqDUT23E2wp
K/44mhJ3d8blYtgBiRXjqRsAFu8ZbzXLc0gaQ9A5woxfx5b7iOMwneCajS9xS5qr
cE0MMEY9XwG8MCp9YBoDJqDJh74oQqcPROBq16L4k2Ys22n1khus4JpwT7VSRE1I
nnt7fGIYsUmNGM+T2E6ubG3FvkY0HbLvNCcGRMCnDYqloo2BthuSG58KbMAku7VD
hMxzzJte5yMuRpHBojQr9N0hZcSJCtSFo6FhlxCzxGzwoSKzqm99ULYL4lf+IORe
DaKoATZJvbnX0LYAKLtPr1Pz9SD9pQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUHpdxehvJwYL2o25SXyxsSndDW48wgY4GA1UdIwSBhjCBg4AUHpdx
ehvJwYL2o25SXyxsSndDW4+hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAODRxRi5VXBbMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFGcArNlGB3oRBaXohpnhrnVblhJJa6U7r1/
M5TAJCKCkziSz3lOZmZZ1YgSnQC1blhUD2rhuS8a0Mw1Ml48nLjIYMMK0tkJRKCD
LPxxEZp4EzogYj6PqfSubzm59MmBenIcJPaJ9y2uY1U4Q3PMfU6M1JqqQ0Lzplq0
n9eWpJK3+7UbtuyAzigO4DRWEBMxJBUU7f2LfY+qFjskoeHopX20cmn1vc1TGyAF
Qf8xdt1SaPKC26zJsrCkiMZJNm4aa8KqvhqBHVjV4NrGeVGCcdlmSDiL71Egk9kh
744eGQxNnhZNvePW2kVcSuh0HpAo4Q4vfpjN+jz2Ves3kjFsrgc=
-----END CERTIFICATE-----
```

Kepatuhan STIG untuk instans Anda EC2

Security Technical Implementation Guides (STIGs) adalah standar pengerasan konfigurasi yang dibuat oleh Badan Sistem Informasi Pertahanan (DISA) untuk mengamankan sistem informasi dan perangkat lunak. Untuk membuat sistem Anda sesuai dengan standar STIG, Anda harus menginstal, mengonfigurasi, dan menguji berbagai pengaturan keamanan.

STIGs diterapkan berdasarkan klasifikasi kerentanan berikut. Saat Anda membuat gambar yang diperkeras STIG atau menerapkan pengaturan STIG ke instance yang ada, Anda dapat memilih level mana yang akan diterapkan untuk pengerasan. Level yang lebih tinggi termasuk pengaturan STIG dari semua level yang lebih rendah. Misalnya, level Tinggi (Kategori I) mencakup pengaturan dari kategori Sedang dan Rendah.

Tingkat kepatuhan

- Tinggi (Kategori I)

  Risiko paling parah. Termasuk kerentanan apa pun yang dapat mengakibatkan hilangnya kerahasiaan, ketersediaan, atau integritas.
- Sedang (Kategori II)

  Termasuk kerentanan apa pun yang dapat mengakibatkan hilangnya kerahasiaan, ketersediaan, atau integritas tetapi risikonya dapat dikurangi.
- Rendah (Kategori III)

  Termasuk kerentanan apa pun yang menurunkan tindakan untuk melindungi dari hilangnya kerahasiaan, ketersediaan, atau integritas.

Amazon EC2 menyediakan metode berikut untuk membuat instans STIG yang dikeraskan:

- Anda dapat meluncurkan instance Windows yang telah dikonfigurasi sebelumnya untuk pengerasan STIG dari Windows publik khusus. AWS AMIs Untuk informasi selengkapnya, lihat STIG Hardened AWS Windows Server AMIs di referensi AWS AMI Windows.
- Anda dapat membuat AMI yang disesuaikan untuk meluncurkan instans pra-konfigurasi yang dibuat dengan komponen pengerasan STIG EC2 Image Builder. Untuk informasi selengkapnya, lihat komponen pengerasan STIG di Panduan Pengguna Image Builder.
- Anda dapat menggunakan dokumen perintah AWSEC2-ConfigureSTIG Systems Manager untuk menerapkan pengaturan STIG ke EC2 instance yang ada. Dokumen perintah STIG Systems

Manager memindai kesalahan konfigurasi dan menjalankan skrip remediasi untuk menginstal dan memperbarui sertifikat DoD dan menghapus sertifikat yang tidak perlu untuk mempertahankan kepatuhan STIG. Tidak ada biaya tambahan untuk menggunakan dokumen STIG Systems Manager.

Topik

- Pengaturan pengerasan STIG untuk instance EC2
- Unduhan skrip pengerasan STIG
- Gunakan AWS Systems Manager untuk menerapkan pengaturan STIG ke instans Anda

Pengaturan pengerasan STIG untuk instance EC2

Pengaturan STIG bervariasi berdasarkan sistem operasi instans Anda dan tingkat kepatuhan yang Anda pilih. Konten berikut berisi detail spesifik sistem untuk STIGs yang diterapkan pada setiap tingkat kepatuhan.

Daftar Isi

- Pengaturan STIG untuk instance EC2 Linux
- Pengaturan pengerasan STIG untuk instance Windows EC2

Pengaturan STIG untuk instance EC2 Linux

Bagian ini berisi informasi tentang pengaturan pengerasan STIG Linux yang didukung Amazon EC2 . Skrip pengerasan menerapkan pengaturan STIG yang didukung ke infrastruktur berdasarkan distribusi Linux. Jika distribusi Linux tidak memiliki pengaturan pengerasan STIG sendiri, Amazon EC2 menggunakan pengaturan RHEL, sebagai berikut.

- Red Hat Enterprise Linux (RHEL) 7 pengaturan STIG
  - RHEL 7
  - CentOS 7
  - Amazon Linux 2 (AL2)
- Pengaturan RHEL 8 STIG
  - RHEL 8
  - CentOS 8

- Pengaturan RHEL 9 STIG
  - RHEL 9
  - CentOS Aliran 9

Linux STIG Rendah (Kategori III)

Daftar berikut berisi pengaturan STIG yang EC2 didukung Amazon untuk infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewatkan setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap, lihat Perpustakaan STIGs Dokumen. Untuk informasi tentang cara melihat daftar lengkap, lihat Alat Melihat STIG.

RHEL 7 STIG Versi 3 Rilis 15

- RHEL 7/CentOS 7/ AL2

  V-204452, V-204576, dan V-204605

RHEL 8 STIG Versi 2 Rilis 4

- RHEL 8/CentOS 8

  V-230241, V-230269, V-230270, V-230281, V-230285, V-230346, V-230381, V-230395, V-230468, V-230469, V-230485, V-230486, V-230491, V-230494, V-230495, V-230494 6, V-230497, V-230498, V-230499, dan V-244527

RHEL 9 STIG Versi 2 Rilis 5

- RHEL 9/CentOS Aliran 9

  V-257782, V-257795, V-257796, V-257824, V-257880, V-257946, V-257947, V-258037, V-258067, V-258069, V-258076, V-258138, dan V-258173

Amazon Linux 2023 STIG Versi 1 Rilis 1

V-274141

SLES 12 STIG Versi 3 Rilis 3

V-217108, V-217113, V-217140, V-217198, V-217209, V-217211, V-217212, V-217213, V-217214, V-217215, V-217216, V-217236, V-217237, V-217238, V-217239, V-217282, dan V-255915

SLES 15 STIG Versi 2 Rilis 5

V-234811, V-234850, V-234868, V-234868, V-234873, V-234873, V-234905, V-234907, V-234908, V-234909, V-234933, V-234934, V-234935, V-234936, V-234955, V-234963, V-234967, dan V-255921

Ubuntu 18.04 STIG Versi 2 Rilis 15

V-219163, V-219164, V-219165, V-219172, V-219173, V-219174, V-219175, V-219178, V-219179, V-219180, V-219210, V-219301, V-219327, V-219332, dan V-219333

Ubuntu 20.04 STIG Versi 2 Rilis 3

V-238202, V-238203, V-238221, V-238222, V-238223, V-238224, V-238226, V-238234, V-238235, V-238237, V-238308, V-238323, V-238357, V-238362, dan V-238373

Ubuntu 22.04 STIG Versi 2 Rilis 5

V-260479, V-260480, V-260481, V-260521, V-260520, V-260476, V-260472, V-260549, V-260550, V-260551, V-260552, V-260581, dan V-260596

Ubuntu 24.04 STIG Versi 1 Rilis 2

V-270645, V-270646, V-270664, V-270820, V-270677, V-270690, V-270706, V-270710, V-270695, V-270749, V-270752, dan V-270818

Linux STIG Medium (Kategori II)

Daftar berikut berisi pengaturan STIG yang EC2 didukung Amazon untuk infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewatkan setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap, lihat Perpustakaan STIGs Dokumen. Untuk informasi tentang cara melihat daftar lengkap, lihat Alat Melihat STIG.

> **Note**
>
> Kategori Linux STIG Medium mencakup semua pengaturan pengerasan STIG terdaftar yang berlaku untuk Linux STIG Low (Kategori III), selain pengaturan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II.

RHEL 7 STIG Versi 3 Rilis 15

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

- RHEL 7/CentOS 7/ AL2

  V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204416, V-204417, V-204420, V-204422, V-204423, V-204426, V-204427, V-204431, V-204434, V-204435, V-204437, V-204449, V-204450, V-204451, V-204457, V-204466, V-204490, V-204491, V-204503, V-204507, V-204508, V-204510, V-204511, V-204511, V-204511, V-204511 4512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204542, V-204543, V-204544, V-204545, V-204546, V-204546, V-204546, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204566, V-204567, V-204568, V-204572, V-204579, V-204584, V-204585, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204601, V-204602, V-204609, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204619, V-204622, V-204625, V-204630, V-204631, V-204633, V-233307, V-237634, V-237635, V-251703, V-255925, V-255927, dan V-256970

RHEL 8 STIG Versi 2 Rilis 4

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

- RHEL 8/CentOS 8

  V-230222, V-230228, V-230231, V-230233, V-230236, V-230237, V-230238, V-230239, V-230240, V-230244, V-230245, V-230246, V-230247, V-230248, V-230249, V-230250, V-230255, V-230256, V-230257, V-230258, V-230259, V-230260, V-230261, V-230262, V-230266, V-230267, V-230268,

V-230271, V-230273, V-230275, V-230276, V-230277, V-230278, V-230279, V-230280, V-230282, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230298, V-230310, V-230311, V-230312, V-230313, V-230314, V-230315, V-230316, V-230318, V-230319, V-230320, V-230321, V-230322, V-230324, V-230325, V-230326, V-230327, V-230330, V-230333, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230347, V-230348, V-230352, V-230353, V-230354, V-230354, V-230354 6, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230365, V-230366, V-230368, V-230369, V-230370, V-230372, V-230373, V-230375, V-230377 6, V-230377, V-230378, V-230380, V-230382, V-230383, V-230385, V-230386, V-230387, V-230389, V-230390, V-230392, V-230393, V-230394, V-230396, V-230397, V-230397, V-230397, V-230397, V-230397 30398, V-230399, V-230400, V-230401, V-230402, V-230403, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, V-230419, V-230421, V-230422, V-230423, V-230424, V-230425, V-230426, V-230427, V-230427, V-230427 V-230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444, V-230446, V-230447, V-230448, V-230448, V-230448, V-230448 30449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230470, V-230471, V-230472, V-230473, V-230474, V-230475, V-230478, V-230480, V-230481, V-230482, V-230483, V-230488, V-230489, V-230493, V-230502, V-230503, V-230505, V-230506, V-230507, V-230523, V-230524, V-230525, V-230526, V-230527, V-230532, V-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230541, V-230541 42, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-230550, V-230555, V-230556, V-230557, V-230559, V-230560, V-230561, V-237640, V-237642, V-237643, V-244519, V-244523, V-244524, V-244525, V-244526, V-244528, V-244531, V-244533, V-244535, V-244536, V-244538, V-244539, V-244542, V-244543, V-244544, V-244547, V-244550, V-452450 51, V-244552, V-244553, V-244554, V-250315, V-250316, V-250317, V-251707, V-251708, V-251709, V-251710, V-251711, V-251713, V-251714, V-251715, V-251716, V-251717, V-251718, V-256974, V-257258, dan V-274877

RHEL 9 STIG Versi 2 Rilis 5

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

- RHEL 9/CentOS Aliran 9

V-257780, V-257781, V-257783, V-257786, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257797, V-257798, V-257799, V-257801, V-257802, V-257803, V-257804, V-257804, V-257805, V-257806, V-257807, V-257808, V-257809, V-257810, V-257811, V-257812, V-257813,

V-257814, V-257815, V-257816, V-257817, V-257825, V-257827, V-257828, V-257829, V-257830, V-257831, V-257832, V-257833, V-257834, V-257836, V-257838, V-257839, V-257840, V-257841, V-257842, V-257849, V-257882, V-257883, V-257884, V-257885, V-257886, V-257886, V-257886 887, V-257888, V-257889, V-257890, V-257891, V-257892, V-257893, V-257894, V-257895, V-257896, V-257897, V-257898, V-257899, V-257900, V-257901, V-257902, V-257903, V-257904, V-257905, V-257906, V-257907, V-257907, V-257907, V-257907 7908, V-257909, V-257910, V-257911, V-257912, V-257913, V-257914, V-257915, V-257916, V-257917, V-257918, V-257919, V-257920, V-257921, V-257922, V-257923, V-257924, V-257925, V-257926, V-257927, V-257928, V-257929, V-257930, V-257933, V-257934, V-257935, V-257936, V-257939, V-257940, V-257942, V-257943, V-257944, V-257948, V-257951, V-257952, V-257953, V-257954, V-257954, V-257954, V-257954 57, V-257958, V-257959, V-257960, V-257961, V-257962, V-257963, V-257964, V-257965, V-257966, V-257967, V-257968, V-257969, V-257970, V-257971, V-257972, V-257973, V-257975, V-257976, V-257977, V-257978, V-257979, V-257980, V-257982, V-257983, V-257985, V-257987, V-257988, V-257992, V-257993, V-257994, V-257995, V-257996, V-257997, V-257999, V-258000, V-258001, V-258001, V-258001, V-258001, V-258001 8002, V-258003, V-258004, V-258005, V-258006, V-258007, V-258008, V-258009, V-258010, V-258011, V-258028, V-258034, V-258035, V-258038, V-258039, V-258040, V-258041, V-258043, V-258046, V-258046, V-258046, V-258046, V-258046, V-258049, V-258052, V-258054, V-258055, V-258056, V-258057, V-258060, V-258063, V-258064, V-258065, V-258066, V-258068, V-258070, V-258071, V-258072, V-258073, V-258074, V-258075, V-258077, V-258079, V-258080, V-258081, V-258082, V-258083, V-258084, V-258085, V-258088, V-258089, V-258090, V-258091, V-258092, V-258093, V-258095, V-258097, V-258098, V-258099, V-258100, V-258101, V-258102, V-258102, V-258102 103, V-258104, V-258105, V-258107, V-258108, V-258109, V-258110, V-258111, V-258112, V-258113, V-258114, V-258115, V-258116, V-258117, V-258118, V-258119, V-258120, V-258120, V-258120, V-258120, V-258120 8122, V-258123, V-258124, V-258125, V-258126, V-258128, V-258129, V-258130, V-258133, V-258137, V-258140, V-258141, V-258142, V-258144, V-258145, V-258146, V-258147, V-258148, V-258150, V-258152 1, V-258152, V-258153, V-258154, V-258156, V-258157, V-258158, V-258159, V-258160, V-258161, V-258162, V-258163, V-258164, V-258165, V-258166, V-258167, V-258167, V-258167 168, V-258169, V-258170, V-258171, V-258172, V-258175, V-258176, V-258177, V-258178, V-258179, V-258180, V-258181, V-258182, V-258183, V-258184, V-258185, V-258185, V-258185 6, V-258187, V-258188, V-258189, V-258190, V-258191, V-258192, V-258193, V-258194, V-258195, V-258196, V-258197, V-258198, V-258199, V-258200, V-258201, V-258202, V-258203, V-258204, V-258206, V-258207, V-258208, V-258209, V-258210, V-258211, V-258212, V-258213, V-258214, V-258215, V-258216, V-258217, V-258218, V-258219, V-258220, V-258220, V-258221, V-258222, V-258223, V-258225, V-258226, V-258227, V-258228,

V-258229, V-258232, V-258233, V-258234, V-258237, V-258239, V-258240, V-270174, V-270175, V-270176, V-270177, V-272488, dan V-274878

Amazon Linux 2023 STIG Versi 1 Rilis 1

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

V-273995, V-274000, V-274001, V-274002, V-274003, V-274004, V-274005, V-274006, V-274008, V-274009, V-274010, V-274011, V-274012, V-274013, V-274014, V-274017, V-274018, V-274019, V-274020, V-274020, V-274021, V-274022, V-274023, V-274024, V-274026, V-274027, V-274028, V-274030, V-274031, V-274032, V-274033, V-274034, V-274035, V-274036, V-274040, V-274041, V-274042, V-274044, V-274045, V-274047, V-274048, V-274049, V-274050, V-274051, V-274053, V-274054, V-274059, V-274061, V-274062, V-274065, V-274069, V-274070, V-274071, V-274072, V-274073, V-274074, V-274074, V-274074 75, V-274076, V-274077, V-274078, V-274079, V-274081, V-274082, V-274083, V-274084, V-274085, V-274086, V-274087, V-274088, V-274089, V-274090, V-274091, V-274092, V-274093, V-274094, V-274095, V-274096, V-274097, V-274098, V-274099, V-274100, V-274101, V-274102, V-274103, V-274104, V-274105, V-274106, V-274107, V-274108, V-274110, V-274111, V-274112, V-274112, V-274112, V-274112, V-274112 13, V-274114, V-274115, V-274116, V-274117, V-274119, V-274120, V-274121, V-274122, V-274123, V-274124, V-274125, V-274126, V-274127, V-274129, V-274130, V-274130, V-274130, V-274130, V-274130 4131, V-274132, V-274133, V-274134, V-274135, V-274136, V-274137, V-274138, V-274139, V-274140, V-274142, V-274143, V-274144, V-274145, V-274147, V-274149, V-274151, V-274152, V-274154, V-274155, V-274155, 274156, V-274157, V-274160, V-274161, V-274162, V-274164, V-274165, V-274166, V-274167, V-274168, V-274169, V-274170, V-274173, V-274174, V-274177, V-274181, V-274181, 274182, V-274185, dan V-274187

SLES 12 STIG Versi 3 Rilis 3

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

V-217102, V-217105, V-217110, V-217116, V-217117, V-217118, V-217119, V-217120, V-217121, V-217122, V-217124, V-217125, V-217126, V-217127, V-217128, V-217130, V-217134, V-217138, V-217143, V-217147, V-217152, V-217153, V-217154, V-217155, V-217156, V-217158, V-217161, V-217163, V-217166, V-217167, V-217168, V-217169, V-217169, V-217169 170, V-217171, V-217182, V-217183, V-217188, V-217190, V-217191, V-217194, V-217195, V-217196, V-217197, V-217200, V-217201, V-217202, V-217203, V-217204, V-217204, V-217204, V-217204, V-217204 5,

V-217206, V-217207, V-217208, V-217210, V-217217, V-217218, V-217223, V-217227, V-217230, V-217240, V-217241, V-217242, V-217243, V-217244, V-217245, V-217246, V-217247, V-217248, V-217249, V-217250, V-217251, V-217252, V-217253, V-217254, V-217254, V-217254, V-217254, V-217255, V-217257, V-217258, V-217260, V-217265, V-217266, V-217267, V-217269, V-217272, V-217273, V-217274, V-217275, V-217276, V-217277, V-217278, V-217279, V-217280, V-217283, V-217284, V-217286, V-217287, V-217288, V-217289, V-217290, V-217291, V-217292, V-217293, V-217294, V-217295, V-217296, V-217299, V-217300, V-217301, V-217302, V-233308, V-237606, V-237607, V-237608, V-237609, V-237610, V-237611, V-237612, V-237613, V-237614, V-237615, V-237616, V-237617, V-237618, V-237619, V-237620, V-237621, V-237622, V-237623, V-251720, V-251722, V-255914, dan V-256981

SLES 15 STIG Versi 2 Rilis 5

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

V-234802, V-234807, V-234808, V-234809, V-234813, V-234815, V-234817, V-234821, V-234822, V-234823, V-234825, V-234827, V-234828, V-234829, V-234830, V-234832, V-234833, V-234834, V-234835, V-234836, V-234837, V-234838, V-234839, V-234840, V-234841, V-234842, V-234843, V-234844, V-234845, V-234848, V-234854, V-234855, V-234856, V-234857, V-234858, V-234861, V-234861, V-234862, V-234863, V-234869, V-234870, V-234875, V-234880, V-234881, V-234882, V-234883, V-234884, V-234885, V-234886, V-234887, V-234888, V-234889, V-234891, V-234895, V-234896, V-234897, V-234897, V-234897, V-234897 99, V-234900, V-234901, V-234902, V-234903, V-234904, V-234906, V-234910, V-234911, V-234912, V-234913, V-234914, V-234918, V-234924, V-234928, V-234932, V-234937, V-234938, V-234939, V-234940, V-234941, V-234942, V-234943, V-234944, V-234945, V-234946, V-234947, V-234948, V-234949, V-234950, V-234951, V-234952, V-234954, V-234956, V-234957, V-234958, V-234959, V-234961, V-234961, V-234961, V-234961, V-234961, V-234961, V-234961, V-234961 62, V-234964, V-234966, V-234969, V-234973, V-234975, V-234976, V-234977, V-234978, V-234979, V-234981, V-234982, V-234983, V-234991, V-235002, V-235003, V-235007, V-235008, V-235009, V-235009, V-235009, V-235010, V-235013, V-235014, V-235015, V-235016, V-235017, V-235018, V-235020, V-235021, V-235022, V-235023, V-235024, V-235025, V-235026, V-235028, V-235029, V-235030, V-251724, V-255920, V-256983, dan V-274879

Ubuntu 18.04 STIG Versi 2 Rilis 15

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

V-219149, V-219155, V-219156, V-219160, V-219166, V-219168, V-219176, V-219181, V-219184, V-219186, V-219188, V-219189, V-219190, V-219191, V-219192, V-219193, V-219194, V-219195, V-219196, V-219197, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219219, V-219220, V-219221, V-219222, V-219223, V-219224, V-219225, V-219226, V-219227, V-219227, V-219227, V-219227, V-219227, V-219227, V-219227, V-219227 28, V-219229, V-219230, V-219231, V-219232, V-219233, V-219234, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219296, V-219297, V-219298, V-219299, V-219300, V-219303, V-219304, V-219306, V-219309, V-219310, V-219311, V-219315, V-219318, V-219319, V-219323, V-219326, V-219328, V-219330, V-219331, V-2319331, V-219331, V-219331, V-219331, V-219331 35, V-219336, V-219337, V-219338, V-219339, V-219342, V-219344, V-233779, V-233780, dan V-255906

Ubuntu 20.04 STIG Versi 2 Rilis 3

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

V-238200, V-238205, V-238207, V-238209, V-238210, V-238211, V-238212, V-238213, V-238220, V-238225, V-238227, V-238228, V-238229, V-238230, V-238231, V-238232, V-238236, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238298, V-238300, V-238301, V-238302, V-238303, V-238303, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238318, V-238318 238319, V-238320, V-238324, V-238325, V-238329, V-238333, V-238334, V-238337, V-238338, V-238339, V-238340, V-238341, V-238342, V-238343, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238353, V-238355, V-238356, V-238359, V-238369, V-238370, V-238371, V-238376, V-238377, V-238378, V-251505, V-255912, V-274852, dan V-274853

Ubuntu 22.04 STIG Versi 2 Rilis 5

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

V-260471, V-260473, V-260474, V-260475, V-260477, V-260478, V-260485, V-260486, V-260487, V-260488, V-260489, V-260490, V-260491, V-260492, V-260493, V-260493, V-260493, V-260493, V-260493, V-260493 4, V-260495, V-260496, V-260497, V-260498, V-260499, V-260500, V-260505, V-260506, V-260507, V-260508, V-260509, V-260510, V-260511, V-260512, V-260513, V-260513, V-260513, V-260513 514, V-260522, V-260527, V-260528, V-260530, V-260533, V-260534, V-260535, V-260537, V-260538, V-260540, V-260542, V-260543, V-260545, V-260546, V-260547, V-260547, V-260547, V-260547, V-260547, V-260553, V-260554, V-260555, V-260556, V-260557, V-260560, V-260561, V-260562, V-260563, V-260564, V-260565, V-260566, V-260567, V-260569, V-260572, V-260573, V-260574, V-260575, V-260576, V-260582, V-260584, V-260585, V-260586, V-260588, V-260589, V-260589, V-260589, V-260589, V-260589 90, V-260591, V-260594, V-260597, V-260598, V-260599, V-260600, V-260601, V-260602, V-260603, V-260604, V-260605, V-260606, V-260607, V-260608, V-260609, V-260609, V-260609, V-260609 610, V-260611, V-260612, V-260613, V-260614, V-260615, V-260616, V-260617, V-260618, V-260619, V-260620, V-260621, V-260622, V-260623, V-260624, V-260625, V-260625, V-260625, V-260625, V-260625, V-260626, V-260627, V-260628, V-260629, V-260630, V-260631, V-260632, V-260633, V-260634, V-260635, V-260636, V-260637, V-260638, V-260639, V-260640, V-260641, V-260642, V-260643, V-260644, V-260645, V-260646, V-260648, V-260649, V-274862, V-274864, dan V-274866

Ubuntu 24.04 STIG Versi 1 Rilis 2

Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

V-270649, V-270651, V-270652, V-270653, V-270654, V-270656, V-270657, V-270659, V-270660, V-270661, V-270662, V-270663, V-270669, V-270672, V-270673, V-270674, V-270676, V-270678, V-270679, V-270680, V-270681, V-270683, V-270684, V-270685, V-270686, V-270687, V-270688, V-270689, V-270692, V-270693, V-270696, V-270697, V-270698, V-270700, V-270701, V-270702, V-270702, V-270702, V-270702, V-270702, V-270703, V-270704, V-270705, V-270709, V-270715, V-270716, V-270718, V-270720, V-270721, V-270722, V-270723, V-270724, V-270725, V-270726, V-270727, V-270728, V-270729, V-270730, V-270730, V-270730, V-270730, V-270730, V-270731, V-270732, V-270733, V-270737, V-270739, V-270740, V-270741, V-270742, V-270743, V-270746, V-270750, V-270753, V-270755, V-270756, V-270757, V-270758, V-270759, V-270760, V-270765, V-270766, V-270767, V-270768, V-270769, V-270770, V-270771, V-270772, V-270773, V-270775, V-270776, V-270777, V-270778, V-270779, V-270780, V-270781, V-270782, V-270783, V-270784, V-270785, V-270786, V-270786, V-270786 87, V-270788, V-270789, V-270790, V-270791, V-270792, V-270793, V-270794, V-270795, V-270796, V-270797, V-270798, V-270799, V-270800, V-270801, V-270802, V-270803, V-270804, V-270804, V-270804, V-270804 805, V-270806, V-270807, V-270808, V-270809, V-270810, V-270811, V-270813, V-270814, V-270815, V-270821,

V-270822, V-270823, V-270824, V-270825, V-270826, V-270827, V-270828, V-270828, V-270829, V-270829, 270830, V-270831, V-270832, V-274870, V-274871, V-274872, dan V-274873

Linux STIG Tinggi (Kategori I)

Daftar berikut berisi pengaturan STIG yang EC2 didukung Amazon untuk infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewatkan setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap, lihat Perpustakaan STIGs Dokumen. Untuk informasi tentang cara melihat daftar lengkap, lihat Alat Melihat STIG.

> **Note**
>
> Kategori Linux STIG High mencakup semua pengaturan pengerasan STIG terdaftar yang berlaku untuk kategori Linux STIG Medium dan Low, selain pengaturan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori I.

RHEL 7 STIG Versi 3 Rilis 15

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

- RHEL 7/CentOS 7/ AL2

  V-204424, V-204425, V-204442, V-204443, V-204447, V-204448, V-204455, V-204497, V-204502, V-204594, V-204620, dan V-204621

RHEL 8 STIG Versi 2 Rilis 4

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

- RHEL 8/CentOS 8

  V-230221, V-230223, V-230226, V-230264, V-230265, V-230283, V-230284, V-230487, V-230492, V-230529, V-230530, V-230531, V-230533, V-230558, V-244540, dan V-26822

RHEL 9 STIG Versi 2 Rilis 5

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

- RHEL 9/CentOS Aliran 9

  V-257784, V-257785, V-257820, V-257821, V-257826, V-257835, V-257955, V-257956, V-257984, V-257986, V-258059, V-258078, V-258094, V-258230, V-258235, dan V-258238

Amazon Linux 2023 STIG Versi 1 Rilis 1

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-273996, V-273997, V-273999, V-274007, V-274038, V-274039, V-274046, V-274052, V-274057, dan V-274153

SLES 12 STIG Versi 3 Rilis 3

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-217101, V-217139, V-217141, V-217142, V-217159, V-217160, V-217264, V-217268, V-222386, dan V-251721

SLES 15 STIG Versi 2 Rilis 5

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-234800, V-234804, V-234818, V-234852, V-234859, V-234860, V-234898, V-234984, V-234985, V-234988, V-234989, V-234990, V-235031, V-235032, dan V-251725

Ubuntu 18.04 STIG Versi 2 Rilis 15

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-219157, V-219158, V-219177, V-219212, V-219308, V-219314, V-219316, V-251507, dan V-264388

Ubuntu 20.04 STIG Versi 2 Rilis 3

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-238201, V-238218, V-238219, V-238326, V-238327, V-238380, dan V-251504

Ubuntu 22.04 STIG Versi 2 Rilis 5

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-260469, V-260482, V-260483, V-260523, V-260524, V-260526, V-260529, V-260539, V-260570, V-260571, dan V-260579

Ubuntu 24.04 STIG Versi 1 Rilis 2

Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-270647, V-270648, V-270665, V-270666, V-270708, V-270711, V-270712, V-270713, V-270714, V-270717, dan V-270736

Pengaturan pengerasan STIG untuk instance Windows EC2

Amazon EC2 mendukung garis dasar STIG untuk versi sistem operasi Windows berikut:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Bagian ini mencantumkan pengaturan STIG saat ini yang EC2 didukung Amazon untuk infrastruktur Windows Anda, diikuti oleh log riwayat versi.

Anda dapat menerapkan pengaturan STIG rendah, sedang, atau tinggi.

Windows STIG Rendah (Kategori III)

Daftar berikut berisi pengaturan STIG yang EC2 didukung Amazon untuk infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewatkan setelan

itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap Windows STIGs, lihat Perpustakaan STIGs Dokumen. Untuk informasi tentang cara melihat daftar lengkap, lihat Alat Melihat STIG.

- Windows Server 2022 STIG Versi 2 Rilis 4

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363, dan V-254481
- Windows Server 2019 STIG Versi 3 Rilis 4

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871, dan V-205923
- Windows Server 2016 STIG Versi 2 Rilis 10

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942, dan V-225060
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5

  V-225250, V-225318, V-225319, V-225324, V-225327, V-225330, V-225331, V-225332, V-225333, V-225334, V-225335, V-225336, V-225342, V-225343, V-225355, V-225357, V-225358, V-225359, V-225360, V-225362, V-225363, V-225376, V-225392, V-225394, V-225412, V-225460, V-225462, V-225468, V-225473, V-225473, V-225473 76, V-225479, V-225480, V-225481, V-225482, V-225483, V-225484, V-225485, V-225487, V-225488, V-225489, V-225490, V-225511, V-225514, V-225525, V-225526, V-225526, V-225526, V-225526 25536, dan V-225537
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 6

  Tidak ada pengaturan STIG yang berlaku untuk kerentanan Microsoft .NET Framework untuk Kategori III.
- Windows Firewall STIG Versi 2 Rilis 2

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007, dan V-242008
- Internet Explorer 11 STIG Versi 2 Rilis 5

  V-223016, V-223056, dan V-223078
- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)

  V-235727, V-235731, V-235751, V-235752, dan V-235765

Windows STIG Medium (Kategori II)

Daftar berikut berisi pengaturan STIG yang EC2 didukung Amazon untuk infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewatkan setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap Windows STIGs, lihat Perpustakaan STIGs Dokumen. Untuk informasi tentang cara melihat daftar lengkap, lihat Alat Melihat STIG.

> **Note**
>
> Kategori Windows STIG Medium mencakup semua pengaturan pengerasan STIG yang terdaftar yang berlaku untuk Windows STIG rendah (Kategori III), selain pengaturan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II.

- Windows Server 2022 STIG Versi 2 Rilis 4

  Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

  V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254288, V-254288, V-254288 V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254312, V-254312, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254330, V-254331, V-254332, V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254365, V-254365, V-254365 366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254383, V-254384, V-254431, V-254432, V-254433, V-254434, V-254435, V-254436, V-254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254485, V-254486, V-254486, V-254486 V-254488, V-254489, V-254490, V-254493, V-254494, V-254495, V-254497,

V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254508, V-254509, V-254510, V-254511, dan V-254512

- Windows Server 2019 STIG Versi 3 Rilis 4

  Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

  V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205648, V-205649, V-205650, V-205651, V-205651, V-205652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205681, V-205683, V-205684, V-205685, V-205685, V-205685, V-205685 V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205766, V-205767, V-205768, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205795, V-205796, V-205797, V-205797, V-205797, V-205797, V-205797, V-205797 98, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828, V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205842, V-205861, V-205863, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925, V-236001, dan V-257503

- Windows Server 2016 STIG Versi 2 Rilis 10

  Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

  V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224870, V-224871, V-224871, V-224871, V-224871, V-224871 72, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224894, V-224894, V-224894, V-224894 24895, V-224896, V-224897, V-224898, V-224899, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224910, V-224910, V-224910 224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922,

V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224946, V-224946, V-224946, V-224946, V-224946 47, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040, V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225059, V-225061, V-225061, V-225062, V-225063, V-225064, V-225066, V-225067, V-225068, V-225069, V-225069, V-225069, 225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093 6000, dan V-257502

- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5

  Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

  V-225239, V-225259, V-225260, V-225261, V-225263, V-225264, V-225265, V-225266, V-225267, V-225268, V-225269, V-225270, V-225271, V-225272, V-225273, V-225275, V-225276, V-225277, V-225278, V-225279, V-225280, V-225281, V-225282, V-225283, V-225284, V-225285, V-225286, V-225287, V-225288, V-225289, V-225290, V-225296 1, V-225292, V-225293, V-225294, V-225295, V-225296, V-225297, V-225298, V-225299, V-225300, V-225301, V-225302, V-225303, V-225305, V-225314, V-225314, V-225314, V-225314, V-225314 15, V-225316, V-225317, V-225325, V-225326, V-225329, V-225337, V-225338, V-225339, V-225340, V-225341, V-225344, V-225345, V-225346, V-225347, V-225348, V-225349, V-225350, V-225351, V-225352, V-225353, V-225356, V-225367, V-225368, V-225369, V-225370, V-225371, V-225372, V-225373, V-225374, V-225375, V-225377, V-225378, V-225379, V-225380, V-225381, V-225382, V-225383, V-225384, V-225385, V-225386, V-225386, V-225386 389, V-225391, V-225393, V-225395, V-225397, V-225398, V-225400, V-225401, V-225402, V-225404, V-225405, V-225406, V-225407, V-225408, V-225409, V-225410, V-225410, V-225410, V-225410, V-225410, V-225410 25411, V-225413, V-225414, V-225415, V-225441, V-225442, V-225443, V-225448, V-225452, V-225453, V-225454, V-225455, V-225456, V-225457, V-225458, V-225461, V-225463, V-225464, V-225469, V-225470, V-225471, V-225472, V-225474, V-225475, V-225477, V-225477, V-225477, V-225477, V-225477, V-225477, V-225477 78, V-225486, V-225494, V-225500, V-225501, V-225502, V-225503, V-225504, V-225506, V-225508, V-225509, V-225510, V-225513, V-225515, V-225516, V-225517, V-225517, V-225517, V-225517 518, V-225519, V-225520, V-225521, V-225522, V-225523, V-225524, V-225527, V-225528, V-225529, V-225530, V-225531, V-225532, V-225533, V-225534,

V-225535, V-225535, V-225535, V-225535, V-225535, V-225535, V-225535, V-225538, V-225539, V-225540, V-225541, V-225542, V-225543, V-225544, V-225545, V-225546, V-225548, V-225549, V-225550, V-225551, V-225553, V-225554, V-225555, V-225557, V-225558, V-225559, V-225560, V-225561, V-225562, V-225563, V-225564, V-225565, V-225566, V-225567, V-225568, V-225569, V-225570, V-225571, V-225572, V-225573, dan V-225574

- Microsoft .NET Framework STIG 4.0 Versi 2 Rilis 6

  Termasuk semua setelan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

  V-225238

- Windows Firewall STIG Versi 2 Rilis 2

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

  V-241989, V-241990, V-241991, V-241993, V-241993, V-241998, dan V-242003

- Internet Explorer 11 STIG Versi 2 Rilis 5

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori III (Rendah), ditambah:

  V-223015, V-223017, V-223018, V-223019, V-223020, V-223021, V-223022, V-223023, V-223024, V-223025, V-223026, V-223027, V-223028, V-223029, V-223030, V-223031, V-223032, V-223033, V-223034, V-223035, V-223036, V-223037, V-223038, V-223039, V-223040, V-223041, V-223042, V-223043, V-223044, V-223045, V-223046, V-223048, V-223049, V-223050, V-223051, V-223052, V-223053, V-223053, V-223053, V-223053 54, V-223055, V-223057, V-223058, V-223059, V-223060, V-223061, V-223062, V-223063, V-223064, V-223065, V-223066, V-223067, V-223068, V-223069, V-223070, V-223071, V-223072, V-223073, V-223073, V-223073, V-223073, V-223073 3074, V-223075, V-223076, V-223077, V-223079, V-223080, V-223081, V-223082, V-223083, V-223084, V-223085, V-223086, V-223087, V-223088, V-223089, V-223090, V-223091, V-223092, V-223093, V-223093, V-223094, V-223095, V-223096, V-223097, V-223098, V-223099, V-223100, V-223101, V-223102, V-223103, V-223104, V-223105, V-223106, V-223107, V-223108, V-223109, V-223110, V-223111, V-223112, V-223113, V-223114, V-223115, V-223116, V-223117, V-223118, V-223119, V-223120, V-223121, V-223122, V-223124, V-223125, V-223126, V-223127, V-223128, V-223128, V-223128, V-223128 23129, V-223130, V-223131, V-223132, V-223133, V-223134, V-223135, V-223136, V-223137, V-223138, V-223139, V-223140, V-223141, V-223142, V-223143,

V-223144, V-223145, V-223146, V-223147, V-223148, V-223148 223149, V-250540, dan V-250541

- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)

  V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235768, V-235768, V-235768 69, V-235770, V-235771, V-235772, V-235773, V-235774, dan V-246736

- Microsoft Defender STIG Versi 2 Rilis 4

  V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213439, V-213440, V-213441, V-213442, V-213442, V-213442 43, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465, dan V-213466

Windows STIG Tinggi (Kategori I)

Daftar berikut berisi pengaturan STIG yang EC2 didukung Amazon untuk infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewatkan setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap Windows STIGs, lihat Perpustakaan STIGs Dokumen. Untuk informasi tentang cara melihat daftar lengkap, lihat Alat Melihat STIG.

> **Note**
>
> Kategori Windows STIG High mencakup semua pengaturan pengerasan STIG terdaftar yang berlaku untuk kategori Windows STIG Medium dan Low, selain pengaturan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori I.

- Windows Server 2022 STIG Versi 2 Rilis 4

  V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475, dan V-254500

- Windows Server 2019 STIG Versi 3 Rilis 4

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

  V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914, dan V-205919

- Windows Server 2016 STIG Versi 2 Rilis 10

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

  V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054, dan V-225079

- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

  V-225274, V-225354, V-225364, V-225365, V-225366, V-225390, V-225396, V-225399, V-225444, V-225449, V-225491, V-225492, V-225493, V-225496, V-225497, V-225498, V-225505, V-225507, V-225547, V-225552, dan V-225556

- Microsoft .NET Framework STIG 4.0 Versi 2 Rilis 6

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah) untuk Microsoft .NET Framework. Tidak ada pengaturan STIG tambahan yang berlaku untuk kerentanan Kategori I.

- Windows Firewall STIG Versi 2 Rilis 2

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

  V-241992, V-241997, dan V-242002

- Internet Explorer 11 STIG Versi 2 Rilis 5

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

  V-252910

- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

  V-235758 dan V-235759
- Microsoft Defender STIG Versi 2 Rilis 4

  Termasuk semua pengaturan pengerasan STIG yang EC2 didukung Amazon untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

  V-213426, V-213452, dan V-213453

Unduhan skrip pengerasan STIG

Amazon mengelompokkan skrip pengerasan STIG bersama-sama ke dalam bundel terkait sistem operasi untuk setiap rilis. Bundel adalah file arsip yang sesuai untuk sistem operasi target tempat mereka mengunduh dan menjalankannya. Bundel skrip Linux disimpan sebagai file TAR (ekstensi file.tgz). Bundel skrip Windows disimpan sebagai file ZIP (ekstensi file.zip).

Amazon menyimpan bundel skrip di `STIG` bucket EC2 Windows S3 di masing-masing. AWS Region Bundel Linux tidak memiliki bucket terpisah. Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.

Topik

- Prasyarat IAM untuk unduhan STIG
- Detail bundel unduhan STIG
- Riwayat versi Linux STIG
- Riwayat versi Windows STIG

Prasyarat IAM untuk unduhan STIG

Peran IAM yang Anda kaitkan dengan profil instans Anda harus memiliki `s3:GetObject` izin untuk mengunduh bundel skrip dari Amazon S3. Anda dapat menambahkan contoh kebijakan berikut ke peran profil instans Anda.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DownloadSTIGScriptBundles",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-windows-downloads*/STIG/*.zip",
                "arn:aws:s3:::aws-windows-downloads*/STIG/*.tgz"
            ]
        }
    ]
}
```

Untuk menambahkan contoh kebijakan unduhan STIG ke peran profil instans Anda sebagai kebijakan sebaris, ikuti kebijakan Perbarui izin untuk proses peran di Panduan Pengguna.AWS Identity and Access Management Untuk informasi selengkapnya tentang peran profil instans, lihat Menggunakan profil instance.

Detail bundel unduhan STIG

> **Important**
>
> Dengan beberapa pengecualian, skrip pengerasan STIG yang diunduh dokumen Systems Manager tidak menginstal paket pihak ketiga. Jika paket pihak ketiga sudah diinstal pada instance atau `InstallPackage` parameter disetel keyes, terkait STIGs yang EC2 didukung Amazon untuk paket tersebut diterapkan.

Saat Anda menjalankan perintah berikut dari AWS CLI, Amazon S3 mengunduh file bundel skrip pengerasan STIG terbaru dari bucket.

```
aws s3 cp s3://aws-windows-downloads-region/STIG/operating system/Latest/bundle-name destination-directory
```

Contoh: Unduh ke direktori sementara

Contoh ini menunjukkan bundel Linux yang diunduh ke `/tmp` direktori

```
aws s3 cp s3://aws-windows-downloads-us-east-1/STIG/Linux/
Latest/LinuxAWSConfigureSTIG.tgz /tmp
```

Pola dan contoh untuk jalur penyimpanan file unduhan dan nama file bundel adalah sebagai berikut:

Unduh jalur penyimpanan file

`s3://aws-windows-downloads-<region>/STIG/<operating system>/Latest/<bundle file name>`

Unduh variabel jalur

region

AWS Region (Setiap Wilayah memiliki keranjang unduhannya sendiri.)

operating system

Platform sistem operasi dari instance di mana STIGs diterapkan - baik `Linux` atau`Windows`.

bundle file name

Formatnya adalah*<os bundle name>*. *<file extension>*.

os bundle name

Awalan nama standar untuk bundel sistem operasi adalah salah satu `LinuxAWSConfigureSTIG` atau`AWSConfigureSTIG`. Untuk mempertahankan kompatibilitas mundur, unduhan untuk Windows tidak menyertakan awalan platform.

file extension

Format file terkompresi `tgz` (Linux) atau `zip` (Windows).

Contoh nama file bundel

- `LinuxAWSConfigureSTIG.tgz`
- `AWSConfigureSTIG.zip`

Riwayat versi Linux STIG

Bagian ini mencatat riwayat versi untuk bundel skrip Linux yang diperbarui setiap tiga bulan. Untuk melihat perubahan dan versi yang diterbitkan selama seperempat, pilih judul untuk memperluas

informasi. Jika tidak ada perubahan untuk kuartal tersebut, Anda akan melihatnya tercermin dalam judul.

Perubahan Q3 2025 - 09/04/2025:

Menambahkan dukungan untuk sistem operasi SUSE Linux Enterprise Server (SLES) dan Amazon Linux 2023. Memperbarui versi STIG berikut dan menerapkan STIGS untuk rilis kuartal ketiga 2025 untuk semua tingkat kepatuhan (): low/medium/high

STIG-Build-Linux versi 1.0.x

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 4
- RHEL 9 STIG Versi 2 Rilis 5
- Amazon Linux 2023 STIG Versi 1 Rilis 1
- SLES 12 STIG Versi 3 Rilis 3
- SLES 15 STIG Versi 2 Rilis 5
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 3
- Ubuntu 22.04 STIG Versi 2 Rilis 5
- Ubuntu 24.04 STIG Versi 1 Rilis 2

Perubahan Q2 2025 - 26/06/2025:

Memperbarui versi STIG berikut, menerapkan STIGS untuk rilis kuartal kedua 2025:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 3
- RHEL 9 STIG Versi 2 Rilis 4
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 2
- Ubuntu 22.04 STIG Versi 2 Rilis 4
- Ubuntu 24.04 STIG Versi 1 Rilis 1

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 3
- RHEL 9 STIG Versi 2 Rilis 4
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 2
- Ubuntu 22.04 STIG Versi 2 Rilis 4
- Ubuntu 24.04 STIG Versi 1 Rilis 1

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 3
- RHEL 9 STIG Versi 2 Rilis 4
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 2
- Ubuntu 22.04 STIG Versi 2 Rilis 4
- Ubuntu 24.04 STIG Versi 1 Rilis 1

Perubahan Q1 2025 - 04/11/2025:

Memperbarui versi STIG berikut, menerapkan STIGS untuk rilis kuartal pertama 2025, dan menambahkan dukungan untuk Ubuntu 24.04:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 2
- RHEL 9 STIG Versi 2 Rilis 3
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 2
- Ubuntu 22.04 STIG Versi 2 Rilis 3
- Ubuntu 24.04 STIG Versi 1 Rilis 1

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 2
- RHEL 9 STIG Versi 2 Rilis 3
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 2
- Ubuntu 22.04 STIG Versi 2 Rilis 3
- Ubuntu 24.04 STIG Versi 1 Rilis 1

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 2
- RHEL 9 STIG Versi 2 Rilis 3
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 2
- Ubuntu 22.04 STIG Versi 2 Rilis 3
- Ubuntu 24.04 STIG Versi 1 Rilis 1

Perubahan Q4 2024 - 12/10/2024:

Memperbarui versi STIG berikut, menerapkan STIGS untuk rilis kuartal keempat 2024, dan menambahkan informasi tentang dua parameter input baru untuk komponen Linux:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 1
- RHEL 9 STIG Versi 2 Rilis 2
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 1
- Ubuntu 22.04 STIG Versi 2 Rilis 2

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 1
- RHEL 9 STIG Versi 2 Rilis 2
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 1
- Ubuntu 22.04 STIG Versi 2 Rilis 2

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 15
- RHEL 8 STIG Versi 2 Rilis 1
- RHEL 9 STIG Versi 2 Rilis 2
- Ubuntu 18.04 STIG Versi 2 Rilis 15
- Ubuntu 20.04 STIG Versi 2 Rilis 1
- Ubuntu 22.04 STIG Versi 2 Rilis 2

Perubahan Q3 2024 - 10/04/2024 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Linux STIGS untuk rilis kuartal ketiga 2024.

Perubahan Q2 2024 - 05/10/2024:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal kedua 2024. Juga menambahkan dukungan untuk RHEL 9, CentOS Stream 9, dan Ubuntu 22.04, sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 14
- RHEL 9 STIG Versi 1 Rilis 3
- Ubuntu 18.04 STIG Versi 2 Rilis 14
- Ubuntu 20.04 STIG Versi 1 Rilis 12
- Ubuntu 22.04 STIG Versi 1 Rilis 1

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 14
- RHEL 9 STIG Versi 1 Rilis 3
- Ubuntu 18.04 STIG Versi 2 Rilis 14
- Ubuntu 20.04 STIG Versi 1 Rilis 12
- Ubuntu 22.04 STIG Versi 1 Rilis 1

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 14
- RHEL 9 STIG Versi 1 Rilis 3
- Ubuntu 18.04 STIG Versi 2 Rilis 14
- Ubuntu 20.04 STIG Versi 1 Rilis 12
- Ubuntu 22.04 STIG Versi 1 Rilis 1

Perubahan Q1 2024 - 02/06/2024:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal pertama 2024 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 13
- Ubuntu 18.04 STIG Versi 2 Rilis 13
- Ubuntu 20.04 STIG Versi 1 Rilis 11

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 13
- Ubuntu 18.04 STIG Versi 2 Rilis 13
- Ubuntu 20.04 STIG Versi 1 Rilis 11

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 13
- Ubuntu 18.04 STIG Versi 2 Rilis 13
- Ubuntu 20.04 STIG Versi 1 Rilis 11

Perubahan Q4 2023 - 12/07/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal keempat 2023 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 13
- RHEL 8 STIG Versi 1 Rilis 12
- Ubuntu 18.04 STIG Versi 2 Rilis 12
- Ubuntu 20.04 STIG Versi 1 Rilis 10

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 13
- RHEL 8 STIG Versi 1 Rilis 12
- Ubuntu 18.04 STIG Versi 2 Rilis 12
- Ubuntu 20.04 STIG Versi 1 Rilis 10

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 13
- RHEL 8 STIG Versi 1 Rilis 12
- Ubuntu 18.04 STIG Versi 2 Rilis 12
- Ubuntu 20.04 STIG Versi 1 Rilis 10

Perubahan Q3 2023 - 10/04/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal ketiga 2023 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 12
- RHEL 8 STIG Versi 1 Rilis 11
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 9

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 12
- RHEL 8 STIG Versi 1 Rilis 11
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 9

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 12
- RHEL 8 STIG Versi 1 Rilis 11
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 9

Perubahan Q2 2023 - 05/03/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal kedua 2023 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 11
- RHEL 8 STIG Versi 1 Rilis 10
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 8

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 11

- RHEL 8 STIG Versi 1 Rilis 10
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 8

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 11
- RHEL 8 STIG Versi 1 Rilis 10
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 8

Perubahan Q1 2023 - 27/03/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal pertama 2023 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 10
- RHEL 8 STIG Versi 1 Rilis 9
- Ubuntu 18.04 STIG Versi 2 Rilis 10
- Ubuntu 20.04 STIG Versi 1 Rilis 7

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 10
- RHEL 8 STIG Versi 1 Rilis 9
- Ubuntu 18.04 STIG Versi 2 Rilis 10
- Ubuntu 20.04 STIG Versi 1 Rilis 7

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 10
- RHEL 8 STIG Versi 1 Rilis 9
- Ubuntu 18.04 STIG Versi 2 Rilis 10

- Ubuntu 20.04 STIG Versi 1 Rilis 7

2022 Perubahan Q4 - 02/01/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal keempat 2022 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 9
- RHEL 8 STIG Versi 1 Rilis 8
- Ubuntu 18.04 STIG Versi 2 Rilis 9
- Ubuntu 20.04 STIG Versi 1 Rilis 6

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 9
- RHEL 8 STIG Versi 1 Rilis 8
- Ubuntu 18.04 STIG Versi 2 Rilis 9
- Ubuntu 20.04 STIG Versi 1 Rilis 6

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 9
- RHEL 8 STIG Versi 1 Rilis 8
- Ubuntu 18.04 STIG Versi 2 Rilis 9
- Ubuntu 20.04 STIG Versi 1 Rilis 6

2022 Perubahan Q3 - 30/09/2022 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Linux STIGS untuk rilis kuartal ketiga 2022.

2022 Perubahan Q2 - 08/02/2022:

Memperkenalkan dukungan Ubuntu, versi STIG yang diperbarui, dan menerapkan STIGS untuk rilis kuartal kedua 2022 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 7
- RHEL 8 STIG Versi 1 Rilis 6
- Ubuntu 18.04 STIG Versi 2 Rilis 6 (baru)
- Ubuntu 20.04 STIG Versi 1 Rilis 4 (baru)

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 7
- RHEL 8 STIG Versi 1 Rilis 6
- Ubuntu 18.04 STIG Versi 2 Rilis 6 (baru)
- Ubuntu 20.04 STIG Versi 1 Rilis 4 (baru)

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 7
- RHEL 8 STIG Versi 1 Rilis 6
- Ubuntu 18.04 STIG Versi 2 Rilis 6 (baru)
- Ubuntu 20.04 STIG Versi 1 Rilis 4 (baru)

2022 Perubahan Q1 - 26/04/2022:

Difaktorkan ulang untuk menyertakan dukungan yang lebih baik untuk wadah. Menggabungkan AL2 skrip sebelumnya dengan RHEL 7. Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal pertama 2022 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 6
- RHEL 8 STIG Versi 1 Rilis 5

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 6
- RHEL 8 STIG Versi 1 Rilis 5

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 6
- RHEL 8 STIG Versi 1 Rilis 5

2021 Perubahan Q4 - 12/20/2021:

Versi STIG yang diperbarui, dan menerapkan STIGS untuk rilis kuartal keempat 2021 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 5
- RHEL 8 STIG Versi 1 Rilis 4

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 5
- RHEL 8 STIG Versi 1 Rilis 4

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 5
- RHEL 8 STIG Versi 1 Rilis 4

2021 Perubahan Q3 - 09/30/2021:

Versi STIG yang diperbarui, dan menerapkan STIGS untuk rilis kuartal ketiga 2021 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 4
- RHEL 8 STIG Versi 1 Rilis 3

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 4

- RHEL 8 STIG Versi 1 Rilis 3

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 4
- RHEL 8 STIG Versi 1 Rilis 3

Riwayat versi Windows STIG

Bagian ini mencatat riwayat versi untuk bundel skrip Windows yang diperbarui setiap tiga bulan. Untuk melihat perubahan dan versi yang diterbitkan selama seperempat, pilih judul untuk memperluas informasi. Jika tidak ada perubahan untuk kuartal tersebut, Anda akan melihatnya tercermin dalam judul.

Perubahan Q3 2025 - 9/04/2025 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal ketiga 2025.

Perubahan Q2 2025 - 26/06/2025:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis Q2 2025 sebagai berikut:

Windows STIG Rendah (Kategori III)

- Windows Server 2022 STIG Versi 2 Rilis 4
- Windows Server 2019 STIG Versi 3 Rilis 4
- Windows Server 2016 STIG Versi 2 Rilis 10
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 6
- Windows Firewall STIG Versi 2 Rilis 2
- Internet Explorer 11 STIG Versi 2 Rilis 5
- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)

Windows STIG Medium (Kategori II)

- Windows Server 2022 STIG Versi 2 Rilis 4
- Windows Server 2019 STIG Versi 3 Rilis 4

- Windows Server 2016 STIG Versi 2 Rilis 10
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 6
- Windows Firewall STIG Versi 2 Rilis 2
- Internet Explorer 11 STIG Versi 2 Rilis 5
- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)
- Defender STIG Versi 2 Rilis 4

Windows STIG Tinggi (Kategori I)

- Windows Server 2022 STIG Versi 2 Rilis 4
- Windows Server 2019 STIG Versi 3 Rilis 4
- Windows Server 2016 STIG Versi 2 Rilis 10
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 6
- Windows Firewall STIG Versi 2 Rilis 2
- Internet Explorer 11 STIG Versi 2 Rilis 5
- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)
- Defender STIG Versi 2 Rilis 4

Perubahan Q1 2025 - 05/04/2025:

STIGS yang diperbarui untuk Internet Explorer 11 STIG Versi 2 Rilis 5 untuk semua komponen STIG untuk rilis kuartal pertama 2025.

Perubahan Q4 2024 - 12/10/2024:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis Q4 2024 sebagai berikut:

Windows STIG Rendah (Kategori III)

- Windows Server 2022 STIG Versi 2 Rilis 2
- Windows Server 2019 STIG Versi 3 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 9

- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 2
- Internet Explorer 11 STIG Versi 2 Rilis 5
- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)

Windows STIG Medium (Kategori II)

- Windows Server 2022 STIG Versi 2 Rilis 2
- Windows Server 2019 STIG Versi 3 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 9
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 2
- Internet Explorer 11 STIG Versi 2 Rilis 5
- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)
- Defender STIG Versi 2 Rilis 4

Windows STIG Tinggi (Kategori I)

- Windows Server 2022 STIG Versi 2 Rilis 2
- Windows Server 2019 STIG Versi 3 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 9
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 2
- Internet Explorer 11 STIG Versi 2 Rilis 5
- Microsoft Edge STIG Versi 2 Rilis 2 (hanya Windows Server 2022)
- Defender STIG Versi 2 Rilis 4

Perubahan Q3 2024 - 10/04/2024 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal ketiga 2024.

Perubahan Q2 2024 - 05/10/2024 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal kedua 2024.

Perubahan Q1 2024 - 23/02/2024 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal pertama 2024.

Perubahan Q4 2023 - 12/07/2023 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal keempat 2023.

Perubahan Q3 2023 - 10/04/2023 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal ketiga 2023.

Perubahan Q2 2023 - 05/03/2023 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal kedua 2023.

Perubahan Q1 2023 - 27/03/2023 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal pertama 2023.

2022 Perubahan Q4 - 02/01/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis Q4 2022 sebagai berikut:

Windows STIG Rendah (Kategori III)

- Windows Server 2022 STIG Versi 1 Rilis 1
- Windows Server 2019 STIG Versi 2 Rilis 5
- Windows Server 2016 STIG Versi 2 Rilis 5
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 2 Rilis 3
- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)

Windows STIG Medium (Kategori II)

- Windows Server 2022 STIG Versi 1 Rilis 1

- Windows Server 2019 STIG Versi 2 Rilis 5
- Windows Server 2016 STIG Versi 2 Rilis 5
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 2 Rilis 3
- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)
- Defender STIG Versi 2 Rilis 4 (hanya Windows Server 2022)

Windows STIG Tinggi (Kategori I)

- Windows Server 2022 STIG Versi 1 Rilis 1
- Windows Server 2019 STIG Versi 2 Rilis 5
- Windows Server 2016 STIG Versi 2 Rilis 5
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 2 Rilis 3
- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)
- Defender STIG Versi 2 Rilis 4 (hanya Windows Server 2022)

2022 Perubahan Q3 - 30/09/2022 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal ketiga 2022.

2022 Perubahan Q2 - 08/02/2022:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis Q2 2022.

Windows STIG Rendah (Kategori III)

- Windows Server 2019 STIG Versi 2 Rilis 4
- Windows Server 2016 STIG Versi 2 Rilis 4
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3

- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

Windows STIG Medium (Kategori II)

- Windows Server 2019 STIG Versi 2 Rilis 4
- Windows Server 2016 STIG Versi 2 Rilis 4
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

Windows STIG Tinggi (Kategori I)

- Windows Server 2019 STIG Versi 2 Rilis 4
- Windows Server 2016 STIG Versi 2 Rilis 4
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

2022 Perubahan Q1 - 08/02/2022 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal pertama 2022.

2021 Perubahan Q4 - 12/20/2021:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal keempat 2021.

Windows STIG Rendah (Kategori III)

- Windows Server 2019 STIG Versi 2 Rilis 3
- Windows Server 2016 STIG Versi 2 Rilis 3
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3

- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

Windows STIG Medium (Kategori II)

- Windows Server 2019 STIG Versi 2 Rilis 3
- Windows Server 2016 STIG Versi 2 Rilis 3
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

Windows STIG Tinggi (Kategori I)

- Windows Server 2019 STIG Versi 2 Rilis 3
- Windows Server 2016 STIG Versi 2 Rilis 3
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

2021 Perubahan Q3 - 09/30/2021:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal ketiga 2021.

Windows STIG Rendah (Kategori III)

- Windows Server 2019 STIG Versi 2 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 2
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 2
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 1 Rilis 7
- Internet Explorer 11 STIG Versi 1 Rilis 19

Windows STIG Medium (Kategori II)

- Windows Server 2019 STIG Versi 2 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 2
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 2
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 1 Rilis 7
- Internet Explorer 11 STIG Versi 1 Rilis 19

Windows STIG Tinggi (Kategori I)

- Windows Server 2019 STIG Versi 2 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 2
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 2
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 1 Rilis 7
- Internet Explorer 11 STIG Versi 1 Rilis 19

Gunakan AWS Systems Manager untuk menerapkan pengaturan STIG ke instans Anda

Anda dapat menggunakan dokumen perintah `AWSEC2-ConfigureSTIG` Systems Manager untuk menerapkan pengaturan STIG ke EC2 instance yang ada. Anda harus menjalankan dokumen perintah dari contoh yang diperbarui. Dokumen perintah menerapkan pengaturan yang sesuai berdasarkan sistem operasi dan konfigurasi instance di mana ia berjalan.

Halaman ini berisi rincian tentang dokumen `AWSEC2-ConfigureSTIG` perintah, termasuk parameter input dan cara menjalankannya di konsol Systems Manager atau dengan `send-command` di AWS CLI.

AWSEC2-ConfigureSTIGparameter masukan

Anda dapat memberikan parameter input berikut untuk menentukan bagaimana dokumen perintah harus menerapkan pengaturan STIG ke instance Anda.

Level (string, diperlukan)

Tentukan kategori keparahan STIG untuk diterapkan. Nilai-nilai yang valid meliputi:

- Tinggi
- Sedang
- Rendah

Jika Anda tidak menentukan nilai default sistem. `High`

InstallPackages(string, opsional — hanya Linux)

Jika nilainya`No`, skrip tidak menginstal paket perangkat lunak tambahan apa pun. Jika nilainya`Yes`, skrip menginstal paket perangkat lunak tambahan yang diperlukan untuk kepatuhan maksimum. Nilai default-nya adalah `No`.

SetDoDConsentBanner (string, opsional — hanya Linux)

Jika nilainya`No`, spanduk persetujuan DoD tidak ditampilkan saat Anda melampirkan ke instance yang memiliki skrip STIG Linux diinstal. Jika nilainya`Yes`, spanduk persetujuan DoD ditampilkan sebelum Anda masuk saat Anda melampirkan ke instance yang memiliki salah satu skrip STIG Linux diinstal. Anda harus mengakui spanduk sebelum Anda dapat masuk. Nilai default-nya adalah `No`.

Untuk contoh spanduk persetujuan, lihat Pemberitahuan Privasi dan Persetujuan Departemen Pertahanan Penafian yang muncul saat Anda mengakses situs web Layanan Dokumen DLA.

Jalankan dokumen AWSEC2-ConfigureSTIG perintah

Untuk menjalankan dokumen `AWSEC2-ConfigureSTIG`, ikuti langkah-langkah untuk lingkungan pilihan Anda.

Console

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Pilih Jalankan Perintah dari panel navigasi. Ini menunjukkan daftar perintah yang sedang berjalan di akun Anda, jika berlaku.
3. Pilih Jalankan perintah. Ini membuka dialog Run a command dan menampilkan daftar dokumen perintah yang dapat Anda akses.

4. Pilih `AWSEC2-ConfigureSTIG` dari daftar dokumen perintah. Untuk merampingkan hasil, Anda dapat memasukkan semua atau sebagian dari nama dokumen. Anda juga dapat memfilter berdasarkan pemilik, berdasarkan jenis platform, atau dengan tanda.

   Saat Anda memilih dokumen perintah, detail terisi di bawah daftar.

5. Pilih `Default version at runtime` dari daftar Versi dokumen.

6. Konfigurasikan parameter Command untuk menentukan bagaimana `AWSEC2-ConfigureSTIG` akan menginstal paket skrip dan menjalankannya untuk memperbarui instance Anda. Untuk detail parameter, lihat AWSEC2-ConfigureSTIGparameter masukan.

7. Untuk pemilihan target, tentukan tanda atau pilih instans secara manual untuk mengidentifikasi instans untuk menjalankan operasi ini.

   > **Note**
   >
   > Jika Anda memilih instans secara manual, dan instans yang ingin Anda lihat tidak disertakan dalam daftar, lihat Di Mana Instans Saya? untuk kiat pemecahan masalah.

8. Untuk parameter tambahan guna menentukan perilaku Run Command Systems Manager seperti Kontrol laju, masukkan nilai seperti yang dijelaskan dalam Menjalankan perintah dari konsol.

9. Pilih Jalankan.

   Jika berhasil, dokumen perintah menginstal skrip dan mengkonfigurasi instance Anda. Jika pelaksanaan perintah gagal, lihat output perintah Systems Manager untuk detail tentang alasan pelaksanaan tersebut gagal.

AWS CLI

Contoh 1: Jalankan dengan nilai default

Jalankan perintah berikut untuk menginstal skrip STIG dan menjalankannya dengan nilai default. Untuk informasi selengkapnya tentang parameter input, lihatAWSEC2-ConfigureSTIGparameter masukan.

```
aws ssm send-command \
 --document-name "AWSEC2-ConfigureSTIG" \
 --instance-ids "i-1234567890abcdef0"'
```

Contoh 2: Konfigurasikan pengaturan STIG tingkat Menengah pada instans Anda

Jalankan perintah berikut untuk menginstal skrip STIG dan menjalankannya dengan parameter `Level` input diatur ke`Medium`. Untuk informasi selengkapnya tentang parameter input, lihatAWSEC2-ConfigureSTIGparameter masukan.

```
aws ssm send-command \
 --document-name "AWSEC2-ConfigureSTIG" \
 --instance-ids "i-1234567890abcdef0"
 --parameters '{"Level":"Medium"}'
```

Jika berhasil, dokumen perintah menginstal skrip dan mengkonfigurasi instance Anda. Jika pelaksanaan perintah gagal, lihat output perintah untuk detail tentang alasan pelaksanaan tersebut gagal.

PowerShell

Contoh 1: Jalankan dengan nilai default

Jalankan perintah berikut untuk menginstal skrip STIG dan menjalankannya dengan nilai default. Untuk informasi selengkapnya tentang parameter input, lihatAWSEC2-ConfigureSTIGparameter masukan.

```
Send-SSMCommand -DocumentName "AWSEC2-ConfigureSTIG" -InstanceId
 "i-1234567890abcdef0"}
```

Contoh 2: Konfigurasikan pengaturan STIG tingkat Menengah pada instans Anda

Jalankan perintah berikut untuk menginstal skrip STIG dan menjalankannya dengan parameter `Level` input diatur ke`Medium`. Untuk informasi selengkapnya tentang parameter input, lihatAWSEC2-ConfigureSTIGparameter masukan.

```
Send-SSMCommand -DocumentName "AWSEC2-ConfigureSTIG" -InstanceId
 "i-1234567890abcdef0" -Parameter @{'Level'='Medium'}
```

Jika berhasil, dokumen perintah menginstal skrip dan mengkonfigurasi instance Anda. Jika pelaksanaan perintah gagal, lihat output perintah untuk detail tentang alasan pelaksanaan tersebut gagal.

Jam presisi dan sinkronisasi waktu pada instans EC2 Anda

Referensi waktu yang konsisten dan akurat pada instans Amazon EC2 Anda sangat penting untuk banyak tugas dan proses server. Stempel waktu dalam log sistem memainkan peran penting dalam mengidentifikasi kapan masalah terjadi dan urutan kronologis peristiwa. Saat Anda menggunakan AWS CLI atau AWS SDK untuk membuat permintaan dari instans Anda, alat ini menandatangani permintaan atas nama Anda. Jika pengaturan tanggal dan waktu instans Anda tidak akurat, hal itu dapat mengakibatkan perbedaan antara tanggal dalam tanda tangan dan tanggal permintaan, yang menyebabkan AWS penolakan permintaan Anda.

Untuk mengatasi aspek penting ini, Amazon menawarkan Layanan Amazon Time Sync, yang dapat diakses dari semua instans EC2 dan digunakan oleh berbagai Layanan AWS. Layanan ini menggunakan armada jam referensi yang terhubung dengan satelit dan atom di masing-masing AWS Region untuk memberikan pembacaan waktu yang akurat dan terkini dari standar global Coordinated Universal Time (UTC).

Untuk performa terbaik, sebaiknya gunakan Layanan Sinkronisasi Waktu Amazon lokal pada instans EC2 Anda. Untuk cadangan ke Layanan Sinkronisasi Waktu Amazon lokal pada instans Anda, atau untuk menghubungkan sumber daya di luar Amazon EC2 ke Layanan Sinkronisasi Waktu Amazon, Anda dapat menggunakan Layanan Sinkronisasi Waktu Amazon publik yang terletak di. `time.aws.com` Layanan Amazon Time Sync publik, seperti Layanan Amazon Time Sync, secara otomatis menyebarkan setiap detik kabisat yang ditambahkan ke UTC. Layanan Sinkronisasi Waktu Amazon publik didukung secara global oleh armada jam referensi atom dan terhubung satelit kami di masing-masing. AWS Region

Stempel waktu paket perangkat keras

Anda dapat mengaktifkan stempel waktu paket perangkat keras pada instans Anda untuk menambahkan stempel waktu presisi nanodetik 64-bit ke setiap paket jaringan yang masuk. Karena stempel waktu paket perangkat keras terjadi pada tingkat perangkat keras — sebelum paket mencapai kernel, soket, atau lapisan aplikasi — Anda melewati penundaan yang ditambahkan oleh stempel waktu perangkat lunak. Jam referensi yang mendasari untuk stempel waktu perangkat keras adalah jam perangkat keras Amazon Time Sync Service PTP.

Manfaat

Stempel waktu paket perangkat keras memberikan manfaat sebagai berikut:

- Meningkatkan pemesanan acara, yang juga dapat digunakan untuk menentukan urutan aktual di mana paket tiba di instans EC2 Anda, memastikan pemrosesan paket yang adil.
- Mengukur latensi jaringan satu arah.
- Meningkatkan kecepatan transaksi terdistribusi dengan presisi dan akurasi yang lebih tinggi dibandingkan dengan kebanyakan solusi lokal.

Prasyarat dan konfigurasi

Untuk mengaktifkan stempel waktu paket perangkat keras, instans Anda harus memenuhi prasyarat berikut:

- Harus berupa contoh Linux.
- Memenuhi persyaratan untuk mendukung jam perangkat keras PTP.

Untuk petunjuk konfigurasi, lihat Hardware Packet Timestamping pada driver kernel Linux untuk halaman keluarga Elastic Network Adapter (ENA). GitHub

Detik kabisat

Detik kabisat, diperkenalkan pada tahun 1972, merupakan penyesuaian satu detik sesekali pada waktu UTC untuk memperhitungkan penyimpangan dalam rotasi bumi, untuk mengakomodasi perbedaan antara Waktu Atom Internasional (KAI) dan waktu matahari (Ut1). Untuk mengelola detik kabisat atas nama pelanggan, kami merancang smearing detik kabisat dalam Layanan Amazon Time Sync. Untuk informasi selengkapnya, lihat Lihat Sebelum Anda Melompat — Detik Kabisat yang Akan Datang dan AWS.

Detik kabisat akan hilang, dan kami mendukung penuh keputusan yang dibuat pada Konferensi Umum ke-27 tentang Berat dan Ukuran untuk meninggalkan detik kabisat pada atau sebelum 2035.

Untuk mendukung transisi ini, kami masih berencana untuk smearing waktu peristiwa detik kabisat saat mengakses Layanan Amazon Time Sync melalui koneksi NTP lokal atau kolam NTP publik kami (`time.aws.com`). Namun, jam perangkat keras tidak menyediakan opsi waktu dengan smearing. Jika terjadi detik kabisat, jam perangkat keras PTP akan menambahkan detik kabisat mengikuti standar UTC. Sumber waktu leap-smeared dan detik kabisat adalah sama dalam banyak kasus. Namun, karena keduanya berbeda selama peristiwa detik kabisat, kami tidak menyarankan penggunaan sumber waktu dengan smearing maupun tanpa smearing dalam konfigurasi klien waktu Anda selama peristiwa detik kabisat.

Topik

- Setel referensi waktu pada instans EC2 Anda untuk menggunakan Layanan Sinkronisasi Waktu Amazon lokal
- Tetapkan referensi waktu pada instans EC2 Anda atau perangkat yang terhubung ke internet untuk menggunakan Layanan Sinkronisasi Waktu Amazon publik
- Bandingkan stempel waktu untuk instans Linux Anda
- Ubah zona waktu instans Anda

Sumber daya terkait

- AWS Compute Blog: Sudah Saatnya: Jam Akurat Mikrodetik di Instans Amazon EC2
- AWS Blog Operasi & Migrasi Cloud: Kelola akurasi jam instans Amazon EC2 menggunakan Layanan Sinkronisasi Waktu Amazon dan CloudWatch Amazon - Bagian 1
- (Linux) https://chrony-project.org/

Setel referensi waktu pada instans EC2 Anda untuk menggunakan Layanan Sinkronisasi Waktu Amazon lokal

Layanan Sinkronisasi Waktu Amazon lokal menggunakan Network Time Protocol (NTP), atau menyediakan jam perangkat keras Precision Time Protocol (PTP) lokal pada instans yang didukung. Jam perangkat keras PTP mendukung koneksi NTP (instance Linux dan Windows), atau koneksi PTP langsung (hanya instance Linux). Koneksi NTP dan PTP langsung menggunakan sumber waktu yang sangat akurat yang sama, tetapi koneksi PTP langsung lebih akurat daripada koneksi NTP. Koneksi NTP ke Amazon Time Sync Service mendukung leap smearing sementara koneksi PTP ke jam perangkat keras PTP tidak merusak waktu. Untuk informasi selengkapnya, lihat Detik kabisat.

Instans Anda dapat mengakses Layanan Amazon Time Sync lokal sebagai berikut:

- Melalui NTP di titik akhir alamat IP berikut ini:
  - IPv4: `169.254.169.123`
  - IPv6: `fd00:ec2::123` (Hanya dapat diakses pada instance berbasis Nitro.)

- (Hanya Linux) Melalui koneksi PTP langsung untuk terhubung ke jam perangkat keras PTP lokal:
  - `PHC0`

Amazon Linux AMIs, Windows AMIs, dan sebagian besar mitra AMIs mengonfigurasi instans Anda untuk menggunakan IPv4 titik akhir NTP secara default. Ini adalah pengaturan yang disarankan untuk sebagian besar beban kerja pelanggan. Tidak diperlukan konfigurasi lebih lanjut untuk instance yang diluncurkan dari ini AMIs kecuali Anda ingin menggunakan IPv6 titik akhir atau terhubung langsung ke jam perangkat keras PTP.

Koneksi NTP dan PTP tidak memerlukan perubahan konfigurasi VPC apa pun, dan instans Anda tidak memerlukan akses ke internet.

Pertimbangan-pertimbangan

- Ada batas 1024 paket per detik (PPS) untuk layanan yang menggunakan alamat link-lokal. Batas ini mencakup agregat Kueri DNS Route 53 Resolver, permintaan Layanan Metadata Instans (IMDS), permintaan Amazon Time Service Network Time Protocol (NTP), dan permintaan Layanan Lisensi Windows (untuk instance berbasis Microsoft Windows).
- Hanya instance Linux yang dapat menggunakan koneksi PTP langsung untuk terhubung ke jam perangkat keras PTP lokal. Instans Windows menggunakan NTP untuk terhubung ke jam perangkat keras PTP lokal.

Daftar Isi

- Sambungkan ke IPv4 titik akhir Layanan Sinkronisasi Waktu Amazon
- Sambungkan ke IPv6 titik akhir Layanan Sinkronisasi Waktu Amazon
- Terhubung ke jam perangkat keras PTP

Sambungkan ke IPv4 titik akhir Layanan Sinkronisasi Waktu Amazon

AMI Anda mungkin sudah mengonfigurasi Layanan Sinkronisasi Waktu Amazon secara default. Jika tidak, gunakan prosedur berikut untuk mengonfigurasi instans agar menggunakan Layanan Sinkronisasi Waktu Amazon lokal melalui IPv4 titik akhir.

Untuk membantu mengatasi masalah masalah, lihat Memecahkan masalah sinkronisasi NTP pada instance Linux atau Memecahkan masalah waktu pada instance Windows.

Amazon Linux

AL2023 dan versi terbaru Amazon Linux 2 dikonfigurasi untuk menggunakan IPv4 titik akhir Layanan Sinkronisasi Waktu Amazon secara default. Jika Anda mengonfirmasi bahwa instans Anda sudah dikonfigurasi, Anda dapat melewati prosedur berikut.

Untuk memverifikasi bahwa chrony dikonfigurasi untuk menggunakan titik akhir IPv4

Jalankan perintah berikut. Dalam output, garis yang dimulai dengan ^* menunjukkan sumber waktu yang disukai.

```
chronyc sources -v | grep -F ^*
^* 169.254.169.123               3   4   377    14    +12us[+9653ns] +/-  290us
```

Untuk mengonfigurasi chrony agar terhubung ke IPv4 titik akhir pada versi Amazon Linux 2 yang lebih lama

1. Hubungkan ke instans Anda dan hapus instalasi layanan NTP.

   ```
   [ec2-user ~]$ sudo yum erase 'ntp*'
   ```

2. Instal paket `chrony`.

   ```
   [ec2-user ~]$ sudo yum install chrony
   ```

3. Buka `/etc/chrony.conf` file menggunakan editor teks (sepertivim ataunano). Tambahkan baris berikut sebelum pernyataan lain `server` atau `pool` pernyataan yang mungkin ada dalam file, dan simpan perubahan Anda:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

4. Mulai ulang daemon `chrony` (`chronyd`).

   ```
   [ec2-user ~]$ sudo service chronyd restart
   ```

   ```
   Starting chronyd:                                          [  OK  ]
   ```

> **Note**
>
> Di RHEL dan CentOS (hingga versi 6), nama layanannya adalah `chrony`, bukan `chronyd`.

5. Untuk mengonfigurasi `chronyd` agar dimulai di setiap boot sistem, gunakan perintah `chkconfig`.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. Verifikasi `chrony` bahwa menggunakan `169.254.169.123` IPv4 titik akhir untuk menyinkronkan waktu.

```
[ec2-user ~]$ chronyc sources -v | grep -F ^*
```

Dalam output, `^*` menunjukkan sumber waktu yang disukai.

```
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-  287us
```

7. Verifikasi metrik sinkronisasi waktu yang dilaporkan oleh `chrony`.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
Stratum         : 4
Ref time (UTC)  : Wed Nov 22 13:18:34 2017
System time     : 0.000000626 seconds slow of NTP time
Last offset     : +0.002852759 seconds
RMS offset      : 0.002852759 seconds
Frequency       : 1.187 ppm fast
Residual freq   : +0.020 ppm
Skew            : 24.388 ppm
Root delay      : 0.000504752 seconds
Root dispersion : 0.001112565 seconds
Update interval : 64.4 seconds
Leap status     : Normal
```

Ubuntu

Untuk mengkonfigurasi chrony untuk terhubung ke IPv4 titik akhir di Ubuntu

1. Hubungkan ke instans Anda dan gunakan `apt` untuk memasang paket `chrony`.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> Jika perlu, perbarui instans Anda terlebih dahulu dengan menjalankan `sudo apt update`.

2. Buka file `/etc/chrony/chrony.conf` menggunakan editor teks (seperti vim atau nano). Tambahkan baris sebelum `server` yang lain atau pernyataan `pool` yang sudah ada di file, dan simpan perubahan Anda.

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Mulai ulang layanan `chrony`.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Verifikasi `chrony` bahwa menggunakan `169.254.169.123` IPv4 titik akhir untuk menyinkronkan waktu.

```
ubuntu:~$ chronyc sources -v | grep -F ^*
```

Dalam output, garis yang dimulai dengan `^*` menunjukkan sumber waktu yang disukai.

```
^* 169.254.169.123               3   6    17    12    +15us[  +57us] +/-  320us
```

5. Verifikasi metrik sinkronisasi waktu yang dilaporkan oleh `chrony`.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : 169.254.169.123 (169.254.169.123)
Stratum         : 4
Ref time (UTC)  : Wed Nov 29 07:41:57 2017
System time     : 0.000000011 seconds slow of NTP time
Last offset     : +0.000041659 seconds
RMS offset      : 0.000041659 seconds
Frequency       : 10.141 ppm slow
Residual freq   : +7.557 ppm
Skew            : 2.329 ppm
Root delay      : 0.000544 seconds
Root dispersion : 0.000631 seconds
Update interval : 2.0 seconds
Leap status     : Normal
```

SUSE Linux

Dimulai dengan SUSE Linux Enterprise Server 15, `chrony` adalah implementasi default NTP.

Untuk mengkonfigurasi chrony untuk terhubung ke IPv4 endpoint di SUSE Linux

1. Buka file `/etc/chrony.conf` menggunakan editor teks (seperti vim atau nano).
2. Pastikan bahwa file tersebut berisi baris berikut:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

   Jika baris ini tidak ada, tambahkan.
3. Komentari baris server atau kolam lainnya.
4. Buka YaST dan aktifkan layanan chrony.

Windows

Dimulai dengan rilis Agustus 2018, Windows AMIs menggunakan Layanan Sinkronisasi Waktu Amazon secara default. Tidak diperlukan konfigurasi lebih lanjut untuk instance yang diluncurkan dari ini AMIs dan Anda dapat melewati prosedur berikut.

Jika Anda menggunakan AMI yang tidak memiliki Layanan Sinkronisasi Waktu Amazon yang dikonfigurasi secara default, pertama-tama verifikasi konfigurasi NTP Anda saat ini. Jika instans Anda sudah menggunakan IPv4 titik akhir Layanan Sinkronisasi Waktu Amazon, konfigurasi

lebih lanjut tidak diperlukan. Jika instans Anda tidak menggunakan Layanan Amazon Time Sync, selesaikan prosedur untuk mengubah server NTP agar menggunakan Layanan Amazon Time Sync.

Untuk memverifikasi konfigurasi NTP

1. Dari instans Anda, buka jendela Command Prompt.
2. Dapatkan konfigurasi NTP saat ini dengan mengetikkan perintah berikut:

   ```
   w32tm /query /configuration
   ```

   Perintah ini mengembalikan pengaturan konfigurasi saat ini untuk instans Windows dan akan ditampilkan jika Anda terhubung ke Layanan Amazon Time Sync.
3. (Opsional) Dapatkan status konfigurasi saat ini dengan mengetik perintah berikut:

   ```
   w32tm /query /status
   ```

   Perintah ini mengembalikan informasi seperti terakhir kali instans disinkronkan dengan server NTP dan interval polling.

Untuk mengubah server NTP agar menggunakan Layanan Amazon Time Sync

1. Dari jendela Command Prompt, jalankan perintah berikut:

   ```
   w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
   ```
2. Verifikasi pengaturan baru Anda dengan menggunakan perintah berikut:

   ```
   w32tm /query /configuration
   ```

   Dalam output yang dikembalikan, verifikasi bahwa `NtpServer` menampilkan `169.254.169.123` IPv4 titik akhir.

Pengaturan NTP default untuk Amazon Windows AMIs

Amazon Machine Images (AMI) umumnya mematuhi out-of-the-box default kecuali dalam kasus di mana perubahan diperlukan untuk berfungsi pada infrastruktur EC2. Pengaturan berikut telah

ditetapkan agar bekerja dengan baik di lingkungan virtual, serta untuk menjaga agar setiap perbedaan waktu tetap dalam akurasi satu detik:

- Interval Pembaruan - Mengatur seberapa sering layanan waktu akan menyesuaikan waktu sistem terhadap akurasi. AWS mengonfigurasi interval pembaruan untuk terjadi setiap dua menit sekali.
- Server NTP - Dimulai dengan rilis Agustus 2018, AMIs gunakan Layanan Sinkronisasi Waktu Amazon secara default. Layanan kali ini dapat diakses dari mana saja AWS Region di titik akhir 169.254.169.123 IPv4 . Selain itu, bendera 0x9 menunjukkan bahwa layanan waktu bertindak sebagai klien, dan untuk menggunakan `SpecialPollInterval` untuk menentukan seberapa sering pemeriksaan dengan server waktu yang dikonfigurasi.
- Tipe - "NTP" berarti bahwa layanan bertindak sebagai klien NTP mandiri, alih-alih bertindak sebagai bagian dari domain.
- Diaktifkan dan InputProvider - Layanan waktu diaktifkan dan menyediakan waktu ke sistem operasi.
- Interval Poll Khusus - Memeriksa Server NTP yang dikonfigurasi setiap 900 detik (15 menit).

> **Note**
>
> Untuk Windows Server 2025 AMIs, `SpecialPollInterval` nilainya 1024 detik, bukan 900 detik.

Jalur registri	Nama kunci	Data
HKL M:\System\\ layananCurrentControlSet\ w32time\ Config	UpdateInterval	120
HKL M:\System\\ layananCurrentControlSet\ w32time\ Parameter	NtpServer	169.254.169.123,0x9
HKL M:\System\\ layananCurrentControlSet\ w32time\ Parameter	Tipe	NTP

Jalur registri	Nama kunci	Data
HKL M:\System\\ layananCurrentControlSet\ w32time\\ TimeProviders NtpClient	Aktif	1
HKL M:\System\\ layananCurrentControlSet\ w32time\\ TimeProviders NtpClient	InputProvider	1
HKL M:\System\\ layananCurrentControlSet\ w32time\\ TimeProviders NtpClient	SpecialPollInterval	900 (Windows Server 2016, 2019, dan 2022) atau 1024 (Windows Server 2025)

Sambungkan ke IPv6 titik akhir Layanan Sinkronisasi Waktu Amazon

Bagian ini menjelaskan Sambungkan ke IPv4 titik akhir Layanan Sinkronisasi Waktu Amazon perbedaan langkah yang dijelaskan jika Anda mengonfigurasi instans untuk menggunakan Layanan Sinkronisasi Waktu Amazon lokal melalui titik IPv6 akhir. Bagian ini tidak menjelaskan seluruh proses konfigurasi Layanan Amazon Time Sync.

IPv6 Titik akhir hanya dapat diakses pada instance berbasis Nitro.

Kami tidak menyarankan untuk menggunakan entri IPv4 dan IPv6 endpoint secara bersamaan. Paket IPv4 dan IPv6 NTP berasal dari server lokal yang sama untuk instance Anda. Mengkonfigurasi keduanya IPv4 dan IPv6 titik akhir tidak perlu dan tidak akan meningkatkan akurasi waktu pada instance Anda.

Linux

Bergantung pada distribusi Linux yang Anda gunakan, ketika Anda mencapai langkah untuk mengedit `chrony.conf` file, Anda akan menggunakan IPv6 titik akhir Amazon Time Sync Service (`fd00:ec2::123`) daripada IPv4 endpoint (`169.254.169.123`):

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Simpan file dan verifikasi bahwa chrony menggunakan `fd00:ec2::123` IPv6 titik akhir untuk menyinkronkan waktu:

```
[ec2-user ~]$ chronyc sources -v
```

Dalam output, jika Anda melihat `fd00:ec2::123` IPv6 titik akhir, konfigurasi selesai.

Windows

Saat Anda mencapai langkah untuk mengubah server NTP untuk menggunakan Layanan Sinkronisasi Waktu Amazon, Anda akan menggunakan IPv6 titik akhir Amazon Time Sync Service (`fd00:ec2::123`) daripada IPv4 endpoint (): `169.254.169.123`

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Verifikasi bahwa pengaturan baru Anda menggunakan `fd00:ec2::123` IPv6 titik akhir untuk menyinkronkan waktu:

```
w32tm /query /configuration
```

Dalam output, verifikasi yang `NtpServer` menampilkan `fd00:ec2::123` IPv6 titik akhir.

Terhubung ke jam perangkat keras PTP

Jam perangkat keras PTP adalah bagian dari AWS Sistem Nitro, sehingga dapat diakses langsung pada instans EC2 bare metal dan virtual yang didukung tanpa menggunakan sumber daya pelanggan apa pun.

Titik akhir NTP untuk jam perangkat keras PTP sama dengan yang ada pada Layanan Sinkronisasi Waktu Amazon biasa. Jika instans Anda memiliki jam perangkat keras PTP dan Anda mengonfigurasi koneksi NTP (ke IPv6 titik akhir IPv4 atau titik akhir), waktu instans Anda secara otomatis bersumber dari jam perangkat keras PTP melalui NTP.

Untuk instance Linux, Anda dapat mengonfigurasi koneksi PTP langsung, yang akan memberi Anda waktu yang lebih akurat daripada koneksi NTP. Instans Windows hanya mendukung koneksi NTP ke jam perangkat keras PTP.

Persyaratan

Jam perangkat keras PTP tersedia pada instans ketika persyaratan berikut terpenuhi:

- Didukung Wilayah AWS: AS Timur (Virginia N.), AS Timur (Ohio), Asia Pasifik (Malaysia), Asia Pasifik (Thailand), Asia Pasifik (Tokyo), dan Eropa (Stockholm)

- Local Zones yang Didukung: AS Timur (Kota New York)
- Keluarga instans yang didukung:
  - Tujuan umum: M7a, M7g, M7i
  - Memori dioptimalkan: R7a, R7g, R7i
  - Penyimpanan dioptimalkan: i8G, i8GE
- (Hanya Linux) driver ENA versi 2.10.0 atau yang lebih baru diinstal pada sistem operasi yang didukung. Untuk informasi selengkapnya tentang sistem operasi yang didukung, lihat prasyarat driver di. GitHub

(Hanya Linux) Konfigurasikan koneksi PTP langsung ke jam perangkat keras PTP

Bagian ini menjelaskan cara mengonfigurasi instance Linux Anda untuk menggunakan Layanan Sinkronisasi Waktu Amazon lokal melalui jam perangkat keras PTP menggunakan koneksi PTP langsung. Ini membutuhkan penambahan entri server untuk jam perangkat keras PTP dalam file `chrony` konfigurasi.

Untuk mengonfigurasi koneksi PTP langsung ke jam perangkat keras PTP (hanya instance Linux)

1. Instal prasyarat

   Connect ke instans Linux Anda dan lakukan hal berikut:

   a. Instal driver kernel Linux untuk Elastic Network Adapter (ENA) versi 2.10.0 atau yang lebih baru.

   b. Aktifkan jam perangkat keras PTP.

   Untuk petunjuk penginstalan, lihat Driver kernel Linux untuk keluarga Elastic Network Adapter (ENA) GitHub.
2. Verifikasi perangkat ENA PTP

   Verifikasi bahwa perangkat jam perangkat keras ENA PTP muncul di instans Anda.

   ```
   [ec2-user ~]$ for file in /sys/class/ptp/*; do echo -n "$file: "; cat "$file/
   clock_name"; done
   ```

   Output yang diharapkan

```
/sys/class/ptp/ptp<index>: ena-ptp-<PCI slot>
```

Di mana:

- *index*adalah indeks jam perangkat keras PTP yang terdaftar di kernel.
- *PCI slot*adalah slot PCI pengontrol ethernet ENA. Ini adalah slot yang sama seperti yang ditunjukkan pada`lspci | grep ENA`.

Contoh Output

```
/sys/class/ptp/ptp0: ena-ptp-05
```

Jika `ena-ptp-`*<PCI slot>* tidak ada dalam output, driver ENA tidak akan diinstal dengan benar. Tinjau langkah 1 dalam prosedur ini untuk menginstal driver.

3. Konfigurasikan symlink PTP

Perangkat PTP biasanya diberi nama`/dev/ptp0`,`/dev/ptp1`, dan seterusnya, dengan indeksnya tergantung pada urutan inisialisasi perangkat keras. Membuat symlink memastikan bahwa aplikasi seperti chrony secara konsisten mereferensikan perangkat yang benar, terlepas dari perubahan indeks.

Amazon Linux 2023 terbaru AMIs menyertakan `udev` aturan yang membuat `/dev/ptp_ena` symlink, menunjuk ke `/dev/ptp` entri yang benar terkait dengan host ENA.

Pertama periksa apakah symlink hadir dengan menjalankan perintah berikut.

```
[ec2-user ~]$ ls -l /dev/ptp*
```

Contoh Output

```
crw------- 1 root root 245, 0 Jan 31 2025 /dev/ptp0
lrwxrwxrwx 1 root root      4 Jan 31 2025 /dev/ptp_ena -> ptp0
```

Di mana:

- `/dev/ptp`*<index>*adalah jalur ke perangkat PTP.

- `/dev/ptp_ena`adalah symlink konstan, yang menunjuk ke perangkat PTP yang sama.

Jika `/dev/ptp_ena` symlink ada, lewati ke Langkah 4 dalam prosedur ini. Jika hilang, lakukan hal berikut:

a. Tambahkan `udev` aturan berikut.

```
[ec2-user ~]$ echo "SUBSYSTEM==\"ptp\", ATTR{clock_name}==\"ena-ptp-*\",
 SYMLINK += \"ptp_ena\"" | sudo tee -a /etc/udev/rules.d/53-ec2-network-
interfaces.rules
```

b. Muat ulang `udev` aturan, baik dengan me-reboot instance, atau dengan menjalankan perintah berikut.

```
[ec2-user ~]$ sudo udevadm control --reload-rules && udevadm trigger
```

4. Konfigurasikan chrony

chrony harus dikonfigurasi untuk menggunakan `/dev/ptp_ena` symlink alih-alih langsung mereferensikan/. `dev/ptp`*`<index>`*

a. Edit `/etc/chrony.conf` menggunakan editor teks dan tambahkan baris berikut di mana saja di file.

```
refclock PHC /dev/ptp_ena poll 0 delay 0.000010 prefer
```

b. Mulai ulang chrony.

```
[ec2-user ~]$ sudo systemctl restart chronyd
```

5. Verifikasi konfigurasi kronis

Verifikasi bahwa chrony menggunakan jam perangkat keras PTP untuk menyinkronkan waktu pada instans ini.

```
[ec2-user ~]$ chronyc sources
```

Output yang diharapkan

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
#* PHC0                          0   0    377    1   +2ns[ +1ns] +/-   5031ns
```

Dalam output yang dihasilkan, * menunjukkan sumber waktu pilihan. PHC0 sesuai dengan jam perangkat keras PTP. Anda mungkin perlu menunggu beberapa detik setelah memulai ulang kroni sebelum tanda bintang muncul.

Tetapkan referensi waktu pada instans EC2 Anda atau perangkat yang terhubung ke internet untuk menggunakan Layanan Sinkronisasi Waktu Amazon publik

Anda dapat mengatur instans Anda, atau perangkat apa pun yang terhubung ke internet seperti komputer lokal atau server on-premis, agar menggunakan Layanan Amazon Time Sync publik, yang dapat diakses melalui internet di `time.aws.com`. Anda dapat menggunakan Layanan Sinkronisasi Waktu Amazon publik sebagai cadangan untuk Layanan Sinkronisasi Waktu Amazon lokal dan untuk menghubungkan sumber daya di luar AWS ke Layanan Sinkronisasi Waktu Amazon.

> **Note**
>
> Untuk kinerja terbaik, sebaiknya gunakan Layanan Sinkronisasi Waktu Amazon lokal pada instans Anda, dan hanya menggunakan Layanan Sinkronisasi Waktu Amazon publik sebagai cadangan.

Gunakan instruksi untuk sistem operasi instans atau perangkat Anda.

Linux

Untuk mengatur instans atau perangkat Linux Anda agar menggunakan Layanan Amazon Time Sync publik menggunakan chrony atau ntpd

1. Edit `/etc/chrony.conf` (jika Anda menggunakan chrony) atau `/etc/ntp.conf` (jika Anda menggunakan ntpd) menggunakan editor teks sebagai berikut:

a. Untuk mencegah instans atau perangkat Anda mencoba mencampur server yang dioleskan dan yang tidak diolesi, hapus atau komentari baris yang dimulai `server` kecuali koneksi yang ada ke Layanan Sinkronisasi Waktu Amazon lokal.

> **Important**
>
> Jika Anda menyetel instans EC2 agar terhubung ke Layanan Amazon Time Sync publik, jangan hapus baris berikut yang menetapkan instans yang akan dihubungkan ke Layanan Amazon Time Sync. Layanan Amazon Time Sync lokal adalah koneksi yang lebih langsung dan akan memberikan akurasi jam yang lebih baik. Layanan Amazon Time Sync publik hanya boleh digunakan sebagai cadangan.
>
> ```
> server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
> ```

b. Tambahkan baris berikut untuk terhubung ke Layanan Amazon Time Sync publik.

```
pool time.aws.com iburst
```

2. Mulai ulang daemon menggunakan salah satu perintah berikut.

- chrony

```
sudo service chronyd force-reload
```

- ntpd

```
sudo service ntp reload
```

macOS

Untuk mengatur instans atau perangkat macOS Anda agar menggunakan Layanan Amazon Time Sync publik

1. Buka Preferensi Sistem.
2. Pilih Tanggal & Waktu, lalu pilih tab Tanggal & Waktu.
3. Untuk melakukan perubahan, pilih ikon kunci, dan masukkan kata sandi Anda saat diminta.
4. Untuk Atur tanggal dan waktu secara otomatis, masukkan **`time.aws.com`**.

Windows

Untuk mengatur instans atau perangkat Windows Anda agar menggunakan Layanan Amazon Time Sync publik

1. Buka Panel Kontrol.
2. Pilih ikon Tanggal dan Waktu.
3. Pilih tab Waktu Internet. Tab ini tidak tersedia jika PC Anda adalah bagian dari domain. Dalam hal ini, waktu akan disinkronkan dengan pengontrol domain. Anda dapat mengonfigurasi pengontrol untuk menggunakan Amazon Time Sync Service publik.
4. Pilih Ubah pengaturan.
5. Pilih kotak centang untuk Sinkronisasi dengan server waktu Internet.
6. Di sebelah Server, masukkan **`time.aws.com`**.

Untuk mengatur instans atau perangkat Windows Server Anda agar menggunakan Layanan Amazon Time Sync publik

- Ikuti Instruksi Microsoft untuk memperbarui registri Anda.

Bandingkan stempel waktu untuk instans Linux Anda

Jika Anda menggunakan Layanan Sinkronisasi Waktu Amazon, Anda dapat membandingkan stempel waktu pada instans ClockBound Amazon EC2 Linux untuk menentukan waktu sebenarnya dari suatu peristiwa. ClockBound mengukur akurasi jam instans EC2 Anda, dan memungkinkan Anda untuk memeriksa apakah stempel waktu yang diberikan ada di masa lalu atau masa depan sehubungan dengan jam instans Anda saat ini. Informasi ini berguna untuk menentukan urutan dan konsistensi peristiwa dan transaksi di seluruh instans EC2, terlepas dari lokasi geografis masing-masing instans.

ClockBound adalah daemon dan pustaka open source. Untuk mempelajari selengkapnya ClockBound, termasuk petunjuk penginstalan, lihat ClockBounddi GitHub.

ClockBound hanya didukung untuk instance Linux.

Jika Anda menggunakan koneksi PTP langsung ke jam perangkat keras PTP, daemon waktu Anda, seperti chrony, akan meremehkan batas kesalahan jam. Hal ini karena jam perangkat keras PTP tidak meneruskan informasi batas kesalahan yang benar ke chrony, seperti yang dilakukan NTP. Akibatnya, daemon sinkronisasi jam Anda mengasumsikan jam akurat hingga ke UTC dan

dengan demikian memiliki batas kesalahan `0`. Untuk mengukur batas kesalahan penuh, Sistem Nitro menghitung kesalahan terikat jam perangkat keras PTP, dan membuatnya tersedia untuk instans EC2 Anda melalui sistem file driver ENA. `sysfs` Anda dapat membaca ini secara langsung sebagai nilai, dalam nanodetik.

Untuk mengambil kesalahan jam perangkat keras PTP terikat

1. Pertama dapatkan lokasi yang benar dari perangkat jam perangkat keras PTP dengan menggunakan salah satu perintah berikut. Jalur dalam perintah berbeda tergantung pada AMI yang digunakan untuk meluncurkan instance.

   - Untuk Amazon Linux 2:

     ```
     cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
     ```

   - Untuk Amazon Linux 2023:

     ```
     cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
     ```

   Outputnya adalah nama slot PCI, yang merupakan lokasi perangkat jam perangkat keras PTP. Dalam contoh ini, lokasinya adalah`0000:00:03.0`.

   ```
   PCI_SLOT_NAME=0000:00:03.0
   ```

2. Untuk mengambil kesalahan jam perangkat keras PTP terikat, jalankan perintah berikut. Sertakan nama slot PCI dari langkah sebelumnya.

   ```
   cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
   ```

   Output-nya adalah batas kesalahan jam pada jam perangkat keras PTP, dalam nanodetik.

Untuk menghitung kesalahan jam yang benar yang terikat pada titik waktu tertentu saat menggunakan koneksi PTP langsung ke jam perangkat keras PTP, Anda harus menambahkan kesalahan jam yang terikat dari chrony atau ClockBound pada saat chrony polling jam perangkat keras PTP. Untuk informasi selengkapnya tentang mengukur dan memantau akurasi jam, lihat Mengelola akurasi jam instans Amazon EC2 menggunakan Layanan Sinkronisasi Waktu Amazon dan Amazon CloudWatch — Bagian 1.

Ubah zona waktu instans Anda

Instans Amazon EC2 disetel ke zona waktu UTC (Coordinated Universal Time) secara default. Anda dapat mengubah waktu pada sebuah instans ke zona waktu lokal atau ke zona waktu lain di jaringan Anda.

Gunakan instruksi untuk sistem operasi instans Anda.

Linux

> **Important**
>
> Informasi ini berlaku untuk Amazon Linux. Untuk informasi tentang distribusi lain, lihat dokumentasi spesifik tentangnya.

Untuk mengubah zona waktu di Amazon Linux

1. Lihat pengaturan zona waktu sistem saat ini.

   ```
   [ec2-user ~]$ timedatectl
   ```

2. Buat daftar zona waktu yang tersedia.

   ```
   [ec2-user ~]$ timedatectl list-timezones
   ```

3. Atur zona waktu yang dipilih.

   ```
   [ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
   ```

4. (Opsional) Konfirmasikan bahwa zona waktu saat ini diperbarui ke zona waktu baru dengan menjalankan perintah timedatectl lagi.

   ```
   [ec2-user ~]$ timedatectl
   ```

Windows

Untuk mengubah zona waktu pada instans Windows

1. Dari instans Anda, buka jendela Command Prompt.

2. Identifikasi zona waktu yang akan digunakan pada instans. Untuk mendapatkan daftar zona waktu, gunakan perintah berikut:

```
tzutil /l
```

   Perintah ini mengembalikan daftar semua zona waktu yang tersedia dalam format berikut:

```
display name
time zone ID
```

3. Temukan ID zona waktu untuk ditetapkan ke instans.
4. Contoh: Tetapkan zona waktu UTC:

```
tzutil /s "UTC"
```

   Contoh: Tetapkan Waktu Standar Pasifik:

```
tzutil /s "Pacific Standard Time"
```

Saat Anda mengubah zona waktu pada instans Windows, Anda harus memastikan bahwa zona waktu tidak berubah hingga sistem dimulai ulang. Jika tidak, saat dimulai ulang, instans akan kembali menggunakan waktu UTC. Anda dapat mempertahankan pengaturan zona waktu Anda dengan menambahkan kunci RealTimeIsUniversal registri. Kunci ini disetel secara default pada semua instans generasi saat ini. Untuk memverifikasi apakah kunci RealTimeIsUniversal registri diatur, lihat langkah 3 dalam prosedur berikut. Jika kuncinya belum diatur, ikuti langkah-langkah ini dari awal.

Untuk mengatur kunci RealTimeIsUniversal registri

1. Dari instans Anda, buka jendela Command Prompt.
2. Gunakan perintah berikut untuk menambahkan kunci registri:

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. (Opsional) Pastikan instans tersebut berhasil menyimpan kunci menggunakan perintah berikut:

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

Perintah ini mengembalikan subkunci untuk kunci registri TimeZoneInformation. Anda harus melihat kunci RealTimeIsUniversal di bagian bawah daftar, mirip dengan yang berikut ini:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xffffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B000100020000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

Manajer Kapasitas EC2

Amazon EC2 Capacity Manager membantu Anda memantau, menganalisis, dan mengelola penggunaan kapasitas di seluruh Instans Sesuai Permintaan, Instans Spot, dan Reservasi Kapasitas dari satu lokasi. Capacity Manager menyederhanakan pelacakan kapasitas melalui dasbor terpadu yang menggabungkan data penggunaan Anda dengan penyegaran setiap jam dan peluang pengoptimalan.

Dirancang untuk perusahaan besar dan organisasi multi-akun, Manajer Kapasitas menghilangkan pengumpulan data manual dari berbagai sumber. Alat ini memberikan wawasan mendalam di seluruh Anda Wilayah AWS. Anda dapat menelusuri metrik kapasitas terperinci dan mengambil tindakan segera untuk mengoptimalkan sumber daya cloud Anda.

Saat mengaktifkan integrasi AWS Organizations, Anda dapat melihat dan menganalisis data kapasitas di semua akun anggota di organisasi Anda dari satu dasbor. Tanpa integrasi Organizations, Capacity Manager hanya memantau sumber daya dalam individu Akun AWS di mana ia diaktifkan.

> **Note**
>
> - Anda hanya dapat mengaktifkan Manajer Kapasitas dalam satu AWS Region per akun.
> - Semua biaya yang ditampilkan di Manajer Kapasitas adalah perkiraan biaya berdasarkan harga Sesuai Permintaan yang dipublikasikan. Perkiraan ini tidak termasuk diskon seperti Savings Plans atau Instans Cadangan. Biaya aktual Anda mungkin berbeda dari perkiraan ini.

Fitur Utama

- Dasbor terpusat: Lihat penggunaan kapasitas di semua akun dan wilayah dengan titik data baru diperbarui setiap jam
- Visibilitas lintas akun: Tampilan tingkat organisasi untuk akun admin
- Ekspor data: Ekspor data kapasitas ke Amazon S3
- APIs: Akses terprogram ke metrik kapasitas dan data
- Analisis fleksibel: Pemilih tanggal dinamis untuk mengeksplorasi penggunaan kapasitas di periode waktu yang berbeda dari 90 hari terakhir
- Metrik dan dimensi komprehensif: Akses ke lebih dari 30 metrik di beberapa unit pengukuran (vCPUs, instans, perkiraan biaya) dengan kemampuan penyaringan ekstensif termasuk ID Akun, Wilayah, Keluarga Instance, Zona Ketersediaan, Jenis Instans, Platform, Penyewaan, dan dimensi khusus reservasi

Mengaktifkan Manajer Kapasitas EC2

Manajer Kapasitas dapat diaktifkan pada dua tingkat yang berbeda tergantung pada kebutuhan Anda. Anda dapat mengaktifkannya untuk satu orang Akun AWS untuk memantau sumber daya dalam akun itu saja, atau mengintegrasikannya dengan AWS Organizations untuk visibilitas terpusat di semua akun anggota di organisasi Anda.

- Tingkat organisasi: Melihat dan menganalisis data kapasitas di semua akun anggota di organisasi Anda dari satu dasbor.
- Tingkat akun: Pantau penggunaan kapasitas dalam satu. Akun AWS

Topik

- Mengaktifkan Manajer Kapasitas EC2 dengan Organizations AWS
- Mengaktifkan Manajer Kapasitas EC2 di tingkat akun
- Mendaftarkan administrator yang didelegasikan
- Menggunakan peran terkait layanan untuk Manajer Kapasitas EC2

Mengaktifkan Manajer Kapasitas EC2 dengan Organizations AWS

Anda dapat mengaktifkan EC2 Capacity Manager with AWS Organizations untuk visibilitas tingkat organisasi dan pengelolaan kapasitas Anda di semua akun anggota. Integrasi ini memungkinkan Anda untuk memantau, menganalisis, dan mengelola penggunaan kapasitas dari lokasi terpusat.

Akun manajemen bertanggung jawab untuk memungkinkan akses tingkat organisasi dan mengelola kapasitas di seluruh organisasi.

Mengaktifkan Manajer Kapasitas dengan AWS Organizations memberikan manfaat berikut:

- Visibilitas kapasitas terpusat — Lihat penggunaan kapasitas di semua akun anggota di organisasi Anda dari satu dasbor dengan agregasi lintas akun dan lintas wilayah.
- Optimalisasi seluruh organisasi — Identifikasi Reservasi Kapasitas yang tidak digunakan dan peluang pengoptimalan di semua akun di organisasi Anda.
- Administrator yang didelegasikan - Izinkan akun anggota tertentu untuk mengelola Manajer Kapasitas untuk organisasi sambil mempertahankan kontrol akses yang tepat.

Jika Anda tidak mengaktifkan integrasi dengan AWS Organizations, Anda hanya dapat memantau sumber daya di individu Akun AWS tempat Anda mengaktifkan Capacity Manager.

Prasyarat

- Anda harus memiliki pengaturan AWS Organizations dengan akun manajemen dan satu atau beberapa akun anggota. Untuk informasi selengkapnya tentang jenis akun, lihat Terminologi dan konsep di Panduan Pengguna AWS Organizations.
- Akun manajemen harus memiliki izin untuk tindakan IAM berikut:
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator`(jika menggunakan administrasi yang didelegasikan)
  - `iam:CreateServiceLinkedRole`

- Anda harus membuat peran terkait layanan dengan kasus AWSEC2CapacityManagerServiceRolePolicypenggunaan untuk mengizinkan akses AWS Organisasi. Untuk informasi selengkapnya, lihat Membuat peran terkait layanan untuk Manajer Kapasitas.

Mengaktifkan Manajer Kapasitas dengan Organizations AWS

Menggunakan akun manajemen, aktifkan akses organisasi di Manajer Kapasitas.

Console

Untuk mengaktifkan akses organisasi di Manajer Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Manajer Kapasitas.
3. Pilih tab Pengaturan.
4. Di bagian Akses tepercaya, pilih Kelola akses tepercaya.
5. Pada prompt yang muncul, pilih Aktifkan akses tepercaya. Lalu, pilih Simpan.

AWS CLI

Untuk mengaktifkan akses organisasi di Manajer Kapasitas

1. Buat peran tertaut layanan

```
aws iam create-service-linked-role --aws-service-name
 ec2.capacitymanager.amazonaws.com
```

2. Aktifkan akses AWS Organisasi

```
aws organizations enable-aws-service-access --service-principal
 ec2.capacitymanager.amazonaws.com
```

3. Aktifkan Manajer Kapasitas dengan AWS Organisasi

```
aws ec2 enable-capacity-manager --organizations-access
```

Untuk memperbarui akses organisasi untuk Manajer Kapasitas yang ada, jalankan perintah berikut:

```
aws ec2 update-capacity-manager-organizations-access --organizations-access
```

PowerShell

Untuk mengaktifkan akses organisasi di Manajer Kapasitas

1. Buat peran terkait layanan menggunakan cmdlet Baru. IAMService LinkedRole

```
New-IAMServiceLinkedRole -AWSServiceName "ec2.capacitymanager.amazonaws.com"
```

2. Aktifkan akses AWS Organisasi menggunakan cmdlet Aktifkan- ORGAWSService Akses.

```
Enable-ORGAWSServiceAccess -ServicePrincipal "ec2.capacitymanager.amazonaws.com"
```

3. Aktifkan Manajer Kapasitas dengan AWS Organisasi menggunakan Enable-EC2CapacityManagercmdlet.

```
Enable-EC2CapacityManager -OrganizationsAccess $true
```

Untuk memperbarui akses organisasi untuk Manajer Kapasitas yang ada, jalankan Update-EC2CapacityManagerOrganizationsAccesscmdlet berikut:

```
Update-EC2CapacityManagerOrganizationsAccess -OrganizationsAccess $true
```

Memverifikasi Manajer Kapasitas diaktifkan dengan organisasi Anda

Console

Untuk memverifikasi Manajer Kapasitas diaktifkan dengan organisasi Anda

1. Di konsol Manajer Kapasitas, pilih Pengaturan.
2. Di bagian Akses tepercaya, verifikasi bahwa akses Organisasi ditampilkan sebagai Diaktifkan.
3. Periksa apakah ID Organisasi menampilkan ID organisasi Anda.

AWS CLI

Untuk memverifikasi Manajer Kapasitas diaktifkan dengan organisasi Anda

Jalankan perintah berikut:

```
aws ec2 get-capacity-manager-attributes
```

Output harus menampilkan:

```
{
    "CapacityManagerStatus": "enabled",
    "OrganizationsAccess": true,
    "IngestionStatus": "initial-ingestion-pending",
    "IngestionStatusMessage": "Capacity Manager is collecting historical data from
 2025-10-01T00:00:00Z. Data collection is in progress and may take several hours to
 complete."
}
```

PowerShell

Untuk memverifikasi Manajer Kapasitas diaktifkan dengan organisasi Anda

Gunakan Get-EC2CapacityManagerAttributecmdlet.

```
Get-EC2CapacityManagerAttribute
```

Output harus menampilkan:

```
CapacityManagerStatus      : enabled
DataExportCount            : 0
EarliestDatapointTimestamp :
IngestionStatus            : initial-ingestion-in-progress
IngestionStatusMessage     : Capacity Manager is collecting historical data from
                             2026-03-17T16:00:00Z. Data collection is in progress
 and may take
                             several hours to complete.
LatestDatapointTimestamp   :
OrganizationsAccess        : True
```

Pertimbangan-pertimbangan

- Pembuatan peran terkait layanan: Saat Anda mengaktifkan akses organisasi melalui konsol, Manajer Kapasitas secara otomatis membuat peran AWSServiceRoleForEC2CapacityManager terkait layanan di semua akun m ember. Jika Anda mengaktifkan melalui AWS CLI, Anda harus menelepon `createServiceLinkedRole` secara manual.
- Agregasi data: Setelah mengaktifkan akses organisasi, Manajer Kapasitas mengisi kembali 14 hari data historis dari semua akun anggota. Proses ini biasanya memakan waktu beberapa menit untuk menyelesaikannya.
- Batasan regional: Anda hanya dapat mengaktifkan Manajer Kapasitas di satu Wilayah per organisasi, tetapi akan mengumpulkan data dari semua wilayah komersial.
- Izin: Akun anggota tidak perlu mengambil tindakan apa pun. Manajer Kapasitas menggunakan peran terkait layanan untuk secara otomatis menemukan sumber daya di semua akun.

Mengaktifkan Manajer Kapasitas EC2 di tingkat akun

Aktifkan Manajer Kapasitas di tingkat akun untuk memantau dan menganalisis penggunaan kapasitas EC2 Anda dalam satu akun. AWS Setelah Anda mengaktifkannya, Manajer Kapasitas mengumpulkan data tentang Instans Sesuai Permintaan, Instans Spot, dan Reservasi Kapasitas untuk membantu Anda mengidentifikasi peluang pengoptimalan dan melacak pola penggunaan.

Aktifkan Manajer Kapasitas di tingkat akun

Console

Untuk mengaktifkan Manajer Kapasitas untuk akun Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Manajer Kapasitas.
3. Pada halaman Manajer Kapasitas, pilih Aktifkan di Wilayah.

AWS CLI

Untuk mengaktifkan Manajer Kapasitas untuk akun Anda

Jalankan perintah berikut:

```
aws ec2 enable-capacity-manager
```

PowerShell

Untuk mengaktifkan Manajer Kapasitas untuk akun Anda

Gunakan Enable-EC2CapacityManagercmdlet.

```
Enable-EC2CapacityManager
```

Note

- Setelah Anda mengaktifkan Manajer Kapasitas, ia mengumpulkan dan mengumpulkan 14 hari data historis. Proses ini mungkin memakan waktu beberapa jam.
- Saat mengumpulkan data historis Anda, sebuah `initial-ingestion-in-progress` negara ditampilkan. Selama periode pengumpulan ini, Anda mungkin mengamati kesenjangan dalam data historis Anda. Ketika pengumpulan data selesai, sebuah `ingestion-complete` status ditampilkan.

Mendaftarkan administrator yang didelegasikan

Anda dapat mendaftarkan administrator yang didelegasikan untuk Manajer Kapasitas. Ini memungkinkan akun anggota untuk mengelola Manajer Kapasitas untuk AWS Organisasi Anda. Hanya akun manajemen yang dapat mendaftarkan atau menghapus administrator yang didelegasikan dalam organisasi Anda.

> **Note**
>
> Anda tidak dapat menonaktifkan Manajer Kapasitas untuk organisasi Anda saat ada administrator yang didelegasikan terdaftar.

Topik

- Prasyarat
- Mendaftarkan administrator yang didelegasikan
- Menghapus administrator yang didelegasikan

Prasyarat

Akun manajemen Anda harus mengaktifkan Capacity Manager with AWS Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan Manajer Kapasitas EC2 dengan Organizations AWS.

Mendaftarkan administrator yang didelegasikan

Anda dapat mendaftarkan administrator yang didelegasikan menggunakan konsol Amazon EC2, atau AWS CLI. PowerShell

Console

Untuk mendaftarkan administrator yang didelegasikan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Manajer Kapasitas.
3. Pilih tab Pengaturan.
4. Di bagian Administrator yang didelegasikan, pilih Tambah.
5. Pada prompt yang muncul, masukkan ID akun anggota organisasi yang ingin Anda tambahkan sebagai administrator yang didelegasikan.

6. Pilih Tambahkan administrator yang didelegasikan.

AWS CLI

Untuk mendaftarkan administrator yang didelegasikan

Jalankan perintah berikut:

```
aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal ec2.capacitymanager.amazonaws.com
```

PowerShell

Untuk mendaftarkan administrator yang didelegasikan

Gunakan cmdlet Register- ORGDelegated Administrator.

```
Register-ORGDelegatedAdministrator `
    -AccountId "123456789012" `
    -ServicePrincipal "ec2.capacitymanager.amazonaws.com"
```

Menghapus administrator yang didelegasikan

Anda dapat menghapus administrator yang didelegasikan menggunakan konsol Amazon EC2, atau AWS CLI. PowerShell

Console

Untuk menghapus administrator yang didelegasikan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Manajer Kapasitas.
3. Pilih tab Pengaturan.
4. Di bagian Administrator yang didelegasikan, pilih Kelola.
5. Pada prompt yang muncul, pilih Hapus administrator yang didelegasikan.

AWS CLI

Untuk menghapus administrator yang didelegasikan

Jalankan perintah berikut:

```
aws organizations deregister-delegated-administrator \
    --account-id 123456789012 \
    --service-principal ec2.capacitymanager.amazonaws.com
```

PowerShell

Untuk menghapus administrator yang didelegasikan

Gunakan cmdlet Unregister- ORGDelegated Administrator.

```
Unregister-ORGDelegatedAdministrator `
    -AccountId "123456789012" `
    -ServicePrincipal "ec2.capacitymanager.amazonaws.com"
```

Menggunakan peran terkait layanan untuk Manajer Kapasitas EC2

Manajer Kapasitas EC2 menggunakan peran AWS Identity and Access Management terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke Manajer Kapasitas. Peran terkait layanan telah ditentukan sebelumnya oleh Manajer Kapasitas dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Manajer Kapasitas lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Manajer Kapasitas mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Manajer Kapasitas yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Manajer Kapasitas karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran

terkait layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Manajer Kapasitas

Capacity Manager menggunakan peran terkait layanan yang diberi nama AWSServiceRoleForEC2CapacityManageruntuk memungkinkan Anda mengelola sumber daya kapasitas dan berintegrasi dengan AWS Organizations atas nama Anda.

Peran AWSService RoleFor EC2 CapacityManager terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `ec2.capacitymanager.amazonaws.com`

Kebijakan izin peran bernama AWSEC2 CapacityManagerServiceRolePolicy memungkinkan Manajer Kapasitas menyelesaikan tindakan berikut:

- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListChildren`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

Anda harus mengonfigurasi izin agar pengguna, grup, atau peran Anda membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Manajer Kapasitas

Anda dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan. AWSEC2CapacityManagerServiceRolePolicy Di AWS CLI atau AWS API, buat peran terkait layanan dengan nama `ec2.capacitymanager.amazonaws.com` layanan. Untuk informasi selengkapnya, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait layanan untuk Manajer Kapasitas

Manajer Kapasitas tidak mengizinkan Anda mengedit peran AWSService RoleFor EC2 CapacityManager terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Manajer Kapasitas

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran terkait layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Manajer Kapasitas menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya Manajer Kapasitas yang digunakan oleh AWSService RoleFor EC2 CapacityManager

1. Semua administrator yang didelegasikan harus menonaktifkan Manajer Kapasitas mereka sebelum menghapus akses organisasi.
2. Anda harus menghapus ekspor data aktif sebelum menonaktifkan manajer kapasitas.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSService RoleFor EC2 CapacityManager terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran terkait layanan Manajer Kapasitas

Manajer Kapasitas mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat AWS Wilayah dan titik akhir.

Manajer Kapasitas tidak mendukung penggunaan peran terkait layanan di setiap Wilayah tempat layanan tersedia. Anda dapat menggunakan AWSService RoleFor EC2 CapacityManager peran di Wilayah berikut.

Nama wilayah	Identitas wilayah	Support di Capacity Manager
US East (Northern Virginia)	us-east-1	Ya
US East (Ohio)	us-east-2	Ya
US West (N. California)	us-west-1	Ya
US West (Oregon)	us-west-2	Ya
Africa (Cape Town)	af-south-1	Tidak
Asia Pasifik (Hong Kong)	ap-east-1	Tidak
Asia Pasifik (Jakarta)	ap-southeast-3	Tidak
Asia Pasifik (Mumbai)	ap-south-1	Ya
Asia Pacific (Osaka)	ap-northeast-3	Ya
Asia Pacific (Seoul)	ap-northeast-2	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Ya
Canada (Central)	ca-sentral-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Ya

Nama wilayah	Identitas wilayah	Support di Capacity Manager
Europe (Milan)	eu-south-1	Tidak
Eropa (Paris)	eu-west-3	Ya
Eropa (Stockholm)	eu-north-1	Ya
Timur Tengah (Bahrain)	me-south-1	Tidak
Timur Tengah (UAE)	me-central-1	Tidak
Amerika Selatan (Sao Paulo)	sa-east-1	Ya
AWS GovCloud (AS-Timur)	us-gov-east-1	Tidak
AWS GovCloud (AS-Barat)	us-gov-west-1	Tidak

Mengatur data Anda di Manajer Kapasitas

Manajer Kapasitas menggunakan kombinasi metrik, titik data, dimensi, rentang tanggal, dan periode untuk mengatur data kapasitas Anda. Ini dapat membantu Anda menganalisis pola penggunaan dan membuat keputusan berdasarkan informasi tentang sumber daya Anda.

Metrik dan titik data

Metrik adalah kumpulan titik data yang diurutkan waktu. Misalnya, jika Anda ingin memantau penggunaan Spot Anda di vCPUs, Anda akan menggunakan `SpotTotalUsageHrsVcpu` metrik.

Setiap jam, metrik menghasilkan titik data stempel waktu dengan penggunaan Spot dalam jam vCPU. Misalnya, jika Anda menggunakan 100 v CPUs selama jam 10:00 AM, Manajer Kapasitas membuat titik data dengan stempel waktu 10:00 AM dan nilai 100.

Untuk daftar lengkap metrik yang dianalisis oleh Manajer Kapasitas, lihat. Metrik Manajer Kapasitas EC2

Dimensi

Dimensi adalah pasangan nama-nilai yang membantu Anda mengkategorikan dan mengidentifikasi berbagai aspek metrik. Misalnya, nama satu dimensi di Capacity Manager adalah AccountID, di

mana nilainya adalah ID akun yang sebenarnya. Capacity Manager menyediakan dimensi untuk mengelompokkan dan mengelompokkan data Anda seperti Instance Family, Reservation ARN, Reservation type, dan Tenancy.

Untuk daftar lengkap dimensi, lihatMetrik Manajer Kapasitas EC2.

Rentang tanggal dan periode

Rentang tanggal menentukan berapa banyak waktu yang ingin Anda analisis, dari satu jam hingga 90 hari. Periode menentukan bagaimana Manajer Kapasitas mengumpulkan data Anda sepanjang waktu dan berapa banyak titik data yang akan dikembalikan. Misalnya, jika rentang tanggal Anda adalah satu minggu dan periode Anda adalah 1 hari, Manajer Kapasitas mengembalikan 7 poin data. Setiap titik data mewakili satu hari data agregat. Periode harus interval satu jam dan dibagi secara merata ke dalam rentang tanggal.

Topik

- Metrik Manajer Kapasitas EC2
- Pengelompokan dan penyaringan data

Metrik Manajer Kapasitas EC2

Capacity Manager menawarkan pilihan metrik yang komprehensif untuk melacak kapasitas Anda di berbagai jenis sumber daya. Metrik dapat diukur menggunakan unit yang berbeda tergantung pada kebutuhan analisis Anda.

Nama metrik di Manajer Kapasitas menggunakan empat awalan berbeda untuk mengkategorikan jenis kapasitas yang diukur:

- `Reservation`— Reservasi Kapasitas itu sendiri, termasuk total kapasitas cadangan, tarif pemanfaatan, kapasitas yang tidak terpakai, dan jumlah reservasi.
- `Reserved`— Penggunaan Instans Sesuai Permintaan yang ditanggung oleh Reservasi Kapasitas Anda.
- `Unreserved`— Penggunaan Instans Sesuai Permintaan yang berjalan di luar Reservasi Kapasitas apa pun.
- `Spot`— Khusus untuk penggunaan Instans Spot, termasuk runtime dan perkiraan biaya. Metrik ini terpisah dari kapasitas berbasis reservasi.

Tabel berikut juga menyediakan Dimensi yang tersedia untuk setiap metrik. Kategori dimensi dipecah sebagai berikut:

- Dimensi kapasitas umum — ID Akun, Wilayah, Keluarga Instans, Zona Ketersediaan, Jenis Instans, Platform, dan Penyewaan
- Dimensi Reservasi Kapasitas — ID Reservasi (ID Reservasi Kapasitas), ARN Reservasi, Pemilik Keuangan yang Tidak Digunakan, Jenis Reservasi (ODCR/Blok Kapasitas), Buat stempel waktu, Start timestamp, End timestamp, Status, dan kriteria pencocokan Instance.
- Dimensi penggunaan yang dicadangkan — ID Reservasi (CRID), ARN Reservasi, Jenis reservasi

Metrik	Deskripsi	Dimensi tersedia	Unit tersedia
`ReservationAvgCommittedSize`	Jumlah total rata-rata kapasitas dalam keadaan aktif atau terjadwal dengan komitmen. Ukurannya dijumlahkan di seluruh dimensi dan dirata-ra takan dari waktu ke waktu.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
`ReservationAvgFutureSize`	Jumlah rata-rata Reservasi Kapasitas yang dijadwalkan akan dimulai di masa depan tetapi belum aktif selama periode yang dipilih. Ukurannya dijumlahkan di seluruh dimensi dan dirata-ratakan dari waktu ke waktu.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
`ReservationAvgUtilization`	Persentase rata-rata kapasitas cadangan Anda yang digunakan selama periode yang dipilih.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
`ReservationMaxCommittedSize`	Kapasitas total maksimum dalam keadaan aktif atau terjadwal dengan komitmen. Ukuran dijumlahkan di seluruh	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh

Metrik	Deskripsi	Dimensi tersedia	Unit tersedia
	dimensi dan nilai maksimum diambil untuk periode tersebut.		
ReservationMaxFutureSize	Jumlah maksimum Reservasi Kapasitas yang dijadwalkan akan dimulai di masa depan tetapi belum aktif selama periode yang dipilih. Ukuran dijumlahkan di seluruh dimensi dan nilai maksimum diambil untuk periode tersebut.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
ReservationMaxSize	Ukuran maksimum yang dicapai Reservasi Kapasitas Anda kapan saja selama periode yang dipilih. ID Reservasi Diperlukan.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
ReservationMaxUnusedSize	Jumlah maksimum kapasitas yang tidak terpakai dalam Reservasi Kapasitas Anda kapan saja selama periode yang dipilih. ID Reservasi Diperlukan.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
ReservationMaxUtilization	Persentase pemanfaatan maksimum yang dicapai Reservasi Kapasitas Anda kapan saja selama periode yang dipilih. ID Reservasi Diperlukan.	Kapasitas umum dan dimensi Reservasi Kapasitas	
ReservationMinCommittedSize	Jumlah total minimum kapasitas dalam keadaan aktif atau terjadwal dengan komitmen. Ukuran dijumlahkan di seluruh dimensi dan nilai minimum diambil untuk periode tersebut.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh

Metrik	Deskripsi	Dimensi tersedia	Unit tersedia
`ReservationMinFutureSize`	Jumlah minimum Reservasi Kapasitas yang dijadwalkan akan dimulai di masa depan tetapi belum aktif pada titik mana pun selama periode yang dipilih. Ukuran dijumlahkan di seluruh dimensi dan nilai minimum diambil untuk periode tersebut.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
`ReservationMinSize`	Ukuran minimum yang dicapai Reservasi Kapasitas Anda kapan saja selama periode yang dipilih. ID Reservasi Diperlukan.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
`ReservationMinUnusedSize`	Jumlah minimum kapasitas yang tidak terpakai dalam Reservasi Kapasitas Anda kapan saja selama periode yang dipilih. ID Reservasi Diperlukan.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
`ReservationMinUtilization`	Persentase pemanfaatan minimum yang dicapai Reservasi Kapasitas Anda kapan saja selama periode yang dipilih. ID Reservasi Diperlukan.	Kapasitas umum dan dimensi Reservasi Kapasitas	
`ReservationTotalCapacityHrs`	Jumlah total kapasitas yang telah Anda pesan melalui Reservasi Kapasitas selama periode yang dipilih.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
`ReservationTotalCount`	Jumlah total Reservasi Kapasitas berbeda yang Anda miliki selama periode yang dipilih.	Kapasitas umum dan dimensi Reservasi Kapasitas	

Metrik	Deskripsi	Dimensi tersedia	Unit tersedia
`ReservationTotalEstimatedCost`	Perkiraan biaya total jam kapasitas yang dipesan selama periode yang dipilih.	Kapasitas umum dan dimensi Reservasi Kapasitas	
`ReservationUnusedTotalCapacityHrs`	Jumlah total kapasitas cadangan yang Anda miliki tetapi tidak digunakan selama periode yang dipilih.	Kapasitas umum dan dimensi Reservasi Kapasitas	vCPU, Contoh
`ReservationUnusedTotalEstimatedCost`	Perkiraan biaya kapasitas cadangan yang Anda miliki tetapi tidak digunakan selama periode yang dipilih (dihitung menggunakan tarif Sesuai Permintaan).	Kapasitas umum dan dimensi Reservasi Kapasitas	
`ReservedTotalEstimatedCost`	Perkiraan biaya penggunaan Instans Sesuai Permintaan yang ditanggung oleh Reservasi Kapasitas selama periode yang dipilih. Ini tidak termasuk penggunaan Spot.	Kapasitas umum dan dimensi penggunaan Cadangan	
`ReservedTotalUsageHrs`	Total jam penggunaan Instans Sesuai Permintaan yang dicakup oleh Reservasi Kapasitas selama periode yang dipilih. Ini tidak termasuk penggunaan Spot.	Kapasitas umum dan dimensi penggunaan Cadangan	vCPU, Contoh
`SpotAvgRunTimeBeforeInterruption`	Runtime rata-rata dalam jam untuk instance yang terputus dalam periode yang dipilih.	Dimensi wilayah, AZ, dan ID Akun saja	Instans

Metrik	Deskripsi	Dimensi tersedia	Unit tersedia
SpotInterruptionRate	Persentase Instans Spot yang berjalan yang terputus pada periode yang dipilih.	Dimensi wilayah, AZ, dan ID Akun saja	vCPU, Contoh
SpotMaxRunTimeBeforeInterruption	Runtime maksimum dalam jam untuk instance yang terputus dalam periode yang dipilih.	Dimensi wilayah, AZ, dan ID Akun saja	Instans
SpotMinRunTimeBeforeInterruption	Runtime minimum dalam jam untuk instance yang terputus dalam periode yang dipilih.	Dimensi wilayah, AZ, dan ID Akun saja	Instans
SpotTotalCount	Jumlah Instans Spot atau v CPUs yang berjalan selama periode yang dipilih.	Dimensi wilayah, AZ, dan ID Akun saja	vCPU, Contoh
SpotTotalEstimatedCost	Perkiraan biaya penggunaan Instans Spot selama periode yang dipilih (dihitung menggunakan tarif Spot yang dipublikasikan).	Dimensi kapasitas umum	
SpotTotalInterruptions	Jumlah Instans Spot yang terputus atau v CPUs selama periode yang dipilih.	Dimensi wilayah, AZ, dan ID Akun saja	vCPU, Contoh
SpotTotalUsageHrs	Total jam penggunaan Instans Spot selama periode yang dipilih.	Dimensi kapasitas umum	vCPU, Contoh
UnreservedTotalEstimatedCost	Perkiraan biaya penggunaan Instans Sesuai Permintaan yang tidak ditanggung oleh Reservasi Kapasitas selama periode yang dipilih. Ini tidak termasuk penggunaan Spot.	Dimensi kapasitas umum	

Metrik	Deskripsi	Dimensi tersedia	Unit tersedia
`UnreservedTotalUsageHrs`	Total jam penggunaan Instans Sesuai Permintaan yang tidak tercakup dalam Reservasi Kapasitas selama periode yang dipilih. Ini tidak termasuk penggunaan Spot.	Dimensi kapasitas umum	vCPU, Contoh

> **Note**
>
> Jika Anda menyertakan instance dalam unit Anda, sebaiknya sertakan jenis instans dalam dimensi Anda.

Pengelompokan dan penyaringan data

Manajer Kapasitas menggabungkan metrik Anda berdasarkan dimensi dan periode tanggal yang Anda pilih. Jika tidak ada dimensi yang dipilih, Manajer Kapasitas mengumpulkan data dan mengembalikan satu titik data per periode dalam rentang tanggal. Anda dapat mengelompokkan data Anda ke dalam agregasi yang lebih kecil dengan menambahkan dimensi.

- Pengelompokan — Memecah data kapasitas Anda berdasarkan dimensi seperti Wilayah, Keluarga Instance, atau ID Akun. Anda dapat mengelompokkan metrik berdasarkan beberapa dimensi untuk memecah data lebih lanjut. Misalnya, jika Anda mengelompokkan berdasarkan Wilayah dan Zona Ketersediaan, Anda mendapatkan titik data untuk setiap kombinasi Wilayah dan AZ tempat Anda menggunakan.
- Filtering - Tampilkan hanya subset tertentu dari dimensi yang Anda pilih. Misalnya, jika Anda mengelompokkan berdasarkan keluarga instans, Anda akan mendapatkan titik data untuk semua keluarga yang Anda gunakan. Namun, jika Anda juga memfilter berdasarkan p5, Anda hanya melihat titik data untuk keluarga instance p5.
- Satuan metrik — Lihat hasil berdasarkan unit yang berbeda seperti vCPUs, instans, atau perkiraan biaya. Misalnya, setelah mengelompokkan berdasarkan Wilayah dan memfilter berdasarkan keluarga instance tertentu, Anda dapat melihat data dengan cara yang berbeda. Beralih antara total v yang CPUs digunakan, jumlah instance yang berjalan, atau perkiraan biaya.

Cara mengelompokkan dan memfilter data di konsol

Untuk mengelompokkan dan memfilter data di Manajer Kapasitas

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Manajer Kapasitas.
3. Pilih tab untuk jenis sumber daya yang ingin Anda analisis: Penggunaan, Reservasi, atau Spot.
4. Di bagian Filter tanggal, pilih Rentang tanggal, Zona waktu, dan Interval.
5. Di bagian filter Dimensi, pilih dimensi dari menu tarik-turun Pilih dimensi.
6. Pilih dimensi yang ingin Anda kelompokkan dari dropdown. Perhatikan bahwa opsi dimensi berbeda untuk setiap jenis sumber daya. Untuk informasi selengkapnya, lihat Metrik Manajer Kapasitas EC2.

   Anda dapat menambahkan beberapa dimensi untuk membuat pengelompokan yang lebih terperinci.
7. Untuk memfilter berdasarkan dimensi yang Anda pilih, pilih opsi filter dari dropdown Filter menurut dimensi.
8. Di bagian Agregasi, pilih unit untuk melihat hasil menurut vCPUs, Instans, atau Perkiraan biaya.

Menavigasi Manajer Kapasitas di konsol AWS

Konsol Manajer Kapasitas diatur ke dalam tab yang memberikan tampilan berbeda dari data kapasitas Anda:

- Dasbor - Memberikan ikhtisar tingkat tinggi dari semua Reservasi Kapasitas Sesuai Permintaan, Sesuai Permintaan, dan penggunaan Spot, termasuk metrik utama dan peringatan teratas untuk membantu meningkatkan postur kapasitas Anda.
- Penggunaan — Memberikan gambaran umum tentang pola penggunaan instans Anda untuk instans On-Demand dan Spot. Analisis cakupan berdasarkan Reservasi Kapasitas dan identifikasi peluang pengoptimalan melalui pengelompokan dan penyaringan yang fleksibel.
- Reservasi — Menyediakan analisis pemanfaatan Reservasi Kapasitas, kemampuan manajemen, dan metrik reservasi terperinci di seluruh akun dan Wilayah.
- Spot — Memantau pola penggunaan Spot dan menyediakan analisis biaya untuk instans Spot di seluruh akun dan Wilayah.

- Ekspor data — Mengelola konfigurasi ekspor data ke Amazon S3, termasuk penjadwalan, pemformatan, dan pemilihan templat.
- Pengaturan - Menyediakan opsi konfigurasi layanan termasuk akses organisasi dan pengaturan regional.

Dalam tab Penggunaan dan Pemesanan, Manajer Kapasitas menyediakan struktur navigasi hierarkis yang memungkinkan Anda menelusuri dari ikhtisar tingkat tinggi hingga informasi sumber daya terperinci. Memahami pola navigasi ini membantu Anda menganalisis data kapasitas Anda secara efisien dan mengidentifikasi peluang pengoptimalan.

Topik

- Hirarki navigasi
- Lihat rincian dan rincian untuk Penggunaan dan Reservasi

Hirarki navigasi

Capacity Manager menggunakan struktur navigasi tiga tingkat untuk Penggunaan dan Reservasi:

1. Halaman ikhtisar — Ringkasan tingkat tinggi dengan metrik agregat.
2. Halaman rincian - Analisis rinci dengan pilihan penyaringan dan pengelompokan
3. Halaman detail:
   - Detail penggunaan — Informasi tentang kombinasi dimensi yang Anda pilih, yang menyediakan statistik dan data deret waktu untuk membantu Anda memahami pola penggunaan.
   - Detail reservasi — Informasi tentang Reservasi Kapasitas tertentu termasuk statistik pemanfaatan, pola penggunaan dari waktu ke waktu, dan detail konfigurasi.

> **Note**
>
> Spot mengikuti struktur yang disederhanakan dengan hanya halaman ikhtisar.

Lihat rincian dan rincian untuk Penggunaan dan Reservasi

Tab Penggunaan dan Pemesanan mengikuti struktur navigasi tiga tingkat yang sama, memungkinkan Anda untuk maju dari ikhtisar ke rincian ke halaman detail. Proses untuk mengakses halaman rincian dan rincian serupa, dengan hanya perbedaan kecil di mana link navigasi berada dalam setiap tab.

Untuk mengakses halaman rincian sumber daya

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Manajer Kapasitas.
3. Pilih tab untuk jenis sumber daya yang ingin Anda analisis: Penggunaan atau Reservasi.
4. Di bagian Agregasi, cari tautan rincian:
   - Penggunaan: Di kolom Tindakan, pilih Lihat rincian.

     > **Note**
     >
     > Bergantung pada ukuran layar Anda atau jumlah dimensi yang telah Anda terapkan, Anda mungkin perlu menggulir secara horizontal di seluruh halaman untuk menemukan tautan rincian Tampilan.

   - Reservasi: Di kolom Reservasi, pilih nomor (nomornya adalah tautan) dari reservasi yang ingin Anda lihat.

Untuk mengakses halaman detail

1. Pada halaman rincian, navigasikan ke bagian yang relevan:
   - Penggunaan: Bagian kombinasi dimensi Unik.
   - Reservasi: Bagian Reservasi.
2. Di bagian yang relevan dari sumber daya yang Anda pilih, akses halaman detail.
   - Penggunaan: Di kolom Tindakan, pilih Lihat detail.

> **Note**
>
> Bergantung pada ukuran layar Anda atau jumlah dimensi yang telah Anda terapkan, Anda mungkin perlu menggulir secara horizontal di seluruh halaman untuk menemukan tautan Lihat detail.

- Reservasi: Di kolom ID Reservasi, pilih reservasi yang ingin Anda lihat.

Mengekspor data Manajer Kapasitas Anda

Anda dapat mengekspor data kapasitas dari EC2 Capacity Manager ke Amazon S3 untuk mengaktifkan analisis lebih lanjut, membuat laporan kustom, atau mengintegrasikan dengan AWS layanan lain. Anda dapat mengekspor data Anda dalam format CSV atau Parket. Di bagian berikut, Anda akan menemukan informasi tentang cara mengekspor data Manajer Kapasitas Anda.

> **Note**
>
> Manajer Kapasitas hanya mengizinkan satu ekspor data per Akun AWS.

Topik

- Menyiapkan bucket Amazon S3 untuk ekspor data Capacity Manager
- Membuat ekspor data untuk data Manajer Kapasitas Anda

Menyiapkan bucket Amazon S3 untuk ekspor data Capacity Manager

Untuk menerima ekspor data Manajer Kapasitas, Anda harus memiliki bucket Amazon S3 untuk menerima dan menyimpan file ekspor Anda. Akun AWS Saat membuat ekspor data di konsol Capacity Manager, Anda dapat memilih bucket Amazon S3 yang sudah ada yang Anda miliki atau membuat bucket baru.

Dalam kedua kasus tersebut, Anda harus menerapkan kebijakan bucket yang diperlukan untuk memungkinkan Manajer Kapasitas mengirimkan file ekspor. Mengedit kebijakan ini di konsol Amazon S3 atau mengubah pemilik bucket setelah Anda membuat ekspor data akan mencegah Manajer Kapasitas mengirimkan ekspor Anda.

Untuk membuat bucket Amazon S3, lihat Membuat bucket S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Kebijakan berikut harus diterapkan pada bucket S3 Anda untuk memungkinkan Manajer Kapasitas mengirimkan ekspor data:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.capacitymanager.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:capacity-
manager-data-export/*"
                }
            }
        }
    ]
}
```

Kebijakan bucket ini membantu memastikan bahwa file ekspor data Capacity Manager dapat dikirimkan dengan aman ke bucket Anda. Secara khusus:

- Setiap kali ekspor data Manajer Kapasitas dikirimkan, AWS pertama-tama konfirmasikan apakah bucket tersebut masih dimiliki oleh akun yang mengatur ekspor. Jika kepemilikan bucket telah

berubah, ekspor tidak akan dikirimkan. Ini membantu memastikan keamanan data Manajer Kapasitas. Kebijakan bucket ini memungkinkan AWS (`"Effect": "Allow"`) untuk memeriksa akun mana yang memiliki bucket (`"Action": ["s3:ListBucket"]`).

- Kebijakan ini memberikan izin kepada Capacity Manager service (`"Service": "ec2.capacitymanager.amazonaws.com"`) untuk menulis export files (`"Action": "s3:PutObject"`) dan read objects (`"Action": "s3:GetObject"`) untuk menyalin data ke bucket Anda.

Membuat ekspor data untuk data Manajer Kapasitas Anda

Untuk membuat ekspor data, Anda dapat menggunakan halaman Ekspor Data di konsol Manajer Kapasitas AWS CLI atau.

Prasyarat

Anda harus membuat bucket Amazon Simple Storage Service (Amazon S3). Anda harus memastikan hal-hal berikut:

- Bucket S3 Anda harus sama dengan AWS Region tempat Anda mengaktifkan Capacity Manager.
- Bucket S3 Anda memiliki kebijakan izin yang diperlukan untuk layanan Capacity Manager untuk mengirimkan file.

Untuk informasi selengkapnya, lihat Menyiapkan bucket Amazon S3 untuk ekspor data Capacity Manager.

Prosedur

Anda dapat mengekspor data Pengelola Kapasitas menggunakan AWS Konsol, Konsol AWS CLI, atau PowerShell.

Console

Untuk membuat ekspor data

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Manajer Kapasitas.
3. Pilih tab Ekspor data.
4. Pilih Buat ekspor data.

5. Konfigurasikan properti ekspor, lokasi pengiriman, dan tag Anda (opsional).
6. Pilih Buat.

AWS CLI

Untuk membuat ekspor data

Gunakan perintah berikut untuk membuat ekspor data dengan konfigurasi yang ditentukan:

```
aws ec2 create-capacity-manager-data-export \
    --s3-bucket-name my-exports-bucket \
    --s3-bucket-prefix capacity-data-exports \
    --schedule hourly \
    --output-format parquet/CSV \
    --tag-specifications 'ResourceType=capacity-manager-data-
export,Tags=[{Key=environment,Value=production}]'
```

PowerShell

Untuk membuat ekspor data

Gunakan New-EC2CapacityManagerDataExportcmdlet.

```
New-EC2CapacityManagerDataExport `
    -S3BucketName "my-exports-bucket" `
    -S3BucketPrefix "capacity-data-exports" `
    -Schedule "hourly" `
    -OutputFormat "parquet" `
    -TagSpecification @([Amazon.EC2.Model.TagSpecification]@{
        ResourceType = "capacity-manager-data-export"
        Tags = @([Amazon.EC2.Model.Tag]@{
            Key   = "environment"
            Value = "production"
        })
    })
```

Mengelola driver perangkat untuk instans EC2 Anda

Driver perangkat adalah komponen perangkat lunak yang berkomunikasi dengan perangkat keras virtual untuk instans Amazon EC2 Anda. Untuk mencegah kesalahan sistem, masalah kinerja, dan perilaku tak terduga lainnya, penting untuk menjaga driver Anda up-to-date. Itu terutama berlaku untuk driver yang dapat memiliki dampak kuat pada kinerja sistem tergantung pada penggunaan Anda, seperti jaringan, grafik, dan driver perangkat penyimpanan. Rilis driver baru dapat menyertakan perbaikan cacat atau memperkenalkan fungsionalitas yang diperluas yang mungkin ingin Anda manfaatkan untuk instance yang sedang berjalan.

Driver jaringan

Distribusi Linux dapat menggabungkan fitur jaringan seperti Elastic Network Adapter (ENA) atau Elastic Fabric Adapter (EFA) dalam kernel. Namun, waktunya dapat bervariasi untuk implementasi fitur driver kernel dalam distribusi yang berbeda.

Driver kernel ENA dan EFA Linux tersedia dari GitHub repositori Amazon Drivers. Untuk informasi selengkapnya dan tautan ke driver yang tersedia, lihat Driver Amazon di GitHub.

Untuk informasi lebih lanjut tentang driver ENA, lihatAktifkan jaringan yang disempurnakan dengan ENA pada instans EC2 Anda. Untuk informasi selengkapnya tentang driver EFA, lihat Memulai topik di Adaptor Kain Elastis untuk AI/ML dan beban kerja HPC di Amazon EC2 bagian panduan ini.

Untuk menginstal atau memperbarui driver jaringan pada instance Windows, lihat topik berikut:

- Instal driver ENA di Windows
- Instal driver AWS PV terbaru

  Untuk informasi selengkapnya, lihat Driver paravirtual untuk instans Windows.

> **Note**
>
> EFA tidak didukung pada instance Windows.

Driver grafis

Untuk menginstal atau memperbarui driver grafis, lihat topik berikut:

- Driver AMD untuk instans EC2 Anda
- Driver NVIDIA untuk instans Amazon EC2 Anda

Driver perangkat penyimpanan

Untuk menginstal atau memperbarui driver penyimpanan, lihat topik berikut:

- Untuk instance Linux, lihat Menginstal atau memutakhirkan NVMe driver di Panduan Pengguna Amazon EBS.
- Untuk instance Windows, lihatAWS NVMe driver.

Driver AMD untuk instans EC2 Anda

Instans dengan GPU AMD terlampir, seperti instans G4ad, harus menginstal driver AMD yang sesuai. Tergantung pada kebutuhan Anda, Anda dapat menggunakan AMI dengan driver yang telah diinstal terlebih dahulu atau mengunduh driver dari Amazon S3.

Untuk menginstal driver NVIDIA pada instans dengan GPU NVIDIA terpasang, seperti instans G4dn, lihat Driver NVIDIA sebagai gantinya.

Daftar Isi

- Driver Perangkat Lunak AMD Radeon Pro untuk Korporasi
- AMIs dengan driver AMD diinstal
- Mengunduh driver AMD

Driver Perangkat Lunak AMD Radeon Pro untuk Korporasi

Driver AMD Radeon Pro Software for Enterprise dibangun untuk memberikan support untuk kasus penggunaan grafis kelas profesional. Dengan menggunakan driver tersebut, Anda dapat mengonfigurasi instans dengan dua layar 4K per GPU.

Didukung APIs

- OpenGL, OpenCL
- Vulkan
- Advanced Media Framework AMD

- API Akselerasi Video
- DirectX 9 dan setelahnya
- Media Foundation Transform Perangkat Keras Microsoft

AMIs dengan driver AMD diinstal

AWS menawarkan berbagai Amazon Machine Images (AMIs) yang disertakan dengan driver AMD yang diinstal. Buka Penawaran Marketplace dengan driver AMD.

Mengunduh driver AMD

Jika tidak menggunakan AMI dengan driver AMD terinstal, Anda dapat mengunduh driver AMD dan menginstalnya pada instans Anda. Hanya versi sistem operasi berikut yang mendukung driver AMD:

- Amazon Linux 2 dengan kernel versi 5.4
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Unduhan ini hanya tersedia untuk AWS pelanggan. Dengan mengunduh, Anda setuju untuk menggunakan perangkat lunak yang diunduh hanya untuk dikembangkan AMIs untuk digunakan dengan perangkat keras AMD Radeon Pro V520. Setelah instalasi perangkat lunak, Anda terikat oleh ketentuan Perjanjian Lisensi Pengguna Akhir AMD.

Instal driver AMD di instans Amazon Linux 2 Linux Anda

1. Hubungkan dengan instans Linux Anda.
2. Instal instans AWS CLI Linux Anda dan konfigurasikan kredensi default. Untuk informasi selengkapnya, lihat Menginstal AWS CLI dalam Panduan Pengguna AWS Command Line Interface .

> **Important**
>
> Pengguna atau peran Anda harus memiliki izin yang diberikan yang berisi kebijakan AmazonS3 ReadOnlyAccess. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AmazonS3 ReadOnlyAccess di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

3. Instal kernel 5.4

```
$ sudo amazon-linux-extras disable kernel-5.10
$ sudo amazon-linux-extras enable kernel-5.4
$ sudo yum install -y kernel
```

4. Install gcc dan make, jika belum terinstal.

```
$ sudo yum install gcc make
```

5. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
$ sudo amazon-linux-extras install epel -y
$ sudo yum update -y
```

6. Boot ulang instans.

```
$ sudo reboot
```

7. Hubungkan kembali diri Anda ke instans setelah boot ulang.
8. Unduh driver AMD terbaru.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

9. Ekstrak file.

```
$ tar -xf amdgpu-pro-*rhel*.tar.xz
```

10. Ubah ke folder untuk driver yang diekstrak.
11. Jalankan skrip menginstal mandiri untuk menginstal tumpukan grafis penuh.

```
$ ./amdgpu-pro-install -y --opencl=pal,legacy
```

12. Boot ulang instans.

```
$ sudo reboot
```

13. Konfirmasikan bahwa pengemudi berfungsi.

```
$ sudo dmesg | grep amdgpu
```

Responsnya akan terlihat seperti berikut:

```
Initialized amdgpu
```

Instal driver AMD pada instance Ubuntu Linux Anda

1. Hubungkan dengan instans Linux Anda.
2. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
$ sudo apt-get update --fix-missing && sudo apt-get upgrade -y
```

3. Install gcc dan make, jika belum terinstal.

```
$ sudo apt install build-essential -y
```

4. Instal firmware Linux dan modul kernel

```
$ sudo apt install linux-firmware linux-modules-extra-aws -y
```

5. Contoh reboot

```
$ sudo reboot
```

6. Hubungkan kembali diri Anda ke instans setelah boot ulang.
7. Instal paket driver AMD Linux

   - Untuk Ubuntu 20.04:

```
$ wget https://repo.radeon.com/.preview/afe3e25b8f1beff0bb312e27924d63b5/amdgpu-
install/5.4.02.01/ubuntu/focal/amdgpu-install_5.4.02.01.50402-1_all.deb
$ sudo dpkg --add-architecture i386
```

```
$ sudo apt install ./amdgpu-install_5.4.02.01.50402-1_all.deb
```

- Untuk versi Ubuntu yang lebih baru, buka Driver Linux® untuk AMD Radeon™ Graphics dan unduh paket Ubuntu terbaru dan instal.

```
$ sudo apt install ./amdgpu-install_{version-you-downloaded}.deb
```

8. Jalankan skrip menginstal mandiri untuk menginstal tumpukan grafis penuh.

```
$ amdgpu-install --usecase=workstation --vulkan=pro -y
```

9. Boot ulang instans.

```
$ sudo reboot
```

10. Konfirmasikan bahwa pengemudi berfungsi.

```
$ sudo dmesg | grep amdgpu
```

Responsnya akan terlihat seperti berikut:

```
Initialized amdgpu
```

Instal driver AMD pada instance Windows Anda

1. Connect ke instance Windows Anda dan buka PowerShell jendela.
2. Konfigurasikan kredenal default untuk instans AWS Tools for Windows PowerShell pada Windows Anda. Untuk informasi selengkapnya, lihat Memulai AWS Tools for Windows PowerShell di Panduan Pengguna.AWS Tools for PowerShell

> **Important**
>
> Pengguna atau peran Anda harus memiliki izin yang diberikan yang berisi kebijakan AmazonS3 ReadOnlyAccess. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AmazonS3 ReadOnlyAccess di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

3. Mengatur key prefix sesuai dengan versi Windows Anda:

- Windows 10 dan Windows 11

```
$KeyPrefix = "latest/AMD_GPU_WINDOWS10"
```

- Windows Server 2016

```
$KeyPrefix = "archives"
```

- Windows Server 2019

```
$KeyPrefix = "latest/AMD_GPU_WINDOWS_2K19" # use "archives" for Windows Server
 2016
```

- Windows Server 2022

```
$KeyPrefix = "latest/AMD_GPU_WINDOWS_2K22"
```

4. Unduh driver dari Amazon S3 ke desktop Anda menggunakan perintah berikutPowerShell .

```
$Bucket = "ec2-amd-windows-drivers"
$LocalPath = "$home\Desktop\AMD"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
    }
}
```

5. Buka zip file driver yang diunduh dan jalankan penginstal menggunakan perintah berikutPowerShell .

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Sekarang, periksa isi direktori baru. Nama direktori dapat diambil menggunakan `Get-ChildItem` PowerShell perintah.

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

Output harus serupa dengan yang berikut ini:

```
Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Instal driver:

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

6. Ikuti petunjuk untuk menginstal driver dan mem-boot ulang instans Anda sesuai kebutuhan.
7. Untuk memverifikasi bahwa GPU berfungsi dengan benar, periksa Device Manager. Anda akan melihat “AMD Radeon Pro V520 MxGPU” terdaftar sebagai adaptor tampilan.
8. Untuk membantu memanfaatkan empat layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi, Amazon DCV.

Driver NVIDIA untuk instans Amazon EC2 Anda

Instance dengan GPU NVIDIA yang terpasang, seperti tipe instans seri P- atau G-, harus memiliki driver NVIDIA yang sesuai diinstal. Bergantung pada jenis instans, Anda dapat mengunduh driver NVIDIA publik, mengunduh driver dari Amazon S3 yang hanya tersedia untuk AWS pelanggan, atau menggunakan AWS AMI dengan driver yang sudah diinstal sebelumnya.

Untuk menginstal driver AMD pada instans dengan GPU AMD terpasang, seperti instans G4ad, lihat Driver AMD sebagai gantinya.

Topik

- Jenis driver NVIDIA
- Driver yang tersedia berdasarkan tipe instans
- Opsi penginstalan
- Gunakan AMIs itu termasuk driver NVIDIA
- Instal driver publik NVIDIA

- Instal driver NVIDIA GRID (instans G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn, dan G3)
- Instal driver game NVIDIA (instans G7e, G6, G6e, G5, dan G4dn)

Jenis driver NVIDIA

Berikut ini adalah tipe utama driver NVIDIA yang dapat digunakan dengan instans berbasis GPU.

Driver Tesla

Driver ini ditujukan terutama untuk beban kerja komputasi, yang digunakanGPUs untuk tugas komputasi seperti penghitungan floating-point paralel untuk pembelajaran mesin dan transformasi Fourier cepat untuk aplikasi komputasi performa tinggi.

Driver GRID

Driver ini disertifikasi untuk memberikan performa optimal untuk aplikasi visualisasi profesional yang melakukan render konten seperti model 3D atau video resolusi tinggi. Anda dapat mengonfigurasi driver GRID untuk mendukung dua mode. Quadro Virtual Workstations menyediakan akses ke empat layar 4K per GPU. GRID vApps menyediakan kemampuan hosting Aplikasi RDSH.

Driver game

Driver ini berisi optimisasi untuk game dan diperbarui secara frekuen untuk memberikan peningkatan performa. Driver ini juga mendukung satu layar 4K per GPU.

Mode terkonfigurasi

Di Windows, driver Tesla dikonfigurasi untuk berjalan dalam mode Tesla Compute Cluster (TCC). Driver GRID dan game dikonfigurasi untuk berjalan dalam mode Windows Display Driver Model (WDDM). Dalam mode TCC, kartu tersebut dikhususkan untuk beban kerja komputasi. Dalam mode WDDM, kartu mendukung beban kerja komputasi dan grafis.

Panel kontrol NVIDIA

Panel kontrol NVIDIA didukung dengan driver GRID dan Gaming. Panel kontrol NVIDIA tidak didukung dengan driver Tesla.

Didukung APIs untuk driver Tesla, GRID, dan game

- OpenCL, OpenGL, dan Vulkan

- NVIDIA CUDA dan pustaka terkait (misalnya, cuDNN, TensorRT, nvJPEG, and cuBLAS)
- NVENC untuk enkode video dan NVDEC untuk dekode video
- Khusus Windows: APIs DirectX, Direct2D, Akselerasi Video DirectX, DirectX Raytracing

Driver yang tersedia berdasarkan tipe instans

Tabel berikut merangkum driver NVIDIA yang didukung untuk setiap tipe instans GPU.

Jenis instans	Driver Tesla	Driver GRID	Driver game
G3	Ya	Ya	Tidak
G4dn	Ya	Ya	Ya
G5	Ya	Ya	Ya
G5g	Ya [1]	Tidak	Tidak
G6	Ya	Ya	Ya
G6e	Ya	Ya	Ya
G6f	Tidak	Ya	Tidak
Gr6	Ya	Ya	Tidak
GR6f	Tidak	Ya	Tidak
G7e	Ya	Ya	Ya
P2	Ya	Tidak	Tidak
P3	Ya	Tidak	Tidak
P4d	Ya	Tidak	Tidak
P4de	Ya	Tidak	Tidak
P5	Ya	Tidak	Tidak

Jenis instans	Driver Tesla	Driver GRID	Driver game
P5e	Ya	Tidak	Tidak
P5en	Ya	Tidak	Tidak
P6-B200	Ya	Tidak	Tidak
P6e- GB200	Ya	Tidak	Tidak
P6-B300	Ya	Tidak	Tidak

[1] Driver Tesla ini juga mendukung aplikasi grafis yang dioptimalkan khusus untuk platform ARM64

Opsi penginstalan

Gunakan salah satu opsi berikut untuk mendapatkan driver NVIDIA yang diperlukan untuk instans GPU Anda.

Pilihan

1. Gunakan AMIs itu termasuk driver NVIDIA
2. Instal driver publik NVIDIA
3. Instal driver NVIDIA GRID (instans G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn, dan G3)
4. Instal driver game NVIDIA (instans G7e, G6, G6e, G5, dan G4dn)

Gunakan AMIs itu termasuk driver NVIDIA

AWS dan NVIDIA menawarkan Gambar Mesin Amazon yang berbeda (AMIs) yang disertakan dengan driver NVIDIA yang diinstal.

- Penawaran Marketplace dengan pengemudi umum Tesla
- Penawaran pasar dengan driver GRID
- Penawaran pasar dengan driver Gaming

Untuk meninjau pertimbangan yang bergantung pada platform sistem operasi (OS) Anda, pilih tab yang berlaku untuk AMI Anda.

Linux

Untuk memperbarui versi driver yang diinstal menggunakan salah satu dari ini AMIs, Anda harus menghapus paket NVIDIA dari instance Anda untuk menghindari konflik versi. Gunakan perintah ini untuk menghapus paket NVIDIA:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Paket kit alat CUDA memiliki dependensi terhadap driver NVIDIA. Menghapus instalasi paket NVIDIA akan menghapus kit alat CUDA. Anda harus menginstal ulang kit alat CUDA setelah menginstal driver NVIDIA.

Windows

Jika Anda membuat AMI Windows kustom menggunakan salah satu AWS Marketplace penawaran, AMI harus berupa gambar standar yang dibuat dengan Windows Sysprep untuk memastikan bahwa driver GRID berfungsi. Lihat informasi yang lebih lengkap di Buat Amazon EC2 AMI menggunakan Windows Sysprep.

Instal driver publik NVIDIA

Jika yang AWS Marketplace AMIs dijelaskan dalam Gunakan AMIs itu termasuk driver NVIDIA tidak sesuai dengan kasus penggunaan Anda, Anda dapat menginstal driver publik dan membawa lisensi Anda sendiri. Opsi instalasi meliputi yang berikut:

- Opsi 1: Instalasi khusus driver
- Opsi 2: Instal dengan toolkit CUDA(direkomendasikan untuk distribusi Linux)

Pertimbangan tipe instans P6-B200 dan P6-B300

Platform P6-B200 dan P6-B300 unik karena mengekspos kartu antarmuka jaringan Mellanox ConnectX () ke instance sebagai perangkat. NICs PCIe Ini NICs tidak bertindak sebagai antarmuka jaringan yang khas tetapi berfungsi sebagai NVSwitch jembatan yang menyediakan jalur kontrol untuk menginisialisasi dan mengkonfigurasi NVFabric, yang merupakan NVLink topologi interkoneksi GPU.

Untuk sepenuhnya menginisialisasi sistem, NVIDIA Fabric Manager harus mengkonfigurasi `NVFabric` dan menetapkan NVSwitch topologi. Hal ini memungkinkan modul InfiniBand kernel untuk berkomunikasi dengan Mellanox ConnectX. NICs

NVIDIA Fabric Manager disertakan dalam toolkit CUDA. Kami merekomendasikan Opsi 2: Instal dengan toolkit CUDA untuk jenis contoh ini.

Opsi 1: Instalasi khusus driver

Untuk menginstal driver tertentu, masuk ke instans Anda dan unduh driver publik NVIDIA 64-bit untuk jenis instans dari http://www.nvidia. com/Download/Find.aspx. Untuk Jenis Produk, Seri Produk, dan Produk, gunakan opsi yang ditunjukkan pada tabel berikut.

Kemudian ikuti petunjuk Instalasi Repositori Lokal di Panduan Instalasi Driver NVIDIA.

> **Note**
>
> Jenis instans P6-B200 dan P6-B300 memerlukan instalasi dan konfigurasi paket tambahan yang disertakan dengan NVIDIA CUDA Toolkit. Untuk informasi selengkapnya, lihat petunjuk untuk distribusi Linux Anda diOpsi 2: Instal dengan toolkit CUDA.

Instans	Jenis produk	Seri produk	Produk	Versi driver minimum
G3	Tesla	Kelas M	M60	--
G4dn	Tesla	T-Series	T4	--
G5	Tesla	A-Series	A10	470.00 atau yang lebih baru
G5g 1	Tesla	T-Series	T4G	470.82.01 atau yang lebih baru
G6	Tesla	Seri-L	L4	525.0 atau yang lebih baru
G6e	Tesla	Seri-L	L40-AN	535.0 atau yang lebih baru

Instans	Jenis produk	Seri produk	Produk	Versi driver minimum
Gr6	Tesla	Seri-L	L4	525.0 atau yang lebih baru
G7e	Tesla	Seri RTX	RTX PRO 6000 Blackwell	575.0 atau yang lebih baru
P2	Tesla	K-Series	K80	--
P3	Tesla	V-Series	V100	--
P4d	Tesla	A-Series	A100	--
P4de	Tesla	A-Series	A100	--
P5	Tesla	H-Series	H100	530 atau yang lebih baru
P5e	Tesla	H-Series	H200	550 atau lebih baru
P5en	Tesla	H-Series	H200	550 atau lebih baru
P6-B200 [2]	Tesla	Seri HGX	B200	570 atau yang lebih baru
P6e- 00 GB2	Tesla	Seri HGX	B200	570 atau yang lebih baru
P6-B300 [2]	Tesla	Seri HGX	B300	580 atau yang lebih baru

[1] Sistem operasi untuk instance G5G adalah Linux aarch64.

[2] Untuk jenis instans P6-B200 dan P6-B300, ada persyaratan instalasi tambahan untuk mengkonfigurasi NVIDIA Fabric Manager.

Opsi 2: Instal dengan toolkit CUDA

Instruksi penginstalan sedikit berbeda menurut sistem operasi. Untuk menginstal driver publik pada instans Anda dengan toolkit NVIDIA CUDA, ikuti petunjuk untuk sistem operasi instans Anda. Misalnya sistem operasi yang tidak ditampilkan di sini, ikuti petunjuk untuk sistem operasi dan arsitektur tipe instans Anda di situs web Pengembang NVIDIA. Untuk informasi selengkapnya, lihat Unduhan Toolkit CUDA.

Misalnya arsitektur tipe atau spesifikasi lainnya, lihat Spesifikasi komputasi Akselerasi dalam referensi Jenis EC2 Instance Amazon.

Amazon Linux 2023

Bagian ini mencakup instalasi toolkit NVIDIA CUDA pada instans Amazon Linux 2023. Contoh perintah di bagian ini didasarkan pada `x86_64` arsitektur.

Untuk `arm64-sbsa` perintah, lihat CUDA Toolkit Downloads dan pilih opsi yang berlaku untuk distribusi Anda. Instruksi muncul setelah Anda membuat pilihan akhir.

Prasyarat

Sebelum menginstal toolkit dan driver, jalankan perintah berikut untuk memastikan bahwa Anda memiliki versi header kernel dan paket pengembangan yang benar.

```
[ec2-user ~]$ sudo dnf install kernel-devel-$(uname -r) kernel-headers-$(uname -r) -y
```

Unduh toolkit dan driver

Pilih jenis instalasi yang akan digunakan untuk instans Anda, dan ikuti langkah-langkah terkait.

RPM local installation

Anda dapat mengikuti petunjuk ini untuk mengunduh bundel repositori installer toolkit CUDA ke instance Anda, lalu ekstrak dan daftarkan bundel yang ditentukan.

Untuk melihat petunjuk di situs web pengembang NVIDIA, lihat CUDA Toolkit Downloads.

```
[ec2-user ~]$ wget https://developer.download.nvidia.com/compute/cuda/13.0.0/
local_installers/cuda-repo-amzn2023-13-0-local-13.0.0_580.65.06-1.x86_64.rpm
[ec2-user ~]$ sudo rpm -i cuda-repo-amzn2023-13-0-
local-13.0.0_580.65.06-1.x86_64.rpm
```

RPM network installation

Anda dapat mengikuti petunjuk ini untuk mendaftarkan repositori CUDA dengan manajer paket pada instance Anda. Saat Anda menjalankan langkah-langkah penginstalan, manajer paket hanya mengunduh paket yang diperlukan.

Untuk melihat petunjuk di situs web pengembang NVIDIA, lihat CUDA Toolkit Downloads.

```
[ec2-user ~]$ wget https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2404/x86_64/cuda-keyring_1.1-1_all.deb
[ec2-user ~]$ sudo dpkg -i cuda-keyring_1.1-1_all.deb
```

Langkah-langkah yang tersisa sama untuk instalasi lokal dan jaringan.

1. Selesaikan instalasi toolkit CUDA

```
[ec2-user ~]$ sudo dnf clean all
[ec2-user ~]$ sudo dnf install cuda-toolkit -y
```

2. Instal varian modul kernel terbuka dari driver

```
[ec2-user ~]$ sudo dnf module install nvidia-driver:open-dkms -y
```

3. Instal GPUDirect Penyimpanan dan Manajer Kain

```
[ec2-user ~]$ sudo dnf install nvidia-gds -y
[ec2-user ~]$ sudo dnf install nvidia-fabric-manager -y
```

4. Aktifkan Manajer Fabric dan ketekunan pengemudi

```
[ec2-user ~]$ sudo systemctl enable nvidia-fabricmanager
[ec2-user ~]$ sudo systemctl enable nvidia-persistenced
```

5. (Hanya P6-B200 dan P6-B300) Jenis instans ini memerlukan instalasi dan konfigurasi paket tambahan yang dibundel dengan NVIDIA CUDA Toolkit.

   1. Instal NVIDIA Link Subnet Manager dan`ibstat`.

      ```
      [ec2-user ~]$ sudo dnf install nvlink5
      ```

   2. Aktifkan pemuatan otomatis modul Infiniband saat startup.

```
[ec2-user ~]$ echo "ib_umad" | sudo tee -a /etc/modules-load.d/modules.conf
```

6. Nyalakan ulang instance

```
[ec2-user ~]$ sudo reboot
```

Ubuntu 24.04

Bagian ini mencakup instalasi toolkit NVIDIA CUDA pada instance Ubuntu 24.04. Contoh perintah di bagian ini didasarkan pada `x86_64` arsitektur.

Untuk `arm64-sbsa` perintah, lihat CUDA Toolkit Downloads dan pilih opsi yang berlaku untuk distribusi Anda. Instruksi muncul setelah Anda membuat pilihan akhir.

Prasyarat

Sebelum menginstal toolkit dan driver, jalankan perintah berikut untuk memastikan bahwa Anda memiliki versi header kernel dan paket pengembangan yang benar.

```
$ apt install linux-headers-$(uname -r)
```

Unduh toolkit dan driver

Pilih jenis instalasi yang akan digunakan untuk instans Anda, dan ikuti langkah-langkah terkait.

RPM local installation

Anda dapat mengikuti petunjuk ini untuk mengunduh bundel repositori installer toolkit CUDA ke instance Anda, lalu ekstrak dan daftarkan bundel yang ditentukan.

Untuk melihat petunjuk di situs web pengembang NVIDIA, lihat CUDA Toolkit Downloads.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/
x86_64/cuda-ubuntu2404.pin
$ sudo mv cuda-ubuntu2404.pin /etc/apt/preferences.d/cuda-repository-pin-600
$ wget https://developer.download.nvidia.com/compute/cuda/13.0.0/
local_installers/cuda-repo-ubuntu2404-13-0-local_13.0.0-580.65.06-1_amd64.deb
$ sudo dpkg -i cuda-repo-ubuntu2404-13-0-local_13.0.0-580.65.06-1_amd64.deb
$ sudo cp /var/cuda-repo-ubuntu2404-13-0-local/cuda-*-keyring.gpg /usr/share/
keyrings/
```

RPM network installation

Anda dapat mengikuti petunjuk ini untuk mendaftarkan repositori CUDA dengan manajer paket pada instance Anda. Saat Anda menjalankan langkah-langkah penginstalan, manajer paket hanya mengunduh paket yang diperlukan.

Untuk melihat petunjuk di situs web pengembang NVIDIA, lihat CUDA Toolkit Downloads.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/x86_64/
cuda-keyring_1.1-1_all.deb
$ sudo dpkg -i cuda-keyring_1.1-1_all.deb
```

Langkah-langkah yang tersisa sama untuk instalasi lokal dan jaringan.

1. Selesaikan instalasi toolkit CUDA

```
$ sudo apt update
$ sudo apt install cuda-toolkit -y
```

2. Instal varian modul kernel terbuka dari driver

```
$ sudo apt install nvidia-open -y
```

3. Instal GPUDirect Penyimpanan dan Manajer Kain

```
$ sudo apt install nvidia-gds -y
$ sudo apt install nvidia-fabricmanager -y
```

4. Aktifkan Manajer Fabric dan ketekunan pengemudi

```
$ sudo systemctl enable nvidia-fabricmanager
$ sudo systemctl enable nvidia-persistenced
```

5. (Hanya P6-B200 dan P6-B300) Jenis instans ini memerlukan instalasi dan konfigurasi paket tambahan yang dibundel dengan NVIDIA CUDA Toolkit.

    1. Instal driver perangkat InfiniBand khusus terbaru dan utilitas diagnostik.

    ```
    $ sudo apt install linux-modules-extra-$(uname -r) -y
    $ sudo apt install infiniband-diags -y
    ```

2. Instal NVIDIA Link Subnet Manager.

```
$ sudo apt install nvlsm -y
```

6. Nyalakan ulang instance

```
sudo reboot
```

7. Perbarui jalur Anda dan tambahkan variabel lingkungan berikut.

```
$ export PATH=${PATH}:/usr/local/cuda-13.0/bin
$ export LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/usr/local/cuda-13.0/lib64
```

Sistem operasi Windows

Untuk menginstal driver NVIDIA di Windows, ikuti langkah-langkah ini:

1. Buka folder tempat Anda mengunduh driver dan luncurkan file instalasi. Ikuti petunjuk untuk menginstal driver dan mem-boot ulang instans Anda sesuai kebutuhan.
2. Nonaktifkan adaptor tampilan bernama Microsoft Basic Display Adapter yang ditandai dengan ikon peringatan menggunakan Device Manager. Instal fitur Windows ini: Media Foundation dan Quality Windows Audio Video Experience.

> **Important**
>
> Jangan nonaktifkan adaptor tampilan bernama Microsoft Remote Display Adapter. Jika Microsoft Remote Display Adapter dinonaktifkan, koneksi Anda mungkin terputus dan upaya untuk menyambung ke instans setelah reboot mungkin gagal.

3. Periksa Manajer Perangkat untuk memverifikasi bahwa GPU berfungsi dengan benar.
4. Untuk mencapai kinerja terbaik dari GPU Anda, selesaikan langkah-langkah pengoptimalan di Optimalkan pengaturan GPU di instans Amazon EC2.

Instal driver NVIDIA GRID (instans G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn, dan G3)

Unduhan ini hanya tersedia untuk AWS pelanggan. Dengan mengunduh, untuk mematuhi persyaratan AWS solusi sebagaimana dimaksud dalam Perjanjian Lisensi Pengguna Akhir Cloud

NVIDIA GRID (EULA), Anda setuju untuk menggunakan perangkat lunak yang diunduh hanya untuk dikembangkan AMIs untuk digunakan dengan perangkat keras NVIDIA L4, NVIDIA L40S, NVIDIA A10G, NVIDIA Tesla T4, atau NVIDIA Tesla M60. Anda dapat menggunakan driver GRID untuk membuat dan menggunakan AMIs dalam AWS lingkungan. Setelah menginstal perangkat lunak, Anda terikat oleh persyaratan Perjanjian Lisensi Pengguna Akhir Cloud NVIDIA GRID. Untuk informasi tentang versi driver NVIDIA GRID untuk sistem operasi Anda, lihat Perangkat Lunak GPU Virtual NVIDIA (vGPU) di situs web NVIDIA.

Pertimbangan-pertimbangan

- Instans G7e memerlukan GRID 19.1 atau yang lebih baru untuk Linux dan 19.3 (581.192) atau yang lebih baru untuk Windows.
- Instans G6f dan Gr6f memerlukan GRID 18.4 atau yang lebih baru.
- Instans G6e membutuhkan GRID 17.4 atau yang lebih baru.
- Instans G6 dan Gr6 memerlukan GRID 17.1 atau yang lebih baru.
- Instans G5 memerlukan GRID 13.1 atau setelahnya (atau GRID 12.4 atau setelahnya).
- Instans G3 memerlukan resolusi DNS AWS yang disediakan agar lisensi GRID berfungsi.
- IMDSv2hanya didukung dengan driver NVIDIA versi 14.0 atau lebih tinggi.
- Untuk instance Windows, jika Anda meluncurkan instans Anda dari AMI Windows kustom, AMI harus berupa gambar standar yang dibuat dengan Windows Sysprep untuk memastikan bahwa driver GRID berfungsi. Untuk informasi selengkapnya, lihat Buat Amazon EC2 AMI menggunakan Windows Sysprep.
- GRID 17.0 dan yang lebih baru tidak mendukung Windows Server 2019.
- GRID 14.2 dan yang lebih baru tidak mendukung Windows Server 2016.
- GRID 17.0 dan yang lebih baru tidak didukung dengan instance G3.
- Untuk instance Linux, Anda mungkin perlu menginstal atau memperbarui paket, seperti gcc, jika penginstal NVIDIA gagal dengan pesan kesalahan. Spesifikasinya tergantung pada versi sistem operasi dan kernel. Untuk informasi selengkapnya, lihat Portal Dukungan Perusahaan NVIDIA.

Prasyarat

- (Linux) Verifikasi bahwa diinstal pada instans Anda dan dikonfigurasi dengan kredensi default. AWS CLI Untuk informasi selengkapnya, lihat Menginstal AWS CLI dalam Panduan Pengguna AWS Command Line Interface .

- (Windows) Konfigurasikan kredenal default untuk instans AWS Tools for Windows PowerShell Anda. Untuk informasi selengkapnya, lihat Memulai AWS Tools for Windows PowerShell dalam Panduan Pengguna AWS Tools for PowerShell .
- Pengguna atau peran Anda harus memiliki izin yang diberikan yang berisi kebijakan AmazonS3 ReadOnlyAccess.

Amazon Linux 2023

Untuk menginstal driver NVIDIA GRID pada instans Anda

1. Terhubung ke instans Anda. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
[ec2-user ~]$ sudo dnf update -y
```

2. Install gcc dan make, jika belum terinstal.

```
[ec2-user ~]$ sudo dnf install gcc make
```

3. Boot ulang untuk memuat versi kernel terbaru.

```
[ec2-user ~]$ sudo reboot
```

4. Hubungkan kembali ke instans Anda setelah boot ulang.
5. Instal paket header kernel.

```
[ec2-user ~]$ sudo dnf install -y kernel-devel kernel-modules-extra
```

6. Unduh utilitas instalasi driver GRID menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Beberapa versi driver GRID disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Tambahkan izin untuk menjalankan utilitas penginstalan driver menggunakan perintah berikut.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Jalankan skrip instalasi mandiri sebagai berikut untuk menginstal driver GRID yang Anda unduh. Misalnya:

   ```
   [ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
   ```

   Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

9. Konfirmasikan bahwa pengemudi berfungsi. Respons untuk perintah berikut mencantumkan versi driver NVIDIA yang diinstal dan detail tentang GPUs.

   ```
   [ec2-user ~]$ nvidia-smi -q | head
   ```

10. Jika Anda menggunakan perangkat lunak NVIDIA vGPU versi 14.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
    etc/modprobe.d/nvidia.conf
    ```

11. Boot ulang instans.

    ```
    [ec2-user ~]$ sudo reboot
    ```

12. (Opsional) Bergantung pada kasus penggunaan Anda, Anda dapat menyelesaikan langkah opsional berikut. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah-langkah ini.

    a. Untuk membantu memanfaatkan empat layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

    b. Mode NVIDIA Quadro Virtual Workstation diaktifkan secara default. Untuk mengaktifkan Aplikasi Virtual GRID untuk kemampuan hosting Aplikasi RDSH, selesaikan langkah-langkah aktivasi Aplikasi Virtual GRID di Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon.

Amazon Linux 2

Untuk menginstal driver NVIDIA GRID pada instans Anda

1. Terhubung ke instans Anda. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

2. Install gcc dan make, jika belum terinstal.

   ```
   [ec2-user ~]$ sudo yum install gcc make
   ```

3. Boot ulang untuk memuat versi kernel terbaru.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Hubungkan kembali ke instans Anda setelah boot ulang.
5. Instal paket header kernel untuk versi kernel yang sedang berjalan.

   ```
   [ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
   ```

6. Unduh utilitas instalasi driver GRID menggunakan perintah berikut:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
   ```

   Beberapa versi driver GRID disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut.

   ```
   [ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
   ```

7. Tambahkan izin untuk menjalankan utilitas penginstalan driver menggunakan perintah berikut.

   ```
   [ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
   ```

8. Jalankan skrip instalasi mandiri sebagai berikut untuk menginstal driver GRID yang Anda unduh. Misalnya:

   ```
   [ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
   ```

Jika Anda menggunakan Amazon Linux 2 dengan kernel versi 5.10, gunakan perintah berikut untuk menginstal driver GRID.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

9. Konfirmasikan bahwa pengemudi berfungsi. Respons untuk perintah berikut mencantumkan versi driver NVIDIA yang diinstal dan detail tentang GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Jika Anda menggunakan perangkat lunak NVIDIA vGPU versi 14.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

12. (Opsional) Bergantung pada kasus penggunaan Anda, Anda dapat menyelesaikan langkah opsional berikut. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah-langkah ini.

    a. Untuk membantu memanfaatkan empat layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

    b. Mode NVIDIA Quadro Virtual Workstation diaktifkan secara default. Untuk mengaktifkan Aplikasi Virtual GRID untuk kemampuan hosting Aplikasi RDSH, selesaikan langkah-langkah aktivasi Aplikasi Virtual GRID di Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon.

CentOS 7 dan Red Hat Enterprise Linux 7

Untuk menginstal driver NVIDIA GRID pada instans Anda

1. Terhubung ke instans Anda. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
[ec2-user ~]$ sudo yum update -y
```

2. Install gcc dan make, jika belum terinstal.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

3. Boot ulang untuk memuat versi kernel terbaru.

```
[ec2-user ~]$ sudo reboot
```

4. Hubungkan kembali ke instans Anda setelah boot ulang.
5. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Nonaktifkan driver `nouveau` sumber terbuka untuk kartu grafis NVIDIA.

   a. Menambahkan `nouveau` ke file daftar hitam `/etc/modprobe.d/blacklist.conf`. Salin blok kode berikut dan tempelkan ke terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edit file `/etc/default/grub` dan tambahkan baris berikut:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Bangun kembali konfigurasi Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Unduh utilitas instalasi driver GRID menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Beberapa versi driver GRID disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Tambahkan izin untuk menjalankan utilitas penginstalan driver menggunakan perintah berikut.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Jalankan skrip instalasi mandiri sebagai berikut untuk menginstal driver GRID yang Anda unduh. Misalnya:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

10. Konfirmasikan bahwa pengemudi berfungsi. Respons untuk perintah berikut mencantumkan versi driver NVIDIA yang diinstal dan detail tentang GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Jika Anda menggunakan perangkat lunak NVIDIA vGPU versi 14.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

12. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

13. (Opsional) Bergantung pada kasus penggunaan Anda, Anda dapat menyelesaikan langkah opsional berikut. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah-langkah ini.

    a. Untuk membantu memanfaatkan empat layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

    b. Mode NVIDIA Quadro Virtual Workstation diaktifkan secara default. Untuk mengaktifkan Aplikasi Virtual GRID untuk kemampuan hosting Aplikasi RDSH, selesaikan langkah-langkah aktivasi Aplikasi Virtual GRID di Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon.

    c. Instal desktop/workstation paket GUI.

    ```
    [ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
    ```

CentOS Stream 8 dan Red Hat Enterprise Linux 8

Untuk menginstal driver NVIDIA GRID pada instans Anda

1. Terhubung ke instans Anda. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

2. Install gcc dan make, jika belum terinstal.

   ```
   [ec2-user ~]$ sudo yum install -y gcc make
   ```

3. Boot ulang untuk memuat versi kernel terbaru.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Hubungkan kembali ke instans Anda setelah boot ulang.

5. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Unduh utilitas instalasi driver GRID menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Beberapa versi driver GRID disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Tambahkan izin untuk menjalankan utilitas penginstalan driver menggunakan perintah berikut.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Jalankan skrip instalasi mandiri sebagai berikut untuk menginstal driver GRID yang Anda unduh. Misalnya:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

9. Konfirmasikan bahwa pengemudi berfungsi. Respons untuk perintah berikut mencantumkan versi driver NVIDIA yang diinstal dan detail tentang GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Jika Anda menggunakan perangkat lunak NVIDIA vGPU versi 14.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

12. (Opsional) Bergantung pada kasus penggunaan Anda, Anda dapat menyelesaikan langkah opsional berikut. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah-langkah ini.

    a. Untuk membantu memanfaatkan empat layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

    b. Mode NVIDIA Quadro Virtual Workstation diaktifkan secara default. Untuk mengaktifkan Aplikasi Virtual GRID untuk kemampuan hosting Aplikasi RDSH, selesaikan langkah-langkah aktivasi Aplikasi Virtual GRID di Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon.

    c. Instal paket workstation GUI.

    ```
    [ec2-user ~]$ sudo dnf groupinstall -y workstation
    ```

Rocky Linux 8

Untuk menginstal driver NVIDIA GRID pada instans Linux Anda

1. Terhubung ke instans Anda. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

2. Install gcc dan make, jika belum terinstal.

   ```
   [ec2-user ~]$ sudo yum install -y gcc make
   ```

3. Boot ulang untuk memuat versi kernel terbaru.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Hubungkan kembali ke instans Anda setelah boot ulang.

5. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Unduh utilitas instalasi driver GRID menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Beberapa versi driver GRID disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Tambahkan izin untuk menjalankan utilitas penginstalan driver menggunakan perintah berikut.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Jalankan skrip instalasi mandiri sebagai berikut untuk menginstal driver GRID yang Anda unduh. Misalnya:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

9. Konfirmasikan bahwa pengemudi berfungsi. Respons untuk perintah berikut mencantumkan versi driver NVIDIA yang diinstal dan detail tentang GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Jika Anda menggunakan perangkat lunak NVIDIA vGPU versi 14.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

12. (Opsional) Bergantung pada kasus penggunaan Anda, Anda dapat menyelesaikan langkah opsional berikut. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah-langkah ini.

    a. Untuk membantu memanfaatkan empat layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

    b. Mode NVIDIA Quadro Virtual Workstation diaktifkan secara default. Untuk mengaktifkan Aplikasi Virtual GRID untuk kemampuan hosting Aplikasi RDSH, selesaikan langkah-langkah aktivasi Aplikasi Virtual GRID di Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon.

Ubuntu dan Debian

Untuk menginstal driver NVIDIA GRID pada instans Anda

1. Terhubung ke instans Anda. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
$ sudo apt-get update -y
```

2. Install gcc dan make, jika belum terinstal.

```
$ sudo apt-get install -y gcc make
```

3. (Ubuntu) Mutakhirkan paket `linux-aws` untuk menerima versi terbaru.

```
$ sudo apt-get upgrade -y linux-aws
```

   (Debian) Mutakhirkan paket untuk menerima versi terbaru.

```
$ sudo apt-get upgrade -y
```

4. Boot ulang untuk memuat versi kernel terbaru.

```
$ sudo reboot
```

5. Hubungkan kembali ke instans Anda setelah boot ulang.
6. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
$ sudo apt-get install -y linux-headers-$(uname -r) linux-modules-extra-$(uname -r)
```

7. Nonaktifkan driver nouveau sumber terbuka untuk kartu grafis NVIDIA.

   a. Menambahkan nouveau ke file daftar hitam /etc/modprobe.d/blacklist.conf. Salin blok kode berikut dan tempelkan ke terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edit file /etc/default/grub dan tambahkan baris berikut:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Bangun kembali konfigurasi Grub.

```
$ sudo update-grub
```

8. Unduh utilitas instalasi driver GRID menggunakan perintah berikut:

```
$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Beberapa versi driver GRID disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut.

```
$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Tambahkan izin untuk menjalankan utilitas penginstalan driver menggunakan perintah berikut.

```
$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Jalankan skrip instalasi mandiri sebagai berikut untuk menginstal driver GRID yang Anda unduh. Misalnya:

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

11. Konfirmasikan bahwa pengemudi berfungsi. Respons untuk perintah berikut mencantumkan versi driver NVIDIA yang diinstal dan detail tentang GPUs.

```
$ nvidia-smi -q | head
```

12. Jika Anda menggunakan perangkat lunak NVIDIA vGPU versi 14.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

13. Boot ulang instans.

```
$ sudo reboot
```

14. (Opsional) Bergantung pada kasus penggunaan Anda, Anda dapat menyelesaikan langkah opsional berikut. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah-langkah ini.

    a. Untuk membantu memanfaatkan empat layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

    b. Mode NVIDIA Quadro Virtual Workstation diaktifkan secara default. Untuk mengaktifkan Aplikasi Virtual GRID untuk kemampuan hosting Aplikasi RDSH, selesaikan langkah-langkah aktivasi Aplikasi Virtual GRID di Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon.

    c. Instal desktop/workstation paket GUI.

    ```
    $ sudo apt-get install -y lightdm ubuntu-desktop
    ```

Sistem operasi Windows

Untuk menginstal driver NVIDIA GRID pada instans Windows Anda

1. Connect ke instance Windows Anda dan buka PowerShell jendela.
2. Unduh driver dan Perjanjian Lisensi Pengguna Akhir Cloud NVIDIA GRID dari Amazon S3 ke desktop Anda menggunakan perintah berikut PowerShell .

```
$Bucket = "ec2-windows-nvidia-drivers"
$KeyPrefix = "latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
$LocalFilePath = Join-Path $LocalPath $LocalFileName
Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Banyak versi driver NVIDIA GRID disimpan dalam bucket ini. Anda dapat mengunduh semua versi Windows yang tersedia di bucket dengan menghapus opsi `-KeyPrefix $KeyPrefix`. Untuk informasi tentang versi driver NVIDIA GRID untuk sistem operasi Anda, lihat Perangkat Lunak GPU Virtual NVIDIA (vGPU) di situs web NVIDIA.

   Dimulai dengan GRID versi 11.0, Anda dapat menggunakan driver di `latest` untuk instans G3 dan G4dn. Kami tidak akan menambahkan versi setelah 11.0 hingga `g4/latest`, tetapi akan mempertahankan versi 11.0 dan versi sebelumnya khusus untuk G4dn di `g4/latest`.

   Instans G5 memerlukan GRID 13.1 atau setelahnya (atau GRID 12.4 atau setelahnya).
3. Arahkan ke desktop dan klik dua kali file instalasi untuk meluncurkannya (pilih versi driver yang sesuai dengan versi OS instans Anda). Ikuti petunjuk untuk menginstal driver dan mem-boot ulang instans Anda sesuai kebutuhan. Untuk memverifikasi bahwa GPU berfungsi dengan benar, periksa Device Manager.
4. (Opsional) Gunakan perintah berikut untuk menonaktifkan halaman lisensi di panel kontrol untuk mencegah pengguna mengubah jenis produk secara tidak sengaja (NVIDIA GRID Virtual Workstation diaktifkan secara default). Untuk informasi selengkapnya, lihat Panduan Pengguna Lisensi GRID.

PowerShell

Jalankan PowerShell perintah berikut untuk membuat nilai registri untuk menonaktifkan halaman lisensi di panel kontrol. AWS Tools for PowerShell Di AWS Windows AMIs default ke versi 32-bit dan perintah ini gagal. Sebagai gantinya, gunakan versi 64-bit dari PowerShell disertakan dengan sistem operasi.

```
New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
```

Command Prompt

Jalankan perintah registri berikut untuk membuat nilai registri untuk menonaktifkan halaman lisensi di panel kontrol. Anda dapat menjalankannya menggunakan jendela Command Prompt atau versi 64-bitPowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
 NvCplDisableManageLicensePage /t REG_DWORD /d 1
```

5. (Opsional) Bergantung pada kasus penggunaan Anda, Anda dapat menyelesaikan langkah opsional berikut. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah-langkah ini.

   a. Untuk membantu memanfaatkan empat layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi, Amazon DCV.

   b. Mode NVIDIA Quadro Virtual Workstation diaktifkan secara default. Untuk mengaktifkan Aplikasi Virtual GRID untuk kemampuan hosting Aplikasi RDSH, selesaikan langkah-langkah aktivasi Aplikasi Virtual GRID di Aktifkan Aplikasi Virtual NVIDIA GRID di instans berbasis EC2 GPU Amazon.

Instal driver game NVIDIA (instans G7e, G6, G6e, G5, dan G4dn)

Driver ini hanya tersedia untuk AWS pelanggan. Dengan mengunduhnya, Anda setuju untuk menggunakan perangkat lunak yang diunduh hanya untuk dikembangkan AMIs untuk digunakan dengan perangkat keras RTX PRO 6000 Blackwell, NVIDIA L4, NVIDIA L40S, NVIDIA A10G, NVIDIA Tesla T4, atau NVIDIA Tesla M60. Anda dapat menggunakan driver GRID untuk membuat dan

menggunakan AMIs dalam AWS lingkungan. Setelah menginstal perangkat lunak, Anda terikat oleh persyaratan Perjanjian Lisensi Pengguna Akhir Cloud NVIDIA GRID.

Pertimbangan-pertimbangan

- Instans G3 memerlukan resolusi DNS AWS yang disediakan agar lisensi GRID berfungsi.
- IMDSv2hanya didukung dengan driver NVIDIA versi 495.x atau lebih tinggi.

Prasyarat

- (Linux) Verifikasi bahwa diinstal pada instans Anda dan dikonfigurasi dengan kredensyal default. AWS CLI Untuk informasi selengkapnya, lihat Menginstal AWS CLI dalam Panduan Pengguna AWS Command Line Interface .
- Pengguna atau peran Anda harus memiliki izin yang diberikan yang berisi kebijakan AmazonS3 ReadOnlyAccess.

Amazon Linux 2023

Untuk menginstal driver game NVIDIA pada instans Anda

1. Terhubung ke instans Anda. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
[ec2-user ~]$ sudo dnf update -y
```

2. Install gcc dan make, jika belum terinstal.

```
[ec2-user ~]$ sudo dnf install gcc make
```

3. Boot ulang untuk memuat versi kernel terbaru.

```
[ec2-user ~]$ sudo reboot
```

4. Sambungkan kembali ke instance Anda setelah di-boot ulang.
5. Instal paket header kernel.

```
[ec2-user ~]$ sudo dnf install -y kernel-devel kernel-modules-extra kernel-devel-
$(uname -r) kernel-headers-$(uname -r) dkms
```

6. Unduh utilitas instalasi driver game menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Beberapa versi driver game disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Ekstrak utilitas instalasi driver game dari `.zip` arsip yang diunduh.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

8. Tambahkan izin untuk menjalankan utilitas instalasi driver menggunakan perintah berikut:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Jalankan penginstal menggunakan perintah berikut:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

   Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

10. Gunakan perintah berikut untuk membuat file konfigurasi yang diperlukan.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Gunakan perintah berikut untuk mengunduh dan mengganti nama file sertifikasi.
    - Untuk versi 590.48 atau yang lebih baru:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
```

    - Untuk versi 460.39 hingga 580.95:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Untuk versi 440.68 hingga 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Untuk versi sebelumnya:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Jika Anda menggunakan driver NVIDIA versi 510.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

14. Verifikasi lisensi NVIDIA Gaming menggunakan perintah berikut.

```
[ec2-user ~]$ nvidia-smi.exe -q
```

Dalam output, carivGPU `Software Licensed Product`.

15. (Opsional) Untuk membantu memanfaatkan satu layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

Amazon Linux 2

Untuk menginstal driver game NVIDIA pada instans Anda

1. Terhubung ke instans Anda. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
[ec2-user ~]$ sudo yum update -y
```

2. Install gcc dan make, jika belum terinstal.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Boot ulang untuk memuat versi kernel terbaru.

```
[ec2-user ~]$ sudo reboot
```

4. Sambungkan kembali ke instance Anda setelah di-boot ulang.
5. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Unduh utilitas instalasi driver game menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Beberapa versi driver game disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Ekstrak utilitas instalasi driver game dari `.zip` arsip yang diunduh.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

8. Tambahkan izin untuk menjalankan utilitas instalasi driver menggunakan perintah berikut:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Jalankan penginstal menggunakan perintah berikut:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Jika Anda menggunakan Amazon Linux 2 dengan kernel versi 5.10, gunakan perintah berikut untuk menginstal driver gaming NVIDIA.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

10. Gunakan perintah berikut untuk membuat file konfigurasi yang diperlukan.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Gunakan perintah berikut untuk mengunduh dan mengganti nama file sertifikasi.

    - Untuk versi 590.48 atau yang lebih baru:

    ```
    [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
    gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
    ```

    - Untuk versi 460.39 hingga 580.95:

    ```
    [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
    gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
    ```

    - Untuk versi 440.68 hingga 445.48:

    ```
    [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
    gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
    ```

    - Untuk versi sebelumnya:

    ```
    [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
    gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
    ```

12. Jika Anda menggunakan driver NVIDIA versi 510.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

14. Verifikasi lisensi NVIDIA Gaming menggunakan perintah berikut.

```
[ec2-user ~]$ nvidia-smi.exe -q
```

    Dalam output, carivGPU `Software Licensed Product`.

15. (Opsional) Untuk membantu memanfaatkan satu layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

CentOS 7 dan Red Hat Enterprise Linux 7

Untuk menginstal driver game NVIDIA pada instans Anda

1. Hubungkan dengan instans Linux Anda. Install gcc dan make, jika belum terinstal.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
[ec2-user ~]$ sudo yum update -y
```

3. Boot ulang untuk memuat versi kernel terbaru.

```
[ec2-user ~]$ sudo reboot
```

4. Hubungkan kembali ke instans Anda setelah boot ulang.
5. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Nonaktifkan driver `nouveau` sumber terbuka untuk kartu grafis NVIDIA.

a. Menambahkan nouveau ke file daftar hitam `/etc/modprobe.d/blacklist.conf`. Salin blok kode berikut dan tempelkan ke terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Edit file `/etc/default/grub` dan tambahkan baris berikut:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Bangun kembali konfigurasi Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Unduh utilitas instalasi driver game menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Beberapa versi driver game disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Ekstrak utilitas instalasi driver game dari `.zip` arsip yang diunduh.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Tambahkan izin untuk menjalankan utilitas instalasi driver menggunakan perintah berikut:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

10. Jalankan penginstal menggunakan perintah berikut:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

11. Gunakan perintah berikut untuk membuat file konfigurasi yang diperlukan.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Gunakan perintah berikut untuk mengunduh dan mengganti nama file sertifikasi.
    - Untuk versi 590.48 atau yang lebih baru:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
```

    - Untuk versi 460.39 hingga 580.95:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

    - Untuk versi 440.68 hingga 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Untuk versi sebelumnya:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Jika Anda menggunakan driver NVIDIA versi 510.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

14. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

15. (Opsional) Untuk membantu memanfaatkan satu layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah ini.

CentOS Stream 8 dan Red Hat Enterprise Linux 8

Untuk menginstal driver game NVIDIA pada instans Anda

1. Hubungkan dengan instans Linux Anda. Install gcc dan make, jika belum terinstal.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
[ec2-user ~]$ sudo yum update -y
```

3. Boot ulang untuk memuat versi kernel terbaru.

```
[ec2-user ~]$ sudo reboot
```

4. Hubungkan kembali ke instans Anda setelah boot ulang.
5. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Unduh utilitas instalasi driver game menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Beberapa versi driver game disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Ekstrak utilitas instalasi driver game dari `.zip` arsip yang diunduh.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Tambahkan izin untuk menjalankan utilitas instalasi driver menggunakan perintah berikut:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Jalankan penginstal menggunakan perintah berikut:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

   Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

10. Gunakan perintah berikut untuk membuat file konfigurasi yang diperlukan.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Gunakan perintah berikut untuk mengunduh dan mengganti nama file sertifikasi.
    - Untuk versi 590.48 atau yang lebih baru:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
```

    - Untuk versi 460.39 hingga 580.95:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

    - Untuk versi 440.68 hingga 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Untuk versi sebelumnya:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Jika Anda menggunakan driver NVIDIA versi 510.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

14. (Opsional) Untuk membantu memanfaatkan satu layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

Rocky Linux 8

Untuk menginstal driver game NVIDIA pada instans Anda

1. Hubungkan dengan instans Linux Anda. Install gcc dan make, jika belum terinstal.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
[ec2-user ~]$ sudo yum update -y
```

3. Boot ulang untuk memuat versi kernel terbaru.

```
[ec2-user ~]$ sudo reboot
```

4. Hubungkan kembali ke instans Anda setelah boot ulang.
5. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
[ec2-user ~]$ sudo dnf install -y unzip elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Unduh utilitas instalasi driver game menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Beberapa versi driver game disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Ekstrak utilitas instalasi driver game dari `.zip` arsip yang diunduh.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Tambahkan izin untuk menjalankan utilitas instalasi driver menggunakan perintah berikut:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Jalankan penginstal menggunakan perintah berikut:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

10. Gunakan perintah berikut untuk membuat file konfigurasi yang diperlukan.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Gunakan perintah berikut untuk mengunduh dan mengganti nama file sertifikasi.
    - Untuk versi 590.48 atau yang lebih baru:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
      ```

    - Untuk versi 460.39 hingga 580.95:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
      ```

    - Untuk versi 440.68 hingga 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Untuk versi sebelumnya:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Jika Anda menggunakan driver NVIDIA versi 510.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Boot ulang instans.

```
[ec2-user ~]$ sudo reboot
```

14. (Opsional) Untuk membantu memanfaatkan satu layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV.

Ubuntu dan Debian

Untuk menginstal driver game NVIDIA pada instans Anda

1. Hubungkan dengan instans Linux Anda. Install gcc dan make, jika belum terinstal.

```
$ sudo apt-get install -y gcc make build-essential
```

2. Perbarui cache paket Anda dan dapatkan pembaruan paket untuk instans Anda.

```
$ sudo apt-get update -y
```

3. Mutakhirkan paket `linux-aws` untuk menerima versi terbaru.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Boot ulang untuk memuat versi kernel terbaru.

```
$ sudo reboot
```

5. Hubungkan kembali ke instans Anda setelah boot ulang.
6. Instal paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
$ sudo apt install -y unzip dkms linux-headers-$(uname -r)
```

7. Nonaktifkan driver nouveau sumber terbuka untuk kartu grafis NVIDIA.

   a. Menambahkan nouveau ke file daftar hitam /etc/modprobe.d/blacklist.conf. Salin blok kode berikut dan tempelkan ke terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edit file /etc/default/grub dan tambahkan baris berikut:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Bangun kembali konfigurasi Grub.

```
$ sudo update-grub
```

8. Unduh utilitas instalasi driver game menggunakan perintah berikut:

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Beberapa versi driver game disimpan dalam bucket ini. Anda dapat melihat semua versi yang tersedia menggunakan perintah berikut:

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Ekstrak utilitas instalasi driver game dari .zip arsip yang diunduh.

```
$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Tambahkan izin untuk menjalankan utilitas instalasi driver menggunakan perintah berikut:

```
$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

11. Jalankan penginstal menggunakan perintah berikut:

```
$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

    Saat diminta, terima perjanjian lisensi dan tentukan opsi penginstalan yang diperlukan (Anda dapat menerima opsi default).

12. Gunakan perintah berikut untuk membuat file konfigurasi yang diperlukan.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Gunakan perintah berikut untuk mengunduh dan mengganti nama file sertifikasi.
    - Untuk versi 590.48 atau yang lebih baru:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
```

    - Untuk versi 460.39 hingga 580.95:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

    - Untuk versi 440.68 hingga 445.48:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Untuk versi sebelumnya:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Jika Anda menggunakan driver NVIDIA versi 510.x atau lebih tinggi pada instans G4dn, G5, atau G5G, nonaktifkan GSP dengan perintah berikut. Untuk informasi lebih lanjut tentang mengapa ini diperlukan, lihat dokumentasi NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

15. Boot ulang instans.

```
$ sudo reboot
```

16. (Opsional) Untuk membantu memanfaatkan satu layar hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah ini.

Sistem operasi Windows

Sebelum Anda menginstal driver game NVIDIA pada instans Anda, Anda harus memastikan bahwa prasyarat berikut terpenuhi selain pertimbangan yang disebutkan untuk semua driver game.

- Jika Anda meluncurkan instans Windows menggunakan AMI Windows kustom, AMI harus berupa gambar standar yang dibuat dengan Windows Sysprep untuk memastikan bahwa driver game berfungsi. Untuk informasi selengkapnya, lihat Buat Amazon EC2 AMI menggunakan Windows Sysprep.
- Konfigurasikan kredensyal default untuk instans AWS Tools for Windows PowerShell pada Windows Anda. Untuk informasi selengkapnya, lihat Memulai AWS Tools for Windows PowerShell di Panduan Pengguna.AWS Tools for PowerShell

Untuk menginstal driver game NVIDIA pada instans Windows Anda

1. Connect ke instance Windows Anda dan buka PowerShell jendela.
2. Unduh dan instal driver game menggunakan perintah PowerShell berikut ini.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
```

```
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
$LocalFilePath = Join-Path $LocalPath $LocalFileName
Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

Beberapa versi driver NVIDIA GRID disimpan dalam bucket S3 ini. Anda dapat mengunduh semua versi yang tersedia di bucket jika Anda mengubah nilai variabel `$KeyPrefix` dari “windows/latest” menjadi “windows”.

3. Arahkan ke desktop dan klik dua kali file instalasi untuk meluncurkannya (pilih versi driver yang sesuai dengan versi OS instans Anda). Ikuti petunjuk untuk menginstal driver dan mem-boot ulang instans Anda sesuai kebutuhan. Untuk memverifikasi bahwa GPU berfungsi dengan benar, periksa Device Manager.
4. Gunakan salah satu metode berikut untuk mendaftarkan driver.

   Version 527.27 or above

   Buat kunci registri berikut dengan versi 64-bit PowerShell, atau jendela Command Prompt.

   kunci: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

   nama: vGamingMarketplace

   jenis: DWord

   nilai: 2

   PowerShell

   Jalankan PowerShell perintah berikut untuk membuat nilai registri ini. AWS Tools for PowerShell Di AWS Windows AMIs default ke versi 32-bit dan perintah ini gagal. Sebagai gantinya, gunakan versi 64-bit yang PowerShell disertakan dengan sistem operasi.

   ```
   New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
    -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
   ```

Command Prompt

Jalankan perintah registri berikut untuk membuat nilai registri ini. Anda dapat menjalankannya menggunakan jendela Command Prompt atau versi 64-bit PowerShell.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
 vGamingMarketplace /t REG_DWORD /d 2
```

Earlier versions

Buat kunci registri berikut dengan versi 64-bit PowerShell, atau jendela Command Prompt.

kunci: `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

nama: vGamingMarketplace

jenis: DWord

nilai: 2

PowerShell

Jalankan PowerShell perintah berikut untuk membuat nilai registri ini. AWS Tools for PowerShell Di AWS Windows AMIs default ke versi 32-bit dan perintah ini gagal. Sebagai gantinya, gunakan versi 64-bit yang PowerShell disertakan dengan sistem operasi.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Command Prompt

Jalankan perintah registri berikut untuk membuat kunci registri ini dengan jendela Command Prompt. Anda juga dapat menggunakan perintah ini dalam versi 64-bitPowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Jalankan perintah berikut di PowerShell. Hal ini akan mengunduh file sertifikasi, mengganti nama file `GridSwCert.txt`, dan memindahkan file ke folder Dokumen Publik di drive sistem Anda. Biasanya, jalur foldernya adalah `C:\Users\Public\Documents`.

- Untuk versi 591.59 atau yang lebih baru:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert_2026_03_02.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

- Untuk versi 460.39 hingga 581.80:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCertWindows_2024_02_22.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

- Untuk versi 445.87:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

- Untuk versi sebelumnya:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016 atau yang lebih lama, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

6. Booting ulang instans Anda.
7. Temukan `nvidia-smi.exe` file pada instance.

```
Get-ChildItem -Path C:\ -Recurse -Filter "nvidia-smi.exe"
```

Verifikasi lisensi NVIDIA Gaming menggunakan perintah berikut. Ganti *`path`* dengan nama folder di output dari perintah sebelumnya.

```
C:\Windows\System32\DriverStore\FileRepository\path\nvidia-smi.exe -q
```

Output harus serupa dengan yang berikut ini.

```
vGPU Software Licensed Product
Product Name              : NVIDIA Cloud Gaming
License Status            : Licensed (Expiry: N/A)
```

8. (Opsional) Untuk membantu memanfaatkan tampilan tunggal hingga resolusi 4K, siapkan protokol tampilan berkinerja tinggi Amazon DCV. Jika Anda tidak memerlukan fungsionalitas ini, jangan selesaikan langkah ini.

Instal driver ENA pada instans EC2 Windows

Jika instans Anda tidak didasarkan pada salah satu Windows Amazon Machine Images (AMIs) terbaru yang disediakan Amazon, gunakan prosedur berikut untuk menginstal driver ENA saat ini pada instans Anda. Anda harus melakukan pembaruan ini pada saat yang tepat untuk mem-boot ulang instans Anda. Jika skrip penginstalan tidak secara otomatis me-reboot instans Anda, kami sarankan Anda me-reboot instans sebagai langkah terakhir.

Jika Anda menggunakan volume penyimpanan instans untuk menyimpan data saat instans berjalan, data tersebut akan dihapus saat Anda menghentikan instans. Sebelum Anda menghentikan instans Anda, verifikasi bahwa Anda telah menyalin data apa pun yang Anda perlukan dari volume penyimpanan instans Anda ke penyimpanan persisten, seperti Amazon EBS atau Amazon S3.

Prasyarat

Untuk menginstal atau meng-upgrade driver ENA, instans Windows Anda harus memenuhi prasyarat berikut ini:

- PowerShell versi 3.0 atau yang lebih baru diinstal.
- Perintah yang ditampilkan di bagian ini harus berjalan dalam versi 64-bitPowerShell. Jangan gunakan x86 versi PowerShell. Itu adalah versi 32-bit dari shell, dan tidak didukung untuk perintah ini.

Langkah 1: Mencadangkan data Anda

Kami menyarankan Anda membuat AMI cadangan, jika Anda tidak dapat mengembalikan perubahan Anda melalui Device Manager. Untuk membuat AMI cadangan dengan Konsol Manajemen AWS, ikuti langkah-langkah berikut:

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans yang memerlukan peningkatan driver, dan pilih Hentikan instans dari menu Status instans.
4. Setelah instans dihentikan, pilih instans lagi. Untuk membuat cadangan, pilih Gambar dan templat dari menu Tindakan, lalu pilih Buat gambar.
5. Untuk memulai ulang instans Anda, pilih Mulai instans dari menu status Instans.

Langkah 2: Menginstal atau meningkatkan driver ENA Anda

Anda dapat menginstal atau meningkatkan driver ENA Anda dengan AWS Systems Manager Distributor, atau dengan PowerShell cmdlet. Untuk petunjuk selengkapnya, pilih tab yang cocok dengan metode yang ingin Anda gunakan.

Systems Manager Distributor

Anda dapat menggunakan fitur Distributor Systems Manager untuk menyebarkan paket ke simpul terkelola Systems Manager Anda. Dengan Systems Manager Distributor, Anda dapat menginstal paket driver ENA satu kali, atau dengan pembaruan terjadwal. Untuk informasi selengkapnya tentang cara menginstal paket driver ENA (`AwsEnaNetworkDriver`) dengan Systems Manager Distributor, lihat Menginstal atau memperbarui paket di Panduan Pengguna AWS Systems Manager .

PowerShell

Bagian ini mencakup cara mengunduh dan menginstal paket driver ENA pada instance Anda dengan PowerShell cmdlet.

Opsi 1: Mengunduh dan mengekstraksi versi terbaru

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.
2. Gunakan cmdlet invoke-webrequest untuk mengunduh paket driver terbaru:

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016 atau yang lebih lama, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```
>
> Atau, Anda dapat mengunduh paket driver terbaru dari jendela browser di instans Anda.

3. Gunakan cmdlet expand-archive untuk mengekstrak arsip zip yang Anda unduh ke instans Anda:

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Opsi 2: Mengunduh dan mengekstraksi versi tertentu

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.
2. Unduh paket driver ENA untuk versi tertentu yang Anda inginkan dari tautan versi di tabel Riwayat versi driver ENA Windows.
3. Ekstrak arsip zip ke instans Anda.

Instal driver ENA dengan PowerShell

Langkah-langkah penginstalan sama apakah Anda telah mengunduh driver terbaru atau versi tertentu. Untuk menginstal driver ENA, ikuti langkah-langkah ini.

1. Untuk menginstal driver, jalankan `install.ps1` PowerShell skrip dari `AwsEnaNetworkDriver` direktori pada instance Anda. Jika Anda mendapatkan kesalahan, pastikan Anda menggunakan PowerShell 3.0 atau yang lebih baru.
2. Jika penginstal tidak secara otomatis me-reboot instance Anda, jalankan Restart-Computer PowerShell cmdlet.

```
PS C:\> Restart-Computer
```

Langkah 3 (opsional): Verifikasi versi driver ENA setelah instalasi

Untuk memastikan bahwa paket driver ENA berhasil diinstal pada instans Anda, Anda dapat memverifikasi versi baru sebagai berikut:

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.
2. Untuk membuka Windows Device Manager, masukkan `devmgmt.msc` di kotak Jalankan.
3. Pilih OKE. Ini membuka jendela Device Manager.
4. Pilih panah di sebelah kiri Adaptor jaringan untuk memperluas daftar.
5. Pilih nama, atau buka menu konteks untuk Adaptor Jaringan Elastis Amazon, lalu pilih Properti. Ini membuka dialog Properti Adaptor Jaringan Elastis Amazon.

> **Note**
>
> Adaptor ENA semua menggunakan driver yang sama. Jika Anda memiliki beberapa adaptor ENA, Anda dapat memilih salah satu dari mereka untuk memperbarui driver untuk semua adaptor ENA.

6. Untuk memverifikasi versi saat ini yang diinstal, buka tab Driver dan periksa Versi Driver. Jika versi saat ini tidak cocok dengan versi target Anda, lihat Memecahkan masalah driver Windows Adaptor Jaringan Elastis.

Putar kembali instalasi driver ENA

Jika ada yang salah dengan instalasi, Anda mungkin perlu memutar kembali driver. Ikuti langkah-langkah ini untuk memutar kembali ke versi driver ENA sebelumnya yang diinstal pada instans Anda.

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.

2. Untuk membuka Windows Device Manager, masukkan `devmgmt.msc` di kotak Jalankan.
3. Pilih OKE. Ini membuka jendela Device Manager.
4. Pilih panah di sebelah kiri Adaptor jaringan untuk memperluas daftar.
5. Pilih nama, atau buka menu konteks untuk Adaptor Jaringan Elastis Amazon, lalu pilih Properti. Ini membuka dialog Properti Adaptor Jaringan Elastis Amazon.

> **Note**
>
> Adaptor ENA semua menggunakan driver yang sama. Jika Anda memiliki beberapa adaptor ENA, Anda dapat memilih salah satu dari mereka untuk memperbarui driver untuk semua adaptor ENA.

6. Untuk memutar kembali driver, buka tab Driver dan pilih Roll Back Driver. Ini membuka jendela rollback Driver Package.

> **Note**
>
> Jika tab Driver tidak menampilkan tindakan Roll Back Driver, atau jika tindakan tidak tersedia, itu berarti bahwa Driver Store pada instans Anda tidak berisi paket driver yang diinstal sebelumnya. Untuk memecahkan masalah ini, lihat Skenario pemecahan masalah, dan perluas bagian yang diinstal versi driver ENA yang tidak terduga. Untuk informasi selengkapnya tentang proses pemilihan paket driver perangkat, lihat Cara Windows memilih paket driver untuk perangkat di situs web dokumentasi Microsoft.

Lacak rilis versi driver ENA Windows

Windows AMIs menyertakan driver ENA Windows untuk mengaktifkan jaringan yang ditingkatkan.

Untuk Windows Server versi 2016 dan di atasnya, kami sarankan Anda menggunakan versi driver terbaru. Untuk versi Windows Server sebelumnya, lihat tabel berikut untuk menentukan versi driver ENA mana yang akan digunakan.

Versi Windows Server	Versi driver ENA
Windows Server 2012 R2	2.6.0 dan sebelumnya
Windows Server 2012	2.6.0 dan sebelumnya

Versi Windows Server	Versi driver ENA
Windows Server 2008 R2	2.2.3 dan sebelumnya

Riwayat versi driver ENA Windows

Tabel berikut merangkum perubahan untuk setiap rilis.

Versi driver	Detail	Tanggal rilis
2.11.0	Fitur baru • Menambahkan dukungan untuk alokasi antrian dinamis dengan penskalaan hingga 64 I/O antrian, tunduk pada batas tipe instans. Perbaikan bug • Memperbaiki penanganan kondisi kesalahan yang hilang saat mengambil lebar alamat DMA fisik dari perangkat.	Agustus 1, 2025
2.10.0	Perbaikan bug • Memperbaiki penanganan kegagalan alokasi memori yang tidak tepat selama inisialisasi antrian untuk mencegah reboot yang tidak terduga. • Memperbaiki kemungkinan kesalahan konfigura si pembongkaran jaringan di mana kemampuan perangkat diabaikan.	Juni 24, 2025
2.9.0		Desember 12, 2024

Versi driver	Detail	Tanggal rilis
	Fitur baru • Menambahkan dukungan untuk permintaan reset asinkron yang dimulai oleh perangkat. • Menambahkan dukungan untuk menangani nilai kedalaman LLQ besar maksimum yang disediakan oleh perangkat. • Menambahkan ID Peristiwa `58001` di Windows Event Viewer untuk meningkatkan visibilitas ke transisi status daya tak terduga yang disebabkan oleh kesalahan konfigurasi perangkat. Perbaikan bug • Memperbaiki penanganan kegagalan alokasi memori yang tidak tepat selama inisialisasi perangkat untuk mencegah reboot yang tidak terduga. • Memperbaiki masalah dalam rutinitas layanan interupsi yang dapat mengantrekan DPC selama perangkat berhenti, mencegah reboot yang tidak terduga.	

Versi driver	Detail	Tanggal rilis
2.8.0	Perbaikan bug • Memperbaiki kondisi balapan dalam aliran lengkap pemrosesan daftar buffer jaringan keluar (NBL), yang dapat menyebabkan kerusakan memori yang disebabkan oleh upaya melepaskan NBL yang sudah dirilis. • Memperbaiki kesalahan deteksi protokol L3 saat menonaktifkan semua pembongkaran LSO dan checksum yang dapat menyebabkan perilaku tak terduga.	September 30, 2024

Versi driver	Detail	Tanggal rilis
2.7.0	Fitur baru • Dihapus dukungan untuk Windows Server 2012 (Windows 8) dan Windows Server 2012 R2 (Windows 8.1). Versi sistem operasi ini telah mencapai akhir dukungan dari AWS. Penginstalan driver akan gagal pada Windows Server 2012 dan sebelumnya. • Menambahkan dukungan untuk pembongkaran perhitungan checksum IPv6 Tx ke perangkat. • Menambahkan dukungan Low Latency Queuing (LLQ) yang luas. Ini diaktifkan secara dinamis berdasark an rekomendasi perangkat. Anda dapat mengganti pengaturan ini dengan kunci registri “WidellQ” yang baru. • Menambahkan pelaporan untuk penurunan paket yang dihasilkan dari Rx overrun, yang menunjukkan ruang yang tidak cukup di ring Rx untuk paket yang masuk. • Menambahkan dukungan untuk pemberitahuan konfigurasi suboptimal dari perangkat. Lihat ID peristiwa `59000` di penampil acara Windows. Perbaikan bug • Hindari reset perangkat yang tidak perlu yang disebabkan oleh paket Tx dengan header yang melebihi ukuran header Low Latency Queuing (LLQ) maksimum.	1 Mei 2024

Versi driver	Detail	Tanggal rilis

2.6.0	Fitur baru
	• Menambahkan metrik performa jaringan berikut untuk tipe instans yang mendukung ENA Ekspres.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Menambahkan metrik performa jaringan `conntrack_allowance_available` untuk tipe instans berbasis Nitro.
	• Menambahkan alasan reset adaptor baru karena deteksi kerusakan data RX.
	• Perbarui infrastruktur pencatatan driver.
	
	Perbaikan bug
	• Mencegah reset adaptor jika terjadi kelaparan CPU menyebabkan pembaruan metrik performa jaringan gagal.
	• Cegah deteksi palsu interupsi pada detak jantung perangkat.
	•
		20 Juni 2023

Versi driver	Detail	Tanggal rilis
	Memperbaiki skrip instalasi driver untuk mendukung operasi downgrade. • Memperbaiki statistik jumlah kesalahan penerimaan.	
2.5.0	Pengumuman ENA Windows driver versi 2.5.0 telah dibatalkan karena kegagalan untuk menginisialisasi pada pengontrol domain Windows. Windows Client dan Windows Server tidak terpengaruh.	17 Februari 2023

Versi driver	Detail	Tanggal rilis
2.4.0	Fitur baru • Menambahkan dukungan untuk Windows Server 2022. • Menghapus dukungan untuk Windows Server 2008 R2. • Menetapkan Low Latency Queuing (LLQ) agar selalu aktif untuk meningkatkan performa pada instans Amazon EC2 generasi keenam. Perbaikan bug • Memperbaiki kegagalan untuk mempublikasikan metrik performa jaringan ke sistem Penghitung Performa untuk Windows (PCW). • Memperbaiki kebocoran memori selama operasi pembacaan kunci registri. • Cegah loop reset tak terbatas jika terjadi kesalahan yang tidak dapat dipulihkan selama proses reset adaptor.	28 April 2022

Versi driver	Detail	Tanggal rilis
2.2.4	Pengumuman ENA Windows driver versi 2.2.4 telah dibatalkan karena potensi penurunan performa pada instans EC2 generasi keenam. Kami menyarankan Anda menurunkan versi driver, menggunakan salah satu metode berikut: • Instal versi sebelumnya 1. Unduh paket versi sebelumnya dari tautan di tabel ini (versi 2.2.3). 2. Jalankan skrip install.ps1 PowerShell instalasi. Untuk detail lebih lanjut untuk langkah-langkah sebelum dan sesudah instalasi lihat Mengaktifkan jaringan yang ditingkatkan di Windows. • Menggunakan Amazon EC2 Systems Manager untuk pembaruan massal • Lakukan pembaruan massal melalui dokumen `AWS-ConfigureAWSPackage` SSM, dengan parameter berikut: • Nama: AwsEnaNetworkDriver • Versi: 2.2.3	26 Oktober 2021

Versi driver	Detail	Tanggal rilis
2.2.3	Fitur baru • Menambahkan dukungan untuk kartu Nitro baru dengan jaringan instans 400 Gbps. Perbaikan bug • Memperbaiki kondisi balapan antara perubahan waktu sistem dan kueri waktu sistem oleh driver ENA, yang menyebabkan deteksi positif palsu dari tidak responsif nya HW. Pengumuman Driver Windows ENA versi 2.2.3 adalah versi final yang mendukung Windows Server 2008 R2. Saat ini tipe instans yang tersedia yang menggunakan ENA akan terus didukung pada Windows Server 2008 R2, dan driver tersedia dengan mengunduh. Tidak ada tipe instans masa depan yang akan mendukung Windows Server 2008 R2, dan Anda tidak dapat meluncurkan, mengimpor, atau memigrasi gambar Windows Server 2008 R2 ke tipe instans masa depan.	25 Maret 2021

Versi driver	Detail	Tanggal rilis
2.2.2	Fitur baru • Menambahkan dukungan ke metrik kinerja adaptor jaringan kueri dengan CloudWatch dan Penghitung Kinerja untuk konsumen Windows. Perbaikan bug • Memperbaiki masalah performa pada instans bare metal.	21 Desember 2020
2.2.1	Fitur baru • Tambahkan metode agar host bisa mengueri Elastic Network Adapter untuk metrik performa jaringan.	1 Oktober 2020

Versi driver	Detail	Tanggal rilis
2.2.0	Fitur baru • Menambahkan dukungan untuk tipe perangkat keras generasi selanjutnya. • Meningkatkan waktu mulai instans setelah melanjutkan dari stop-hibernate, dan menghapus pesan kesalahan ENA positif palsu. Optimalisasi performa • Mengoptimalkan pemrosesan lalu lintas masuk. • Meningkatkan manajemen memori bersama di lingkungan dengan sumber daya rendah. Perbaikan bug • Menghindari sistem crash saat penghapusan perangkat ENA dalam skenario yang jarang terjadi di mana driver gagal untuk mereset.	12 Agustus 2020
2.1.5	Perbaikan bug • Memperbaiki kegagalan inisialisasi adaptor jaringan yang sesekali terjadi pada instans bare metal.	23 Juni 2020

Versi driver	Detail	Tanggal rilis
2.1.4	Perbaikan bug • Mencegah masalah konektivitas yang disebabkan oleh metadata paket LSO yang rusak dari tumpukan jaringan. • Mencegah kerusakan sistem yang disebabkan oleh kondisi race langka yang mengakibatkan pengaksesan memori paket yang sudah dirilis.	25 November 2019
2.1.2	Fitur baru • Menambahkan dukungan untuk laporan ID vendor agar OS bisa menghasilkan UUIDs berbasis MAC. Perbaikan bug • Peningkatan performa konfigurasi jaringan DHCP selama inisialisasi. • Hitung checksum L4 dengan benar pada IPv6 lalu lintas masuk ketika unit transmisi maksimum (MTU) melebihi 4K. • Peningkatan umum untuk stabilitas driver dan perbaikan bug kecil.	4 November 2019

Versi driver	Detail	Tanggal rilis
2.1.1	Perbaikan bug • Mencegah penurunan paket TCP LSO yang sangat terfragmentasi, yang datang dari sistem operasi. • Menangani protokol Encapsulating Security Payload (ESP) dengan benar di dalam jaringan. IPSec IPv6	16 September 2019

Versi driver	Detail	Tanggal rilis

2.1.0	ENA Windows driver v2.1 memperkenalkan kapabilitas perangkat ENA baru, memberikan peningkatan performa, menambahkan fitur baru, dan memasukkan beberapa peningkatan stabilitas.
	
	Fitur baru
	
	• Menggunakan kunci registri Windows standar untuk konfigurasi frame Jumbo.
	• Mengizinkan pengaturan VLAN ID melalui GUI properti driver ENA.
	• Alur Pemulihan yang Ditingkatkan
	  • Mekanisme identifikasi kegagalan yang ditingkatkan.
	  • Menambahkan dukungan untuk parameter pemulihan yang bisa disesuaikan.
	• Support hingga 32 I/O antrian untuk instans EC2 yang lebih baru yang memiliki lebih dari 8 v. CPUs
	• ~90% pengurangan jejak memori driver.
	
	Optimalisasi performa
	
	• Penurunan latensi jalur transmisi.
	• Dukungan untuk menerima checksum offload.
	• Pengoptimalan performa untuk sistem dengan beban berat (penggunaan mekanisme penguncian yang dioptimalkan).
		1 Juli 2019

Versi driver	Detail	Tanggal rilis
	• Penyempurnaan lebih lanjut untuk mengurangi pemakaian CPU dan meningkatkan responsivitas sistem saat diberi beban. Perbaikan bug • Memperbaiki crash karena penguraian yang tidak valid dari header Tx yang tidak berdekatan. • Memperbaiki crash driver v1.5 selama pelepasan antarmuka jaringan elastis pada instans Bare Metal. • Memperbaiki error perhitungan checksum pseudo-he ader LSO di atas IPv6. • Memperbaiki potensi kebocoran sumber daya memori setelah kegagalan inisialisasi. • Nonaktifkan offload TCP/UDP checksum untuk IPv4 fragmen. • Memperbaiki konfigurasi VLAN. VLAN salah dinonakti fkan ketika hanya prioritas VLAN yang seharusnya dinonaktifkan. • Mengaktifkan penguraian yang benar dari pesan driver kustom oleh pelihat peristiwa. • Memperbaiki kegagalan untuk menginisialisasi driver karena penanganan stempel waktu yang tidak valid. • Memperbaiki kondisi race antara pemrosesan data dan penonaktifan perangkat ENA.	

Versi driver	Detail	Tanggal rilis
1.5.0	Pembaruan • Peningkatan stabilitas dan perbaikan performa. • Buffer Terima sekarang dapat dikonfigurasi hingga nilai 8192 di Properti Lanjutan ENA NIC. • Buffer Terima Default adalah 1k.	4 Oktober 2018
1.2.3	Mencakup perbaikan keandalan dan menyatukan dukungan untuk Windows Server 2008 R2 melalui Windows Server 2016.	13 Februari 2018
1.0.8	Rilis awal. Termasuk dalam AMIs untuk Windows Server 2008 R2, Windows Server 2012 RTM, Windows Server 2012 R2, dan Windows Server 2016.	Juli 2016

Berlangganan pemberitahuan rilis driver ENA Windows dari Amazon SNS

Amazon SNS dapat memberi Anda notifikasi saat EC2 Windows Drivers versi baru dirilis. Gunakan prosedur berikut untuk berlangganan notifikasi ini.

Berlangganan notifikasi EC2

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah ini karena notifikasi SNS langganan Anda ada di Wilayah ini.
3. Di panel navigasi, pilih Langganan.
4. Pilih Buat langganan.
5. Di kotak dialog Create subscription (Buat langganan), lakukan hal berikut:
    a. Untuk TopicARN, salin Amazon Resource Name (ARN) berikut:

arn:aws:sns:us-timur- 1:801119661308: ec2-windows-drivers

b. Untuk Protokol, pilih `Email`.

c. Untuk Endpoint, masukkan alamat email tempat Anda ingin notifikasi dikirim.

d. Pilih Buat langganan.

6. Anda akan menerima email konfirmasi. Buka email dan ikuti petunjuk untuk menyelesaikan langganan Anda.

Setiap kali driver EC2 Windows baru dirilis, kami mengirimkan notifikasi ke pelanggan. Jika Anda tidak ingin lagi menerima notifikasi ini, gunakan prosedur berikut untuk berhenti berlangganan.

Berhenti berlangganan dari notifikasi driver Windows Amazon EC2

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di panel navigasi, pilih Berlangganan.
3. Pilih kotak centang untuk langganan lalu pilih Tindakan, Hapus langganan. Ketika diminta konfirmasi, pilih Hapus.

Driver paravirtual untuk instans Windows

AMI Windows berisi seperangkat driver untuk mengizinkan akses ke perangkat keras tervirtualisasi. Driver ini digunakan oleh Amazon EC2 untuk memetakan penyimpanan instans dan volume Amazon EBS ke perangkat mereka. Tabel berikut menunjukkan perbedaan utama antara driver yang berbeda.

	Red Hat PV	Citrix PV	AWS PV
Tipe instans	Tidak didukung untuk semua tipe instans. Jika Anda menentukan tipe instans yang tidak didukung, instans tersebut akan mengalami gangguan.	Didukung untuk tipe instans Xen.	Didukung untuk tipe instans Xen.
Volume terlampir	Mendukung hingga 16 volume terlampir.	Mendukung lebih dari 16 volume terlampir.	Mendukung lebih dari

	Red Hat PV	Citrix PV	AWS PV
			16 volume terlampir.

	Red Hat PV	Citrix PV	AWS PV
Jaringan	Pengemudi memiliki masalah yang diketahui saat koneksi jaringan disetel ulang saat beban tinggi; misalnya, transfer file FTP yang cepat.		Pengemudi secara otomatis mengonfigurasi bingkai jumbo pada adaptor jaringan ketika pada tipe instans yang kompatibel. Ketika instance berada dalam grup penempatan cluster, ini menawarkan kinerja jaringan yang lebih baik antara instance yang ada di grup penempatan cluster. Untuk informasi selengkapnya, lihat Grup penempata

	Red Hat PV	Citrix PV	AWS PV
			n untuk EC2 instans Amazon Anda.

Tabel berikut menunjukkan driver PV mana yang harus Anda jalankan di setiap versi Windows Server di Amazon EC2.

Versi Windows Server	Versi driver PV
Windows Server 2025	Tidak didukung
Windows Server 2022	AWS PV versi terbaru
Windows Server 2019	AWS PV versi terbaru
Windows Server 2016	AWS PV versi terbaru
Windows Server 2012 R2	AWS PV versi 8.4.3
Windows Server 2012	AWS PV versi 8.4.3
Windows Server 2008 R2	AWS PV versi 8.3.5
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Daftar Isi

- AWS Driver PV
- Driver Citrix PV
- Pengemudi Red Hat PV
- Berlangganan notifikasi
- Tingkatkan driver PV pada instans EC2 Windows
- Memecahkan masalah driver PV pada instance Windows

AWS Driver PV

Driver AWS PV disimpan di `%ProgramFiles%\Amazon\Xentools` direktori. Direktori ini juga berisi simbol publik dan alat baris perintah`xenstore_client.exe`, yang memungkinkan Anda mengakses entri. XenStore Misalnya, PowerShell perintah berikut mengembalikan waktu saat ini dari Hypervisor:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Komponen driver AWS PV tercantum dalam registri Windows di bawah`HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services`. Komponen driver tersebut adalah sebagai berikut: xenbus, xeniface, xennet, xenvbd, dan xenvif.

AWS Driver PV juga memiliki layanan Windows bernama LiteAgent, yang berjalan dalam mode pengguna. Ini menangani tugas-tugas seperti shutdown dan restart peristiwa dari instance AWS APIs generasi Xen. Anda dapat mengakses dan mengelola layanan dengan menjalankan `Services.msc` dari baris perintah. Saat berjalan pada instance generasi Nitro, driver AWS PV tidak digunakan dan LiteAgent layanan akan berhenti sendiri dimulai dengan driver versi 8.2.4. Memperbarui ke driver AWS PV terbaru juga memperbarui LiteAgent dan meningkatkan keandalan pada semua generasi instans.

Instal driver AWS PV terbaru

AMI Amazon Windows berisi seperangkat driver untuk mengizinkan akses ke perangkat keras virtual. Driver ini digunakan oleh Amazon EC2 untuk memetakan penyimpanan instans dan volume Amazon EBS ke perangkat mereka. Kami menyarankan Anda menginstal driver terbaru untuk meningkatkan stabilitas dan performa instans EC2 Windows Anda.

Opsi instalasi

- Gunakan AWS Systems Manager untuk memperbarui driver PV secara otomatis. Untuk informasi selengkapnya, lihat Panduan: Memperbarui Driver PV Secara Otomatis pada Instans Windows EC2 di Panduan Pengguna.AWS Systems Manager
- Unduh paket driver dan jalankan program instal secara manual. Pastikan untuk memeriksa file `readme.txt` untuk mengetahui persyaratan sistem. Untuk informasi tentang mengunduh dan menginstal driver AWS PV, atau memutakhirkan kontroler domain, lihat Tingkatkan instans Windows Server (peningkatan AWS PV) secara manual.

AWS Riwayat paket driver PV

Tabel berikut menunjukkan perubahan driver AWS PV untuk setiap rilis driver.

Versi Package	Detail	Tanggal rilis
	• Perbaikan stabilitas untuk XenStore interaksi.	27 Mei 2025
8.5.0	• Perbaikan stabilitas untuk mengatasi kasus crash yang jarang terjadi selama detasemen perangkat jaringan. • Perbaikan stabilitas untuk mengatasi kasus crash yang jarang terjadi selama pelepasan volume EBS. • Memperbaiki bug di penginstal paket. • Memperbarui penginstal PV untuk digunakan`Pnputil`.	31 Oktober 2024
	Memperbaiki bug di penginstal paket untuk meningkatkan pengalaman pemutakhiran. Ini adalah versi terakhir yang dapat berjalan pada Windows Server 2012 dan 2012 R2. Versi ini tersedia untuk diunduh, namun tidak lagi didukung sejak Windows Server 2012 dan 2012 R2 telah mencapai akhir dukungan.	24 Januari 2023
8.4.2	Perbaikan stabilitas untuk mengatasi kondisi balapan.	13 April 2022
8.4.1	Penginstal paket yang ditingkatkan.	7 Januari 2022
8.4.0	• Perbaikan stabilitas untuk mengatasi kasus langka terjebak disk IO. • Perbaikan stabilitas untuk mengatasi kasus crash yang jarang terjadi selama pelepasan volume EBS. • Menambahkan fitur untuk mendistribusikan beban di banyak inti untuk beban kerja yang memanfaatkan lebih dari 20.000 IOPS dan mengalami degradasi akibat hambatan. Untuk mengaktifkan fitur ini, lihat Beban kerja yang memanfaatkan	2 Maret 2021

Versi Package	Detail	Tanggal rilis
	lebih dari 20.000 disk IOPS mengalami degradasi karena kemacetan CPU.	
8.3.5 8.3.5 8.3.5	Penginstal paket yang ditingkatkan. Ini adalah versi terakhir yang dapat berjalan di Windows Server 2008 R2. Versi ini tersedia untuk diunduh tetapi tidak lagi didukung. Windows Server 2008 R2 telah mencapai end-of-life, dan tidak lagi didukung oleh Microsoft.	7 Januari 2022
8.3.4	Peningkatan keandalan lampiran perangkat jaringan.	4 Agustus 2020
8.3.3	• Perbarui ke komponen yang XenStore menghadap ke -facing untuk mencegah pemeriksaan bug selama jalur penanganan kesalahan. • Perbarui ke komponen penyimpanan untuk menghindari kerusakan ketika SRB tidak valid dikirimkan. Untuk memperbarui driver ini pada instans Windows Server 2008 R2, Anda harus terlebih dahulu memverifikasi bahwa patch yang sesuai telah diinstal untuk mengatasi Microsoft Security Advisory berikut ini: Microsoft Security Advisory 3033929.	4 Februari 2020
8.3.2	Keandalan yang ditingkatkan dari komponen jaringan.	30 Juli 2019
8.3.1	Peningkatan kinerja dan ketahanan komponen penyimpanan.	12 Juni 2019
8.2.7	Peningkatan efisiensi untuk mendukung migrasi ke tipe instans generasi terbaru.	20 Mei 2019
8.2.6	Peningkatan efisiensi jalur dump kecelakaan.	15 Januari 2019

Versi Package	Detail	Tanggal rilis
8.2.5	Peningkatan keamanan tambahan. PowerShell installer sekarang tersedia dalam paket.	12 Desember 2018
8.2.4	Peningkatan keandalan.	2 Oktober 2018
8.2.3	Perbaikan bug dan peningkatan performa. Laporkan ID volume EBS sebagai nomor seri disk untuk volume EBS. Hal ini memungkinkan skenario klaster seperti S2D.	29 Mei 2018
8.2.1	Peningkatan kinerja jaringan dan penyimpanan ditambah beberapa perbaikan ketahanan. Untuk memverifikasi bahwa versi ini telah diinstal, lihat nilai registri Windows berikut ini: `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8 Maret 2018
7.4.3	Dukungan tambahan untuk Windows Server 2016. Perbaikan stabilitas untuk semua versi OS Windows yang didukung. * Tanda tangan driver AWS PV versi 7.4.3 berakhir pada 29 Maret 2019. Kami merekomendasikan memperbarui ke driver AWS PV terbaru.	18 November 2016
7.4.2	Perbaikan stabilitas untuk dukungan tipe instans X1.	2 Agu 2016
7.4.1	• Peningkatan kinerja pada driver AWS PV Storage. • Perbaikan stabilitas di driver AWS PV Storage: Memperbaiki masalah saat instance mengalami crash sistem dengan kode pemeriksaan bug 0x0000Dead. • Perbaikan stabilitas pada driver Jaringan AWS PV. • Menambahkan dukungan untuk Windows Server 2008R2.	12 Juli 2016

Versi Package	Detail	Tanggal rilis
7.3.2	• Peningkatan logging dan diagnostik. • Perbaikan stabilitas pada driver AWS PV Storage. Dalam beberapa kasus, disk mungkin tidak muncul di Windows setelah menyambungkan kembali disk ke instans. • Menambahkan dukungan untuk Windows Server 2012.	24 Juni 2015
7.3.1	Pembaruan TRIM: Perbaikan terkait dengan permintaan TRIM. Perbaikan ini menstabilkan instans dan meningkatkan kinerja instans saat mengelola permintaan TRIM dalam jumlah besar.	
7.3.0	Dukungan TRIM: Driver AWS PV sekarang mengirimkan permintaan TRIM ke hypervisor. Disk efemeral akan memproses permintaan TRIM dengan benar karena penyimpanan yang mendasarinya mendukung TRIM (SSD). Perhatikan bahwa penyimpanan berbasis EBS tidak mendukung TRIM mulai Maret 2015.	
7.2.5	• Perbaikan stabilitas pada driver AWS PV Storage: Dalam beberapa kasus driver AWS PV dapat menurunkan memori yang tidak valid dan menyebabkan kegagalan sistem. • Perbaikan stabilitas saat menghasilkan crash dump: Dalam beberapa kasus pengemudi AWS PV bisa terjebak dalam kondisi balapan saat menulis crash dump. Sebelum rilis ini, masalah hanya dapat diatasi dengan memaksa driver untuk berhenti dan memulai ulang yang dapat menyebabkan hilangnya timbunan memori.	
7.2.4	Persistensi ID Perangkat: Perbaikan driver ini menutupi ID perangkat PCI platform dan memaksa sistem untuk selalu memunculkan ID perangkat yang sama, meskipun instans dipindahkan. Secara lebih umum, perbaikan memengaruhi cara hypervisor menampilkan perangkat virtual. Perbaikan ini juga mencakup modifikasi pada co-installer untuk driver AWS PV sehingga sistem tetap dipetakan perangkat virtual.	

Versi Package	Detail	Tanggal rilis
7.2.2	• Muat driver AWS PV dalam mode Directory Services Restore Mode (DSRM): Directory Services Restore Mode adalah opsi boot mode aman untuk pengontrol domain Windows Server. • Menjaga ID perangkat tetap ada ketika perangkat adaptor jaringan virtual terpasang kembali: Perbaikan ini memaksa sistem untuk memeriksa pemetaan alamat MAC dan mempertahankan ID perangkat. Perbaikan ini memastikan bahwa adaptor mempertahankan pengaturan statisnya jika adaptor dipasang kembali.	
7.2.1	• Jalankan di mode aman: Memperbaiki masalah di mana driver tidak mau memuat dalam mode aman. Sebelumnya Driver AWS PV hanya akan membuat instance dalam sistem yang berjalan normal. • Tambahkan disk ke Microsoft Windows Storage Pools: Sebelumnya kami menyintesis kueri halaman 83. Perbaikan menonaktifkan dukungan halaman 83. Perhatikan bahwa ini tidak memengaruhi kolam penyimpanan yang digunakan di lingkungan klaster karena disk PV bukan disk klaster yang valid.	
7.2.0	Basis: Versi dasar AWS PV.	

Driver Citrix PV

Driver Citrix PV disimpan di driektori `%ProgramFiles%\Citrix\XenTools` (instans 32-bit) atau `%ProgramFiles(x86)%\Citrix\XenTools` (64-bit instans).

Komponen driver Citrix PV tercantum dalam registri Windows di bawah `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`. Komponen driver tersebut adalah sebagai berikut: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd, and xenvif.

Citrix juga memiliki komponen driver bernama XenGuestAgent, yang berjalan sebagai layanan Windows. Layanan ini menangani tugas-tugas seperti mematikan dan memulai ulang peristiwa dari

API. Anda dapat mengakses dan mengelola layanan dengan menjalankan `Services.msc` dari baris perintah.

Jika Anda mengalami kesalahan jaringan saat melakukan beban kerja tertentu, Anda mungkin perlu menonaktifkan fitur pemindahan TCP untuk driver Citrix PV. Untuk informasi selengkapnya, lihat Pemindahan TCP.

Pengemudi Red Hat PV

Driver Red Hat didukung untuk instans lama, tetapi tidak direkomendasikan pada instans yang lebih baru dengan RAM lebih dari 12GB karena keterbatasan driver. Instans dengan RAM lebih dari 12GB yang menjalankan driver Red Hat dapat gagal untuk boot dan menjadi tidak dapat diakses. Kami merekomendasikan untuk meningkatkan driver Red Hat ke driver Citrix PV, dan kemudian meng-upgrade driver Citrix PV ke driver PV. AWS

File sumber untuk driver Red Hat ada di direktori `%ProgramFiles%\RedHat` (instance 32-bit) atau `%ProgramFiles(x86)%\RedHat` (instance 64-bit). Kedua driver tersebut adalah`rhelnet`, driver jaringan Red Hat Paravirtualized`rhelscsi`, dan driver miniport Red Hat SCSI.

Berlangganan notifikasi

Amazon SNS dapat memberi Anda notifikasi saat EC2 Windows Drivers versi baru dirilis. Anda dapat berlangganan notifikasi ini.

> **Note**
>
> Anda harus menentukan Wilayah tempat topik SNS dibuat.

Setiap kali driver EC2 Windows baru dirilis, kami mengirimkan notifikasi ke pelanggan. Jika Anda tidak lagi ingin menerima pemberitahuan ini, Anda dapat berhenti berlangganan. Untuk informasi selengkapnya, lihat Menghapus topik dan langganan SNS.

Console

Untuk berlangganan notifikasi

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah ini karena notifikasi SNS langganan Anda ada di Wilayah ini.

3. Di panel navigasi, pilih Langganan.
4. Pilih Buat langganan.
5. Di kotak dialog Create subscription (Buat langganan), lakukan hal berikut:
   a. Untuk TopicARN, salin Amazon Resource Name (ARN) berikut:

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Untuk Protokol, pilih `Email`.
   c. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi.
   d. Pilih Buat langganan.
6. Anda akan menerima email konfirmasi. Buka email dan ikuti petunjuk untuk menyelesaikan langganan Anda.

AWS CLI

Untuk berlangganan notifikasi

Gunakan perintah berikut ini.

```
aws sns subscribe \
    --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers \
    --region us-east-1 \
    --protocol email \
    --notification-endpoint YourUserName@YourDomainName.ext
```

PowerShell

Untuk berlangganan notifikasi

Gunakan perintah berikut ini.

```
Connect-SNSNotification `
    -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers' `
    -Region us-east-1 `
    -Protocol email `
    -Endpoint "YourUserName@YourDomainName.ext"
```

Tingkatkan driver PV pada instans EC2 Windows

Kami menyarankan Anda menginstal driver PV terbaru untuk meningkatkan stabilitas dan performa instans EC2 Windows Anda. Petunjuk di halaman ini membantu Anda mengunduh paket driver dan menjalankan program penginstalan.

Untuk memverifikasi driver mana yang digunakan instans Windows Anda

Buka Device Manager dan lihat Network Adapters. Periksa apakah driver PV adalah salah satu dari yang berikut:

- AWS Perangkat Jaringan PV
- Adaptor Ethernet Citrix PV
- Pengemudi Red Hat PV NIC

Persyaratan sistem

Pastikan untuk memeriksa file `readme.txt` di unduhan untuk mengetahui persyaratan sistem.

Daftar Isi

- Tingkatkan instans Windows Server (peningkatan AWS PV) dengan Distributor
- Tingkatkan instans Windows Server (peningkatan AWS PV) secara manual
- Tingkatkan pengontrol domain (peningkatan AWS PV)
- Tingkatkan instans Windows Server 2008 dan 2008 R2 (peningkatan Red Hat ke Citrix PV)
- Mutakhirkan layanan agen tamu Citrix Xen Anda

Tingkatkan instans Windows Server (peningkatan AWS PV) dengan Distributor

Anda dapat menggunakan Distributor, kemampuan AWS Systems Manager, untuk menginstal atau meng-upgrade paket driver AWS PV. Instalasi atau peningkatan dapat dilakukan satu kali, atau Anda dapat menginstal atau memperbaruinya sesuai jadwal. `In-place update`Opsi untuk Jenis Instalasi tidak didukung untuk paket Distributor ini.

> **Important**
>
> Jika instans Anda adalah kontroler domain, lihat Tingkatkan pengontrol domain (peningkatan AWS PV). Proses pemutakhiran versi untuk instans kontroler domain berbeda dari edisi standar Windows.

1. Kami menyarankan Anda membuat cadangan jika Anda perlu memutar kembali perubahan Anda.

   > **Tip**
   >
   > Alih-alih membuat AMI dari konsol Amazon EC2, Anda dapat menggunakan Systems Manager Automation untuk membuat AMI menggunakan runbook. `AWS-CreateImage` Untuk informasi selengkapnya, lihat AWS-CreateImagedi Panduan Pengguna referensi buku runbook AWS Systems Manager Otomasi.

   a. Ketika Anda menghentikan suatu instans, data pada setiap instans volume penyimpanan akan dihapus. Sebelum Anda menghentikan sebuah instans, pastikan bahwa Anda telah menyalin data apa pun yang Anda perlukan dari volume penyimpanan instans ke penyimpanan persisten, seperti Amazon EBS atau Amazon S3.

   b. Di panel navigasi, pilih Contoh.

   c. Pilih instans yang memerlukan pemutakhiran driver, dan pilih Status instans, Hentikan instans.

   d. Setelah instans dihentikan, pilih instans, pilih Tindakan, lalu Gambar dan templat, lalu pilih Buat gambar.

   e. Pilih Status instans, Mulai instans.

2. Hubungkan ke instans menggunakan Desktop Jarak Jauh. Untuk informasi selengkapnya, lihat the section called “Connect menggunakan klien RDP”.

3. Kami menyarankan Anda untuk membuat semua disk non-sistem offline dan mencatat setiap pemetaan huruf drive ke disk sekunder di Manajemen Disk sebelum Anda melakukan pemutakhiran ini. Langkah ini tidak diperlukan jika Anda melakukan pembaruan driver AWS PV di tempat. Kami juga merekomendasikan pengaturan layanan yang tidak penting ke start-up Manual di konsol Layanan.

4. Untuk petunjuk cara menginstal atau meng-upgrade paket driver AWS PV menggunakan Distributor, lihat prosedur di Menginstal atau memperbarui paket di Panduan AWS Systems Manager Pengguna.
5. Untuk Nama, pilih AWSPVDriver.
6. Untuk jenis Instalasi, pilih Uninstall dan instal ulang.
7. Konfigurasikan parameter lain untuk paket seperlunya dan jalankan instalasi atau tingkatkan menggunakan prosedur yang direferensikan diStep 4.

   Setelah menjalankan paket Distributor, instance secara otomatis reboot dan kemudian meningkatkan driver. Instans tidak akan tersedia hingga 15 menit.
8. Setelah pemutakhiran selesai, dan instans melewati kedua pemeriksaan kesehatan di konsol Amazon EC2, verifikasi bahwa driver baru telah diinstal dengan menghubungkan ke instans menggunakan Remote Desktop.
9. Setelah Anda terhubung, jalankan PowerShell perintah berikut:

   ```
   Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
   ```
10. Pastikan versi driver sama dengan versi terbaru yang terdaftar pada tabel Riwayat Versi Driver. Untuk informasi selengkapnya, lihat AWS Riwayat paket driver PV Buka Manajemen Disk untuk meninjau volume sekunder offline apa pun dan membawanya online sesuai dengan huruf drive yang tercantum dalamStep 3.

Jika sebelumnya Anda dinonaktifkan Pemindahan TCP menggunakan Netsh untuk driver PV Citrix, kami sarankan Anda mengaktifkan kembali fitur ini setelah memutakhirkan ke driver PV. AWS Masalah pembongkaran TCP dengan driver Citrix tidak ada di driver PV. AWS Hasilnya, TCP Offloading memberikan kinerja yang lebih baik dengan driver AWS PV.

Jika sebelumnya Anda menerapkan alamat IP statis atau konfigurasi DNS ke antarmuka jaringan, Anda mungkin perlu menerapkan kembali alamat IP statis atau konfigurasi DNS setelah memutakhirkan AWS driver PV.

Tingkatkan instans Windows Server (peningkatan AWS PV) secara manual

Gunakan prosedur berikut untuk melakukan peningkatan driver AWS PV di tempat, atau untuk meningkatkan dari driver Citrix PV ke driver AWS PV pada Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, atau Windows

Server 2022. Upgrade ini tidak tersedia untuk driver Red Hat, atau untuk versi Windows Server lainnya.

Beberapa versi Windows Server sebelumnya tidak dapat menggunakan driver terbaru. Untuk memverifikasi versi driver mana yang akan digunakan untuk sistem operasi Anda, lihat tabel versi driver di halaman Driver paravirtual untuk instans Windows.

> **Important**
>
> Jika instans Anda adalah kontroler domain, lihat Tingkatkan pengontrol domain (peningkatan AWS PV). Proses pemutakhiran versi untuk instans kontroler domain berbeda dari edisi standar Windows.

Untuk memutakhirkan driver AWS PV secara manual

1. Kami menyarankan Anda membuat cadangan jika Anda perlu memutar kembali perubahan Anda.

   > **Tip**
   >
   > Alih-alih membuat AMI dari konsol Amazon EC2, Anda dapat menggunakan Systems Manager Automation untuk membuat AMI menggunakan runbook. `AWS-CreateImage` Untuk informasi selengkapnya, lihat AWS-CreateImagedi Panduan Pengguna referensi buku runbook AWS Systems Manager Otomasi.

   a. Ketika Anda menghentikan suatu instans, data pada setiap instans volume penyimpanan akan dihapus. Sebelum Anda menghentikan sebuah instans, pastikan bahwa Anda telah menyalin data apa pun yang Anda perlukan dari volume penyimpanan instans ke penyimpanan persisten, seperti Amazon EBS atau Amazon S3.

   b. Di panel navigasi, pilih Contoh.

   c. Pilih instans yang memerlukan pemutakhiran driver, dan pilih Status instans, Hentikan instans.

   d. Setelah instans dihentikan, pilih instans, pilih Tindakan, lalu Gambar dan templat, lalu pilih Buat gambar.

   e. Pilih Status instans, Mulai instans.

2. Hubungkan ke instans menggunakan Desktop Jarak Jauh.
3. Kami menyarankan Anda untuk membuat semua disk non-sistem offline dan mencatat setiap pemetaan huruf drive ke disk sekunder di Manajemen Disk sebelum Anda melakukan pemutakhiran ini. Langkah ini tidak diperlukan jika Anda melakukan pembaruan driver AWS PV di tempat. Kami juga merekomendasikan pengaturan layanan yang tidak penting ke start-up Manual di konsol Layanan.
4. Unduh driver ke instans Anda menggunakan salah satu opsi berikut:
   - Browser — https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/Latest/AWSPVDriver.zip paket driver terbaru ke instance dan ekstrak arsip zip.
   - PowerShell— Jalankan perintah berikut:

     ```
     Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
     Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath $env:userprofile\pv_drivers
     ```

     Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016 atau sebelumnya, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:

     ```
     [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
     ```
5. Jalankan `AWSPVDriverSetup.msi`.

Setelah menjalankan MSI, instans secara otomatis melakukan boot ulang kemudian memutakhirkan driver. Instance tidak akan tersedia hingga 15 menit. Setelah pemutakhiran selesai dan instans melewati kedua pemeriksaan kesehatan di konsol Amazon EC2, Anda dapat memverifikasi bahwa driver baru telah diinstal dengan menghubungkan ke instance menggunakan Remote Desktop dan kemudian menjalankan perintah berikut: PowerShell

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Pastikan versi driver sama dengan versi terbaru yang terdaftar pada tabel Riwayat Versi Driver. Untuk informasi selengkapnya, lihat AWS Riwayat paket driver PV Buka Manajemen Disk untuk meninjau volume sekunder offline apa pun dan membawanya online sesuai dengan huruf drive yang tercantum dalamStep 3.

Jika sebelumnya Anda dinonaktifkan Pemindahan TCP menggunakan Netsh untuk driver PV Citrix, kami sarankan Anda mengaktifkan kembali fitur ini setelah memutakhirkan ke driver PV. AWS Masalah pembongkaran TCP dengan driver Citrix tidak ada di driver PV. AWS Hasilnya, TCP Offloading memberikan kinerja yang lebih baik dengan driver AWS PV.

Jika sebelumnya Anda menerapkan alamat IP statis atau konfigurasi DNS ke antarmuka jaringan, Anda mungkin perlu menerapkan kembali alamat IP statis atau konfigurasi DNS setelah memutakhirkan AWS driver PV.

Tingkatkan pengontrol domain (peningkatan AWS PV)

Gunakan prosedur berikut pada pengontrol domain untuk melakukan peningkatan driver AWS PV di tempat, atau untuk meningkatkan dari driver Citrix PV ke AWS driver PV. Untuk memastikan bahwa peran FSMO Anda tetap beroperasi selama pemutakhiran, sebaiknya Anda mentransfer peran tersebut ke pengontrol domain lain sebelum memulai pemutakhiran. Untuk informasi selengkapnya, lihat Cara melihat dan mentransfer peran FSMO di situs web Microsoft Learn.

Untuk meningkatkan kontroler domain

1. Kami menyarankan agar Anda membuat cadangan kontroler domain jika Anda perlu mengembalikan perubahan Anda. Menggunakan AMI sebagai cadangan tidak didukung. Untuk informasi selengkapnya, lihat Backup dan restore pertimbangan dalam dokumentasi Microsoft.
2. Jalankan perintah berikut untuk mengonfigurasi Windows agar booting ke Mode Pemulihan Layanan Direktori (DSRM).

   > **Warning**
   >
   > Sebelum menjalankan perintah ini, konfirmasikan bahwa Anda mengetahui kata sandi DSRM. Anda akan memerlukan informasi ini agar Anda dapat masuk ke instans setelah pemutakhiran versi selesai dan instans di-boot ulang secara otomatis.

   ```
   bcdedit /set {default} safeboot dsrepair
   ```

   PowerShell:

   ```
   PS C:\> bcdedit /set "{default}" safeboot dsrepair
   ```

Sistem harus boot ke DSRM karena utilitas upgrade menghapus driver penyimpanan Citrix PV sehingga dapat menginstal driver PV. AWS Oleh karena itu kami menyarankan untuk mencatat pemetaan huruf dan folder drive apa pun ke disk sekunder di Manajemen Disk. Jika driver penyimpanan Citrix PV tidak ada, drive sekunder tidak terdeteksi. Kontroler domain yang menggunakan folder NTDS di drive sekunder tidak akan bisa di-boot karena disk sekunder tidak terdeteksi.

> **Warning**
>
> Setelah Anda menjalankan perintah ini, jangan boot ulang sistem secara manual. Sistem tidak dapat dijangkau karena driver Citrix PV tidak mendukung DSRM.

3. Jalankan perintah berikut untuk ditambahkan **`DisableDCCheck`** ke pendataan ini:

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
 REG_SZ /d true
```

4. Unduh paket driver terbaru ke instance dan ekstrak arsip zip.
5. Jalankan `AWSPVDriverSetup.msi`.

   Setelah menjalankan MSI, instans secara otomatis melakukan boot ulang kemudian memutakhirkan driver. Instans tidak akan tersedia hingga 15 menit.
6. Setelah pemutakhiran selesai dan instans melewati kedua pemeriksaan kondisi di konsol Amazon EC2, hubungkan ke instans menggunakan Remote Desktop. Buka Manajemen Disk untuk meninjau volume sekunder offline dan membuatnya online sesuai dengan huruf drive dan pemetaan folder yang disebutkan sebelumnya.

   Anda harus terhubung ke instance dengan menentukan nama pengguna dalam format berikut hostname\ administrator. Misalnya, Win2k12TestBox\ administrator.
7. Jalankan perintah berikut untuk menghapus konfigurasi boot DSRM:

```
bcdedit /deletevalue safeboot
```

8. Boot ulang instans.
9. Untuk menyelesaikan proses pemutakhiran, pastikan bahwa driver baru telah diinstal. Di Pengelola Perangkat, di bawah Kontroler Penyimpanan, temukan Adaptor Host Penyimpanan

AWS PV. Pastikan versi driver sama dengan versi terbaru yang terdaftar pada tabel Riwayat Versi Driver. Untuk informasi selengkapnya, lihat AWS Riwayat paket driver PV.

10. Jalankan perintah berikut untuk menghapus **`DisableDCCheck`** dari pendataan ini:

```
reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
```

> **Note**
>
> Jika sebelumnya Anda dinonaktifkan Pemindahan TCP menggunakan Netsh untuk driver PV Citrix, kami sarankan Anda mengaktifkan kembali fitur ini setelah memutakhirkan ke Driver PV. AWS Masalah pembongkaran TCP dengan driver Citrix tidak ada di driver PV. AWS Hasilnya, TCP Offloading memberikan kinerja yang lebih baik dengan driver AWS PV.

Tingkatkan instans Windows Server 2008 dan 2008 R2 (peningkatan Red Hat ke Citrix PV)

Sebelum Anda mulai meningkatkan driver Red Hat Anda ke driver Citrix PV, pastikan Anda melakukan hal berikut:

- Instal versi terbaru dari layanan EC2 Config. Untuk informasi selengkapnya, lihat Instal EC2 Config versi terbaru.
- Verifikasi bahwa Anda telah menginstal Windows PowerShell 3.0. Untuk memverifikasi versi yang telah Anda instal, jalankan perintah berikut di file PowerShell jendela:

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  Windows PowerShell 3.0 dibundel dalam paket instalasi Windows Management Framework (WMF) versi 3.0. Jika Anda perlu menginstal Windows PowerShell 3.0, lihat Windows Management Framework 3.0 di Pusat Unduhan Microsoft.
- Cadangkan informasi penting Anda pada instans, atau buat AMI dari instans. Untuk informasi selengkapnya tentang cara membuat AMI, lihat Buat AMI yang didukung Amazon EBS-Backed.

> **Tip**
>
> Alih-alih membuat AMI dari konsol Amazon EC2, Anda dapat menggunakan Systems Manager Automation untuk membuat AMI menggunakan runbook. `AWS-CreateImage`

Untuk informasi selengkapnya, lihat AWS-CreateImagedi Panduan Pengguna referensi buku runbook AWS Systems Manager Otomasi.

Jika Anda membuat AMI, pastikan Anda melakukan hal berikut:

- Tuliskan kata sandi Anda.
- Jangan menjalankan alat Sysprep secara manual atau menggunakan layanan Config EC2.
- Setel adaptor Ethernet Anda untuk mendapatkan alamat IP secara otomatis menggunakan DHCP.

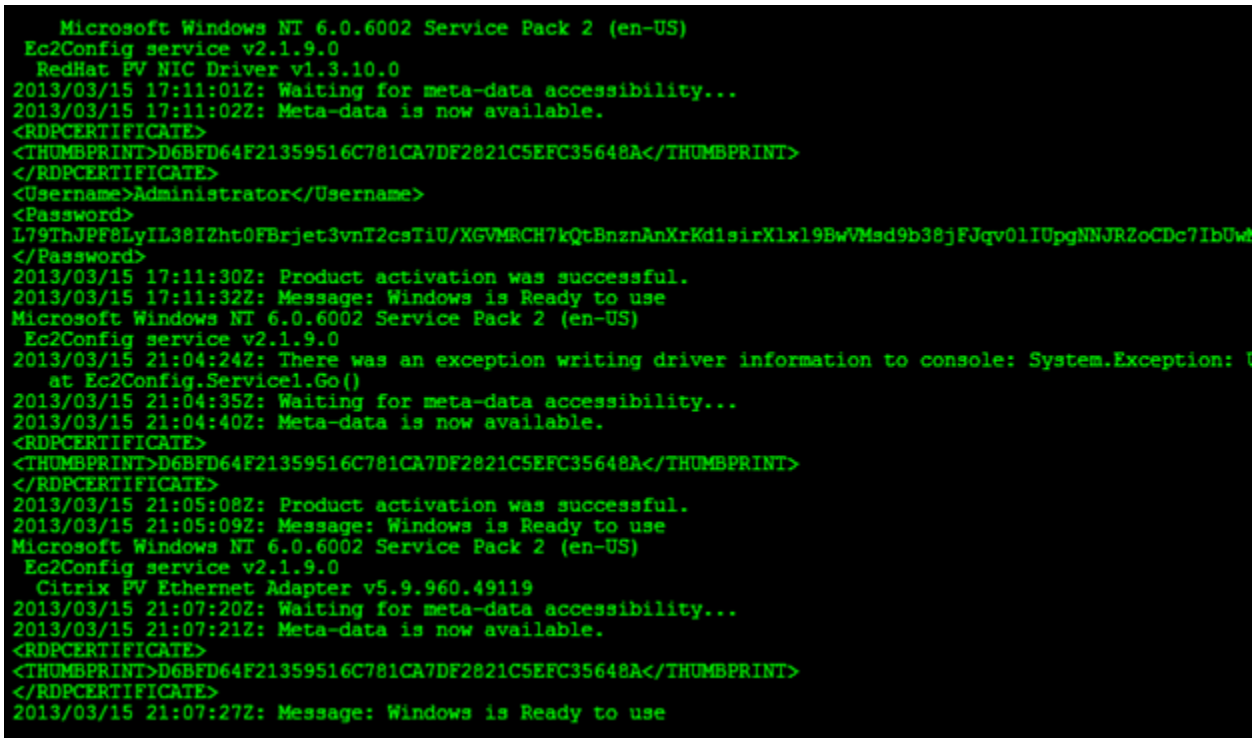
Untuk meningkatkan driver Red Hat

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal. Untuk informasi selengkapnya tentang menghubungkan ke instans Anda, lihat Hubungkan ke instans Windows Anda menggunakan RDP.
2. Dalam instans Anda, unduh paket pemutakhiran Citrix PV.
3. Ekstrak konten paket yang dimutakhirkan ke lokasi pilihan Anda.
4. Klik dua kali file Upgrade.bat. Jika Anda mendapatkan peringatan keamanan, pilih Jalankan.
5. Di kotak dialog Tingkatkan Driver, tinjau informasinya dan pilih Ya jika Anda siap untuk memulai peningkatan.
6. Di kotak dialog Red Hat Paravirtualized Xen Drivers untuk Windows uninstaller, pilih Ya untuk menghapus perangkat lunak Red Hat. Instans Anda akan di-boot ulang.

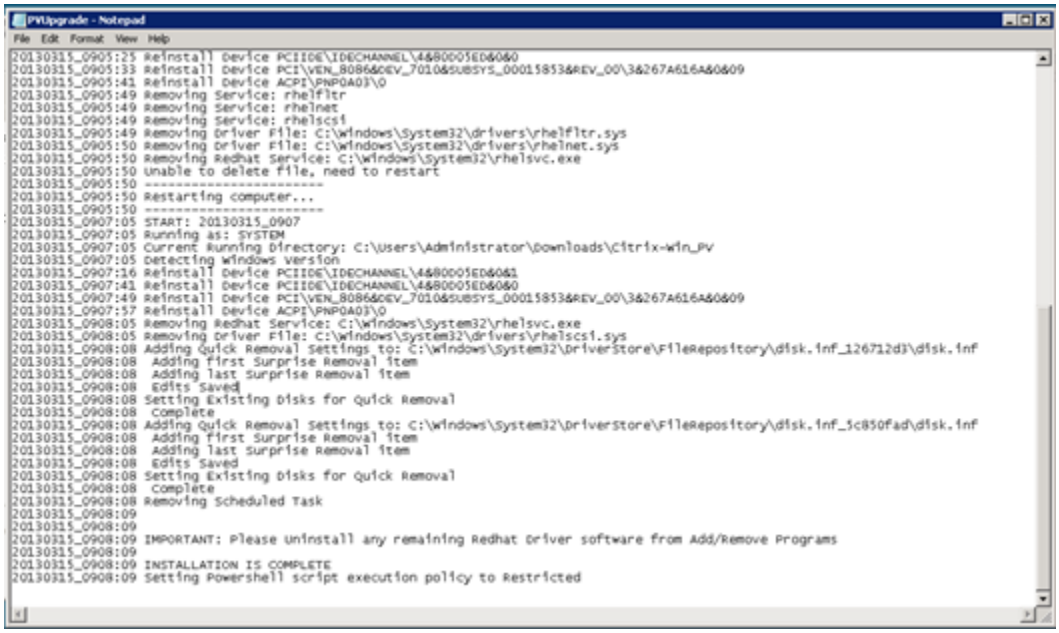
> **Note**
>
> Jika Anda tidak melihat kotak dialog uninstaller, pilih Red Hat Paravirtualize di taskbar Windows.

7. Periksa apakah instans telah di-boot ulang dan siap digunakan.
   a. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
   b. Pada halaman Instans, pilih Tindakan, lalu Pantau dan pecahkan masalah, lalu pilih Dapatkan log sistem.

c. Operasi pemutakhiran harus memulai ulang server 3 atau 4 kali. Anda dapat melihat ini di file log dengan berapa kali `Windows is Ready to use` ditampilkan.



8. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.
9. Tutup kotak dialog Red Hat Paravirtualized Xen Drivers untuk pelepas instalasi Windows.
10. Konfirmasikan bahwa penginstalan selesai. Arahkan ke folder `Citrix-WIN_PV` yang Anda ekstrak sebelumnya, buka file `PVUpgrade.log`, lalu centang teks `INSTALLATION IS COMPLETE`.



Mutakhirkan layanan agen tamu Citrix Xen Anda

Jika Anda menggunakan driver Citrix PV di Windows Server, Anda dapat memutakhirkan layanan agen tamu Citrix Xen. Layanan Windows menangani tugas-tugas seperti mematikan dan memulai ulang peristiwa dari API. Anda dapat menjalankan paket pemutakhiran ini di versi Windows Server apa pun, selama instans menjalankan driver Citrix PV.

> **Important**
>
> Untuk Windows Server 2008 R2 dan yang lebih baru, kami sarankan Anda meningkatkan ke driver AWS PV yang menyertakan pembaruan Agen Tamu.

Sebelum Anda mulai memutakhirkan driver, pastikan Anda mencadangkan informasi penting pada instans, atau buat AMI dari instans. Untuk informasi selengkapnya tentang membuat AMI, lihat Buat AMI yang didukung Amazon EBS-Backed.

> **Tip**
>
> Alih-alih membuat AMI dari konsol Amazon EC2, Anda dapat menggunakan Systems Manager Automation untuk membuat AMI menggunakan runbook. `AWS-CreateImage`

Untuk informasi selengkapnya, lihat AWS-CreateImagedi Panduan Pengguna referensi buku runbook AWS Systems Manager Otomasi.

Jika Anda membuat AMI, pastikan Anda melakukan hal berikut:

- Jangan aktifkan alat Sysprep di layanan Config EC2.
- Tuliskan kata sandi Anda.
- Setel adaptor Ethernet Anda ke DHCP.

Untuk meningkatkan layanan agen tamu Citrix Xen Anda

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal. Untuk informasi selengkapnya tentang menghubungkan ke instans Anda, lihat Hubungkan ke instans Windows Anda menggunakan RDP.
2. Pada instans, unduh paket pemutakhiran Citrix.
3. Ekstrak konten paket yang dimutakhirkan ke lokasi pilihan Anda.
4. Klik dua kali file Upgrade.bat. Jika Anda mendapatkan peringatan keamanan, pilih Jalankan.
5. Di kotak dialog Tingkatkan Driver, tinjau informasinya dan pilih Ya jika Anda siap untuk memulai peningkatan.
6. Saat pemutakhiran selesai, file `PVUpgrade.log` akan terbuka dan berisi teks `UPGRADE IS COMPLETE`.
7. Booting ulang instans Anda.

Memecahkan masalah driver PV pada instance Windows

Berikut ini adalah solusi untuk masalah yang mungkin Anda temui dengan image Amazon EC2 dan driver PV yang lebih lama.

Daftar Isi

- Windows Server 2012 R2 kehilangan konektivitas jaringan dan penyimpanan setelah boot ulang instans
- Pemindahan TCP
- Sinkronisasi waktu

- Beban kerja yang memanfaatkan lebih dari 20.000 disk IOPS mengalami degradasi karena kemacetan CPU

Windows Server 2012 R2 kehilangan konektivitas jaringan dan penyimpanan setelah boot ulang instans

> **Important**
>
> Masalah ini hanya terjadi dengan AMIs tersedia sebelum September 2014.

Windows Server 2012 R2 Amazon Machine Images (AMIs) yang tersedia sebelum 10 September 2014 dapat kehilangan konektivitas jaringan dan penyimpanan setelah reboot instance. Kesalahan dalam log Konsol Manajemen AWS sistem menyatakan: “Kesulitan mendeteksi detail driver PV untuk Output Konsol.” Hilangnya konektivitas disebabkan oleh fitur Plug and Play Cleanup. Fitur ini memindai dan menonaktifkan perangkat sistem yang tidak aktif setiap 30 hari. Fitur tersebut salah mengidentifikasi perangkat jaringan EC2 sebagai tidak aktif dan menghapusnya dari sistem. Jika ini terjadi, instans kehilangan konektivitas jaringan setelah boot ulang.

Untuk sistem yang Anda curigai dapat terpengaruh oleh masalah ini, Anda dapat mengunduh dan menjalankan pemutakhiran driver langsung. Jika Anda tidak dapat melakukan pemutakhiran driver di tempat, Anda dapat menjalankan skrip pembantu. Skrip menentukan apakah instans Anda terpengaruh. Jika terpengaruh, dan perangkat jaringan Amazon EC2 belum dihapus, skrip menonaktifkan pemindaian Plug and Play Cleanup. Jika perangkat jaringan dihapus, skrip memperbaiki perangkat, menonaktifkan pemindaian Plug and Play Cleanup, dan memungkinkan instans Anda melakukan boot ulang dengan konektivitas jaringan diaktifkan.

Daftar Isi

- Pilih cara memperbaiki masalah
- Metode 1 - Jaringan yang ditingkatkan
- Metode 2 - Konfigurasi registri
- Jalankan skrip remediasi

Pilih cara memperbaiki masalah

Ada dua metode untuk memulihkan konektivitas jaringan dan penyimpanan ke instans yang terpengaruh oleh masalah ini. Pilih salah satu dari metode berikut:

Metode	Prasyarat	Ringkasan Prosedur
Metode 1 - Jaringan yang ditingkatkan	Jaringan yang ditingkatkan hanya tersedia di cloud privat virtual (VPC) yang memerluka n tipe instans C3. Jika server saat ini tidak menggunak an tipe instans C3, Anda harus mengubahnya untuk sementara.	Anda mengubah tipe instans server menjadi instans C3. Jaringan yang ditingkatkan kemudian memungkinkan Anda untuk terhubung ke instans yang terpengaruh dan memperbaiki masalah. Setelah Anda memperbaiki masalah, Anda mengubah instans kembali ke tipe instans asli. Metode ini biasanya lebih cepat daripada Metode 2 dan lebih kecil kemungkinannya dalam kesalahan pengguna. Anda akan dikenai biaya tambahan selama instans C3 berjalan.
Metode 2 - Konfigurasi registri	Kemampuan untuk membuat atau mengakses server kedua. Kemampuan untuk mengubah pengaturan Registri.	Anda melepaskan volume root dari instans yang terpengaruh, melampirk annya ke instans yang berbeda, menghubungkan, dan membuat perubahan di Registri. Anda akan dikenai biaya tambahan selama server tambahan berjalan. Metode ini lebih lambat daripada Metode 1, tetapi metode ini berhasil dalam situasi di mana Metode 1 gagal menyelesa ikan masalah.

Metode 1 - Jaringan yang ditingkatkan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Cari instans yang terpengaruh. Pilih instans dan pilih status Instans, lalu pilih Hentikan instans.

   > **Warning**
   >
   > Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instans akan hilang. Untuk melestarikan data ini, buat cadangan ke penyimpanan persisten.

4. Setelah instans dihentikan, buat cadangan. Pilih instans dan pilih Tindakan, lalu image dan templat, lalu pilih Buat image.
5. Ubah tipe instans menjadi tipe instans C3 apa pun.
6. Mulai instans.
7. Connect ke instance menggunakan Remote Desktop dan kemudian unduh paket AWS PV Drivers Upgrade ke instance.
8. Ekstrak isi folder dan jalankan.`AWSPVDriverSetup.msi`

   Setelah menjalankan MSI, instans secara otomatis melakukan boot ulang kemudian memutakhirkan driver. Instans tidak akan tersedia hingga 15 menit.
9. Setelah peningkatan selesai dan instans lulus pada pemeriksaan kondisi di konsol Amazon EC2, hubungkan ke instans menggunakan Desktop Jarak Jauh dan pastikan driver baru terinstal. Di Pengelola Perangkat, di bawah Kontroler Penyimpanan, temukan Adaptor Host Penyimpanan AWS PV. Pastikan versi driver sama dengan versi terbaru yang terdaftar pada tabel Riwayat Versi Driver. Untuk informasi selengkapnya, lihat AWS Riwayat paket driver PV.
10. Hentikan instans dan ubah kembali ke tipe instans aslinya.
11. Mulai instans dan lanjutkan penggunaan normal.

Metode 2 - Konfigurasi registri

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Cari instans yang terpengaruh. Pilih instans, pilih status Instans, lalu pilih Hentikan instans.

> **Warning**
>
> Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instans akan hilang. Untuk melestarikan data ini, buat cadangan ke penyimpanan persisten.

4. Pilih Luncurkan instans dan buat instans Windows Server 2008 atau Windows Server 2012 sementara di Zona Ketersediaan yang sama dengan instans yang terpengaruh. Jangan membuat instans Windows Server 2012 R2.

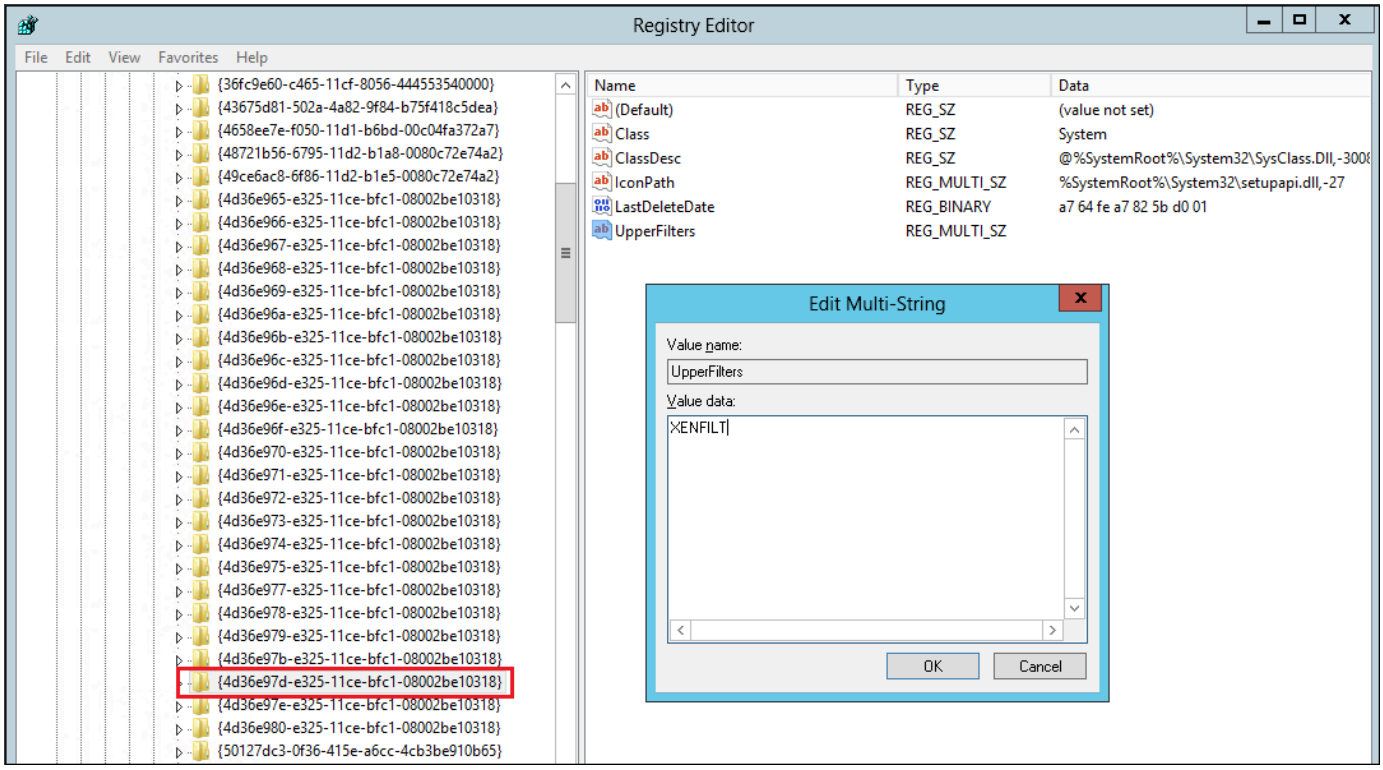
> **Important**
>
> Jika Anda tidak membuat instans di Zona Ketersediaan yang sama dengan instans yang terpengaruh, Anda tidak akan dapat melampirkan volume root dari instans yang terpengaruh ke instans baru.

5. Pada panel navigasi, pilih Volume.
6. Cari volume root dari instans yang terdampak. Lepaskan volume dan Lampirkan volume ke instans sementara yang Anda buat sebelumnya. Lampirkan dengan nama perangkat default (xvdf).
7. Gunakan Remote Desktop untuk terhubung ke instans sementara, dan kemudian gunakan utilitas Disk Management agar volume tersedia untuk digunakan.
8. Pada instans sementara, buka kotak dialog Jalankan, ketik **`regedit`**, dan tekan Enter.
9. Di panel navigasi Editor Registri, pilih HKEY_Local_Machine, lalu dari menu File pilih Muat Hive.
10. Di kotak dialog Muat Hive, arahkan ke Volume yang Terpengaruh\Windows\System32\config \System dan ketik nama sementara di kotak dialog Nama Kunci. Misalnya, enter OldSys .
11. Di panel navigasi Editor Registri, cari kunci berikut:

    HKEY_LOCAL_MACHINE\\ 001\ Kontrol\ Kelas***`your_temporary_key_name`***\ ControlSet 4d36e97d-e325-11ce-bfc1-08002be10318

    HKEY_LOCAL_MACHINE\\ 001\ Kontrol\ Kelas***`your_temporary_key_name`***\ ControlSet 4d36e96a-e325-11ce-bfc1-08002be10318

12. Untuk setiap kunci, klik dua kaliUpperFilters , masukkan nilai XENFILT, lalu pilih OK .



13. Temukan kunci berikut:

    HKEY_LOCAL_MACHINE\\ ControlSet 001\ Layanan\ ***your_temporary_key_name*** XENBUS\ Parameter

14. Buat string baru (REG_SZ) dengan nama ActiveDevice dan nilai berikut:

    PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Temukan kunci berikut:

    HKEY_LOCAL_MACHINE\\ 001\ Layanan\ ***your_temporary_key_name*** XENBUS ControlSet

16. Ubah Count dari 0 menjadi 1.

17. Temukan dan hapus kunci berikut:

    HKEY_LOCAL_MACHINE\\ 001\ Layanan\ ***your_temporary_key_name*** xenvbd\ ControlSet StartOverride

    HKEY_LOCAL_MACHINE\\ 001\ Layanan\ ***your_temporary_key_name*** xenfilt\ ControlSet StartOverride

18. Di panel navigasi Editor Registri, pilih kunci sementara yang Anda buat saat pertama kali membuka Editor Registri.

19. Dari File pilihan, pilih Pembongkaran Hive.
20. Di Disk Management Utility, pilih drive yang Anda pasang sebelumnya, buka menu konteks (klik kanan), dan pilih Offline.
21. Di konsol Amazon EC2, lepaskan volume yang terpengaruh dari instans sementara dan pasang kembali ke instans Windows Server 2012 R2 Anda dengan nama perangkat /dev/sda1. Anda harus menentukan nama perangkat ini untuk menetapkan volume sebagai volume root.
22. Mulai instans.
23. Connect ke instance menggunakan Remote Desktop dan kemudian unduh paket AWS PV Drivers Upgrade ke instance.
24. Ekstrak isi folder dan jalankan.`AWSPVDriverSetup.msi`

    Setelah menjalankan MSI, instans secara otomatis melakukan boot ulang kemudian memutakhirkan driver. Instans tidak akan tersedia hingga 15 menit.
25. Setelah peningkatan selesai dan instans lulus pada pemeriksaan kondisi di konsol Amazon EC2, hubungkan ke instans menggunakan Desktop Jarak Jauh dan pastikan driver baru terinstal. Di Pengelola Perangkat, di bawah Kontroler Penyimpanan, temukan Adaptor Host Penyimpanan AWS PV. Pastikan versi driver sama dengan versi terbaru yang terdaftar pada tabel Riwayat Versi Driver. Untuk informasi selengkapnya, lihat AWS Riwayat paket driver PV.
26. Hapus atau hentikan instans sementara yang Anda buat dalam prosedur ini.

Jalankan skrip remediasi

Jika Anda tidak dapat melakukan pemutakhiran driver langsung atau bermigrasi ke instans yang lebih baru, Anda dapat menjalankan skrip perbaikan untuk memperbaiki masalah yang disebabkan oleh tugas Pembersihan Pasang dan Pakai.

Untuk menjalankan skrip remediasi

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans yang ingin Anda jalankan skrip remediasinya. Pilih Status instans, lalu pilih Mulai instans.

> **Warning**
>
> Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instans akan hilang. Untuk melestarikan data ini, buat cadangan ke penyimpanan persisten.

4. Setelah instans dihentikan, buat cadangan. Setelah instans, pilih Tindakan, lalu Gambar dan templat, lalu pilih Buat gambar.
5. Pilih Status instans, lalu pilih Mulai instans.
6. Connect ke instance dengan menggunakan Remote Desktop dan kemudian download RemediateDriverIssue folder.zip ke instance.
7. Ekstrak isi folder tersebut.
8. Jalankan skrip remediasi sesuai petunjuk di file Readme.txt. File tersebut terletak di folder tempat Anda RemediateDriverIssue mengekstraksi.zip.

Pemindahan TCP

> **Important**
>
> Masalah ini tidak berlaku untuk instance yang menjalankan driver jaringan AWS PV atau Intel.

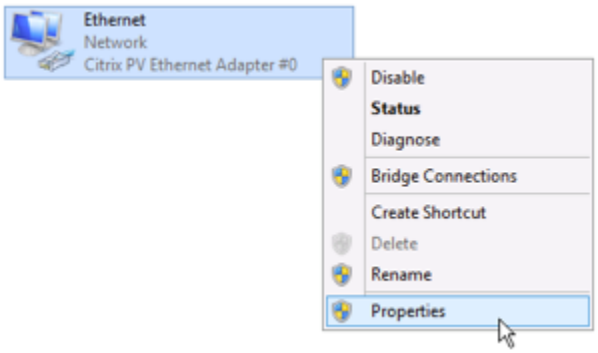
Secara default, pembongkaran TCP diaktifkan untuk driver Citrix PV di Windows. AMIs Jika Anda mengalami kesalahan tingkat pengangkutan atau kesalahan transmisi paket (seperti yang terlihat di Windows Performance Monitor)—misalnya, saat Anda menjalankan beban kerja SQL tertentu—Anda mungkin perlu menonaktifkan fitur ini.

> **Warning**
>
> Menonaktifkan pemindahan TCP dapat mengurangi performa jaringan instans Anda.

Untuk menonaktifkan pemindahan TCP untuk Windows Server 2012 dan 2008

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.

2. Jika Anda menggunakan Windows Server 2012, tekan Ctrl + Esc untuk mengakses layar Mulai, lalu pilih Panel Kontrol. Jika Anda menggunakan Windows Server 2008, pilih Mulai dan pilih Panel Kontrol.
3. Pilih Jaringan dan Internet, lalu Jaringan dan Pusat Berbagi.
4. Pilih Ubah pengaturan adaptor.
5. Klik kanan Citrix PV Ethernet Adapter # 0 dan pilih Properties.



6. Di kotak dialog Properti Koneksi Area Lokal, pilih Konfigurasi untuk membuka kotak dialog Properti #0 Adaptor Ethernet Citrix PV.
7. Pada tab Advanced, nonaktifkan setiap properti, kecuali untuk Nilai TCP/UDP Checksum yang Benar. Untuk menonaktifkan properti, pilih dari Properti dan pilih Dinonaktifkan dari Nilai.
8. Pilih OKE.
9. Jalankan perintah berikut dari jendela Command Prompt.

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Boot ulang instans.

Sinkronisasi waktu

Sebelum rilis AMI Windows 2013.02.13, agen tamu Citrix Xen dapat salah mengatur waktu sistem. Ini dapat menyebabkan sewa DHCP Anda kedaluwarsa. Jika Anda mengalami masalah saat menghubungkan ke instans Anda, Anda mungkin perlu memperbarui agennya.

Untuk menentukan apakah Anda memiliki agen tamu Citrix Xen yang diperbarui, periksa apakah file `C:\Program Files\Citrix\XenGuestAgent.exe` dari bulan Maret 2013. Jika tanggal pada

file ini lebih awal dari itu, perbarui layanan agen tamu Citrix Xen. Untuk informasi selengkapnya, lihat Mutakhirkan layanan agen tamu Citrix Xen Anda.

Beban kerja yang memanfaatkan lebih dari 20.000 disk IOPS mengalami degradasi karena kemacetan CPU

Anda dapat terpengaruh oleh masalah ini jika Anda menggunakan instans Windows yang menjalankan driver AWS PV yang memanfaatkan lebih dari 20.000 IOPS, dan Anda mengalami kode periksa bug `0x9E: USER_MODE_HEALTH_MONITOR`.

Disk membaca dan menulis (IOs) dalam driver AWS PV terjadi dalam dua fase: persiapan IO dan penyelesaian IO. Secara default, tahap persiapan berjalan pada core arbiter tunggal. Tahap penyelesaian berjalan pada inti `0`. Jumlah komputasi yang diperlukan untuk memproses IO berbeda-beda berdasarkan ukuran dan properti lainnya. Beberapa IOs menggunakan lebih banyak perhitungan dalam tahap persiapan, dan lainnya dalam tahap penyelesaian. Ketika sebuah instans menggerakkan lebih dari 20.000 IOPS, tahap persiapan atau penyelesaian dapat mengakibatkan hambatan, di mana CPU tempat instans tersebut berjalan ada pada kapasitas 100%. Apakah fase persiapan atau penyelesaian menjadi hambatan tergantung pada sifat-sifat yang IOs digunakan oleh aplikasi.

Dimulai dengan driver AWS PV 8.4.0, beban fase persiapan dan fase penyelesaian dapat didistribusikan di beberapa core, menghilangkan kemacetan. Setiap aplikasi menggunakan properti IO yang berbeda. Oleh karena itu, menerapkan salah satu konfigurasi berikut dapat meningkatkan, menurunkan, atau tidak mempengaruhi performa aplikasi Anda. Setelah Anda menerapkan salah satu konfigurasi ini, pantau aplikasi untuk memverifikasi bahwa aplikasi memenuhi performa yang Anda inginkan.

1. Prasyarat

   Sebelum Anda memulai prosedur pemecahan masalah ini, verifikasi prasyarat berikut:

   - Instans Anda menggunakan driver AWS PV versi 8.4.0 atau yang lebih baru. Untuk memutakhirkan, lihat Tingkatkan driver PV pada instans EC2 Windows.
   - Anda memiliki akses RDP ke instans. Untuk langkah-langkah agar ter-connect ke instans Windows menggunakan RDP, lihat Connect ke instans Windows Anda menggunakan klien RDP.
   - Anda memiliki akses administrator pada instans.

2. Mengamati beban CPU pada instans Anda

   Anda dapat menggunakan Windows Task Manager untuk melihat beban pada setiap CPU untuk menentukan potensi hambatan pada IO disk.

   1. Verifikasi bahwa aplikasi Anda menjalankan dan menangani lalu lintas mirip dengan beban kerja produksi Anda.
   2. Hubungkan ke instans Anda menggunakan RDP.
   3. Pilih menu Mulai pada instans Anda.
   4. Masukkan `Task Manager` di menu Mulai untuk membuka Task Manager.
   5. Jika Task Manager menampilkan Tampilan Ringkasan, pilih Detail lebih lanjut untuk menampilkan tampilan rinci.
   6. Pilih tab Performa.
   7. Pilih CPU di panel kiri.
   8. Klik kanan grafik pada panel utama dan pilih Ubah grafik ke>Prosesor logis untuk menampilkan masing-masing inti individu.
   9. Tergantung pada berapa banyak inti pada instans, Anda mungkin melihat baris yang menampilkan beban CPU dari waktu ke waktu, atau Anda mungkin hanya melihat angka.
      - Jika Anda melihat grafik menampilkan beban dari waktu ke waktu, cari CPUs di mana kotak hampir seluruhnya diarsir.
      - Jika Anda melihat angka pada setiap inti, cari inti yang secara konsisten menunjukkan angka 95% atau lebih besar.
   10. Perhatikan apakah inti `0` atau inti yang berbeda mengalami beban berat.

3. Pilih konfigurasi mana yang akan diterapkan

Nama konfigurasi	Kapan harus menerapkan konfigurasi ini	Catatan
Default configuration	Beban kerja menggerakkan kurang dari 20.000 IOPS, atau konfigurasi lain tidak meningkatkan performa atau stabilitas.	Untuk konfigurasi ini, IO terjadi pada beberapa inti, yang dapat menguntungkan beban kerja yang lebih kecil dengan meningkatkan cache

Nama konfigurasi	Kapan harus menerapkan konfigurasi ini	Catatan
		lokalitas dan mengurangi konteks beralih.
Allow driver to choose whether to distribute completion	Beban kerja menggerakkan lebih dari 20.000 IOPS dan beban sedang atau tinggi diamati pada inti `0`.	Konfigurasi ini direkomendasikan untuk semua instans Xen menggunakan PV 8.4.0 atau setelahnya dan memanfaatkan lebih dari 20.000 IOPS, baik ditemukan masalah ataupun tidak.
Distribute both preparation and completion	Beban kerja menggerakkan lebih dari 20.000 IOPS, dan menyebabkan driver dapat memilih distribusi tanpa meningkatkan performa, atau inti selain `0` mengalami beban tinggi.	Konfigurasi ini memungkinkan distribusi persiapan IO dan penyelesaian IO.

> **Note**
>
> Kami menyarankan agar Anda tidak mendistribusikan persiapan IO tanpa juga mendistribusikan penyelesaian IO (mengatur `DpcRedirection` tanpa mengatur `NotifierDistributed`) karena tahap penyelesaian peka terhadap kelebihan beban oleh tahap persiapan ketika tahap persiapan berjalan secara paralel.

Nilai-nilai kunci registri

- NotifierDistributed

  Nilai berupa `0` atau tidak ada — Tahap penyelesaian akan berjalan pada inti `0`.

  Nilai `1` — Driver memilih untuk menjalankan tahap penyelesaian atau `0` atau satu inti tambahan per disk terlampir.

Nilai 2 — Driver menjalankan tahap penyelesaian pada satu inti tambahan per disk terpasang.

- DpcRedirection

  Nilai berupa `0` atau tidak ada — Tahap persiapan akan berjalan pada inti tunggal arbiter.

  Nilai 1 — Tahap persiapan didistribusikan di banyak inti.

Konfigurasi default

Terapkan konfigurasi default dengan versi driver AWS PV sebelum 8.4.0, atau jika penurunan kinerja atau stabilitas diamati setelah menerapkan salah satu konfigurasi lain di bagian ini.

1. Hubungkan ke instans Anda menggunakan RDP.
2. Buka prompt PowerShell perintah baru sebagai administrator.
3. Jalankan perintah berikut untuk menghapus kunci registri `NotifierDistributed` dan `DpcRedirection`.

   ```
   Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
   \Parameters -Name NotifierDistributed
   ```

   ```
   Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
   \Parameters -Name DpcRedirection
   ```

4. Booting ulang instans Anda.

Izinkan driver untuk memilih apakah akan mendistribusikan penyelesaian

Atur kunci registri `NotiferDistributed` untuk memungkinkan driver penyimpanan PV untuk memilih apakah akan mendistribusikan penyelesaian IO atau tidak.

1. Hubungkan ke instans Anda menggunakan RDP.
2. Buka prompt PowerShell perintah baru sebagai administrator.
3. Jalankan perintah berikut untuk mengatur kunci registri `NotiferDistributed`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Booting ulang instans Anda.

Distribusikan persiapan dan penyelesaian

Atur kunci registri `NotifierDistributed` dan `DpcRedirection` untuk selalu mendistribusikan tahap persiapan dan penyelesaian.

1. Hubungkan ke instans Anda menggunakan RDP.
2. Buka prompt PowerShell perintah baru sebagai administrator.
3. Jalankan perintah berikut untuk mengatur kunci registri `NotifierDistributed` dan `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Booting ulang instans Anda.

AWS NVMe driver

Volume Amazon EBS dan volume penyimpanan instans diekspos sebagai perangkat NVMe blok pada instans berbasis Nitro. Untuk sepenuhnya memanfaatkan kinerja dan kemampuan fitur Amazon EBS untuk volume yang diekspos sebagai perangkat NVMe blok, instans harus menginstal AWS NVMe driver. Semua AWS Windows generasi saat ini AMIs dilengkapi dengan AWS NVMe driver yang diinstal secara default.

Untuk informasi selengkapnya tentang EBS dan NVMe, lihat Amazon EBS dan NVMe di Panduan Pengguna Amazon EBS. Untuk informasi lebih lanjut tentang toko instans SSD dan NVMe, lihat Volume penyimpanan instans SSD untuk instans EC2.

Instans Linux

Berikut ini AMIs termasuk NVMe driver yang diperlukan:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 atau yang lebih baru dengan kernel `linux-aws`

> **Note**
>
> AWS Jenis instance berbasis Graviton memerlukan Ubuntu 18.04 atau yang lebih baru dengan kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 atau setelahnya
- SUSE Linux Enterprise Server 12 SP2 atau yang lebih baru
- CentOS 7.4.1708 atau setelahnya
- FreeBSD 11.1 atau yang lebih baru
- Debian GNU/Linux 9 atau lebih baru

Untuk mengonfirmasi bahwa instans Anda memiliki NVMe driver

Anda dapat mengonfirmasi bahwa instance Anda memiliki NVMe driver menggunakan perintah berikut.

- Amazon Linux, RHEL, CentOS, dan SUSE Linux Server

```
$ modinfo nvme
```

  Jika instance memiliki NVMe driver, perintah mengembalikan informasi tentang driver.

- Amazon Linux 2 dan Ubuntu

```
$ ls /sys/module/ | grep nvme
```

  Jika instance memiliki NVMe driver, perintah mengembalikan driver yang diinstal.

Untuk memperbarui NVMe driver

Jika instans Anda memiliki NVMe driver, Anda dapat memperbarui driver ke versi terbaru menggunakan prosedur berikut.

1. Terhubung ke instans Anda.
2. Perbarui cache paket Anda untuk mendapatkan pembaruan paket yang diperlukan sebagai berikut.

   - Untuk Amazon Linux 2, Amazon Linux, CentOS, dan Red Hat Enterprise Linux:

     ```
     [ec2-user ~]$ sudo yum update -y
     ```

   - Untuk Ubuntu dan Debian:

     ```
     [ec2-user ~]$ sudo apt-get update -y
     ```

3. Ubuntu 16.04 dan yang lebih baru menyertakan `linux-aws` paket, yang berisi driver NVMe dan ENA yang diperlukan oleh instance berbasis NITRO. Mutakhirkan paket `linux-aws` untuk menerima versi terbaru sebagai berikut.

   ```
   [ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
   ```

   Untuk Ubuntu 14.04, Anda dapat menginstal paket `linux-aws` sebagai berikut:

   ```
   [ec2-user ~]$ sudo apt-get install linux-aws
   ```

4. Lakukan boot ulang instans untuk memuat versi kernel terbaru.

   ```
   sudo reboot
   ```

5. Hubungkan kembali ke instans Anda setelah boot ulang.

Instans Windows

PowerShell

Jika Anda tidak meluncurkan instans Anda dari salah satu AWS Windows terbaru yang AMIs disediakan oleh Amazon, gunakan prosedur berikut untuk menginstal AWS NVMe driver saat ini

pada instans Anda. Reboot diperlukan untuk instalasi ini. Entah skrip instalasi akan mem-boot ulang instans Anda atau Anda harus mem-boot ulang sebagai langkah terakhir.

Prasyarat

- PowerShell versi 3.0 atau yang lebih baru diinstal.
- Perintah yang ditampilkan di bagian ini harus berjalan dalam versi 64-bit PowerShell. Jangan gunakan x86 versi PowerShell. Itu adalah versi 32-bit dari shell, dan tidak didukung untuk perintah ini.

Untuk mengunduh dan menginstal AWS NVMe driver terbaru

1. Kami menyarankan Anda untuk membuat AMI sebagai cadangan sebagai berikut, jika Anda perlu mengembalikan perubahan Anda.
   a. Ketika Anda menghentikan instans, data pada setiap volume penyimpanan instans akan dihapus. Sebelum Anda menghentikan sebuah instans, pastikan bahwa Anda telah menyalin data apa pun yang Anda perlukan dari volume penyimpanan instans ke penyimpanan persisten, seperti Amazon EBS atau Amazon S3.
   b. Di panel navigasi, pilih Contoh.
   c. Pilih instans yang memerlukan pemutakhiran driver, dan pilih Status instans, Hentikan instans.
   d. Setelah instans dihentikan, pilih instans, pilih Tindakan, lalu Gambar dan templat, lalu pilih Buat gambar.
   e. Pilih Status instans, Mulai instans.
2. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.
3. Unduh driver ke instans Anda menggunakan salah satu opsi berikut:
   - Browser — https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/Latest/AWSNVMe.zip paket driver terbaru ke instance dan ekstrak arsip zip.
   - PowerShell— Jalankan perintah berikut:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/
NVMe/Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
 $env:userprofile\nvme_driver
```

Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016 atau yang lebih lama, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:

```
[Net.ServicePointManager]::SecurityProtocol =
 [Net.SecurityProtocolType]::Tls12
```

4. Instal driver ke instance Anda dengan menjalankan `install.ps1` PowerShell skrip dari `nvme_driver` direktori (`.\install.ps1`). Jika Anda mendapatkan kesalahan, pastikan Anda menggunakan PowerShell 3.0 atau yang lebih baru.

   a. (Opsional) Dimulai dengan AWS NVMe versi`1.5.0`, reservasi persisten Antarmuka Sistem Komputer Kecil (SCSI) didukung untuk Windows Server 2016 dan yang lebih baru. Fitur ini menambahkan dukungan untuk Windows Server Failover Clustering dengan penyimpanan Amazon EBS bersama. Secara default, fitur ini tidak diaktifkan selama instalasi.

   Anda dapat mengaktifkan fitur saat menjalankan skrip `install.ps1` untuk menginstal driver dengan menentukan parameter `EnableSCSIPersistentReservations` dengan nilai `$true`.

   ```
   PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
   ```

   Anda dapat mengaktifkan fitur saat menjalankan skrip `install.ps1` untuk menginstal driver dengan menentukan parameter `EnableSCSIPersistentReservations` dengan nilai `$false`.

   ```
   PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
   ```

   b. Dimulai dengan AWS NVMe `1.5.0`, `install.ps1` skrip selalu menginstal `ebsnvme-id` alat dengan driver.

   (Opsional) Untuk versi `1.4.0`, `1.4.1`, dan `1.4.2`, skrip `install.ps1` memungkinkan Anda untuk menentukan apakah alat `ebsnvme-id` harus diinstal dengan driver.

   i. Untuk menginstal alat `ebsnvme-id`, tentukan `InstallEBSNVMeIdTool ‘Yes’`.

   ii. Jika Anda tidak ingin menginstal alat, tentukan `InstallEBSNVMeIdTool ‘No’`.

Jika Anda tidak menentukan `InstallEBSNVMeIdTool`, dan alat sudah ada di `C:\ProgramData\Amazon\Tools`, paket akan memutakhirkan alat secara default. Jika alat tidak ada, `install.ps1` tidak akan memutakhirkan alat secara default.

Jika Anda tidak ingin menginstal alat sebagai bagian dari paket, dan ingin menginstalnya nanti, Anda dapat menemukan versi terbaru atau alat dalam paket driver. Atau, Anda dapat mengunduh versi `1.0.0` dari Amazon S3:

Unduh alat `ebsnvme-id`.

5. Jika penginstal tidak melakukan boot ulang instans Anda, lakukan boot ulang instans tersebut.

Distributor

Anda dapat menggunakan Distributor, kemampuan AWS Systems Manager, untuk menginstal paket NVMe driver satu kali atau dengan pembaruan terjadwal.

Untuk menginstal AWS NVMe driver terbaru

1. Untuk petunjuk cara menginstal paket NVMe driver menggunakan Distributor, lihat prosedur di Menginstal atau memperbarui paket di Panduan Pengguna Amazon EC2 Systems Manager.
2. Untuk Jenis Instalasi, pilih Uninstall dan instal ulang.
3. Untuk Nama, pilih AWSNVMe.
4. (Opsional) Untuk Argumen Tambahan, Anda dapat menyesuaikan instalasi dengan menentukan nilai. Nilai harus diformat menggunakan sintaks JSON yang valid. Untuk contoh cara meneruskan argumen tambahan untuk `aws configure` paket, lihat referensi plugin Command document.

   a. Dimulai dengan AWS NVMe `1.5.0`, driver mendukung reservasi persisten SCSI untuk Windows Server 2016 dan yang lebih baru. Secara default, fitur ini tidak diaktifkan selama instalasi.

      - Untuk mengaktifkan fitur ini, tentukan`{"SSM_EnableSCSIPersistentReservations": "true"}`.
      - Jika Anda tidak ingin mengaktifkan fitur ini, tentukan`{"SSM_EnableSCSIPersistentReservations": "false"}`.

b. Dimulai dengan AWS NVMe `1.5.0`, `install.ps1` skrip akan selalu menginstal `ebsnvme-id` alat.

   (Opsional) Untuk versi `1.4.0`, `1.4.1`, dan `1.4.2`, skrip `install.ps1` memungkinkan Anda untuk menentukan apakah alat ebsnvme-id harus diinstal dengan driver.

   - Untuk menginstal alat ebsnvme-id, tentukan. `{"SSM_InstallEBSNVMeIdTool": "Yes"}`
   - Jika Anda tidak ingin menginstal alat, tentukan `{"SSM_InstallEBSNVMeIdTool": "No"}`.

     Jika tidak `SSM_InstallEBSNVMeIdTool` ditentukan untuk Argumen Tambahan, dan alat sudah ada di`C:\ProgramData\Amazon\Tools`, paket akan meng-upgrade alat secara default. Jika alat tidak ada, paket tidak akan memutakhirkan alat secara default.

     Jika Anda tidak ingin menginstal alat sebagai bagian dari paket, dan ingin menginstalnya nanti, Anda dapat menemukan versi terbaru alat dalam paket driver. Atau, Anda dapat mengunduh versi `1.0.0` dari Amazon S3:

     Unduh alat `ebsnvme-id`.

5. Jika penginstal tidak melakukan boot ulang instans Anda, lakukan boot ulang instans tersebut.

Konfigurasikan reservasi persisten SCSI untuk instance Windows

Setelah versi AWS NVMe driver `1.5.0` atau yang lebih baru diinstal, Anda dapat mengaktifkan atau menonaktifkan reservasi persisten SCSI menggunakan registri Windows untuk Windows Server 2016 dan yang lebih baru. Anda harus melakukan boot ulang instans agar perubahan registri ini diterapkan.

Anda dapat mengaktifkan reservasi persisten SCSI dengan perintah berikut yang mengatur `EnableSCSIPersistentReservations` ke nilai `1`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

Anda dapat menonaktifkan reservasi persisten SCSI dengan perintah berikut yang mengatur `EnableSCSIPersistentReservations` ke nilai `0`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

AWS NVMe Riwayat versi driver Windows

Tabel berikut menunjukkan driver AWS NVMe mana yang berjalan pada setiap versi Windows Server di Amazon EC2.

Versi Windows Server	AWS NVMe versi driver
Windows Server 2025	versi terbaru
Windows Server 2022	versi terbaru
Windows Server 2019	versi terbaru
Windows Server 2016	versi terbaru
Windows Server 2012 R2	versi 1.5.1 dan sebelumnya
Windows Server 2012	versi 1.5.1 dan sebelumnya
Windows Server 2008 R2	versi 1.3.2 dan sebelumnya
Windows Server 2008	versi 1.3.2 dan sebelumnya

Tabel berikut menjelaskan versi AWS NVMe driver yang dirilis.

Versi Package	Versi Driver	Detail	Tanggal rilis
1.8.1 1.8.1	1.8.1	• Memperbaiki masalah kompatibilitas mundur dengan pembuatan nomor seri disk.	24 Februari 2026

Versi Package	Versi Driver	Detail	Tanggal rilis
1.8.0	1.8.0	• Menambahkan dukungan IOCTLs untuk beroperasi dengan perangkat yang menerapkan manajemen namespace dinamis. Untuk informasi selengkapnya, lihat IOCTL_SCSI_MINIPORT IOCTL di dokumentasi Microsoft. • Perbaikan bug dalam perintah Get Log Page dan pembuatan nomor seri.	16 Januari 2026
	1.7.0	• Ditambahkan dukungan untuk NVMe Dapatkan Log Page Command. • Menambahkan dukungan untuk statistik kinerja terperinci untuk volume penyimpanan instans EBS dan EC2. • Perbaikan bug untuk perintah Identify Namespace.	17 September 2025
	1.6.0	• Memperbarui skrip penginstalan untuk menggunakan PnPUtil. • Diperbarui ebsnvme-id.exe untuk menggunakan NVMe IOCTL.	25 Oktober 2024
1.5.1 1.5.1	1.5.0	Memperbaiki skrip penginstalan untuk membuat folder untuk `ebsnvme-id` alat jika tidak ada.	17 November 2023
1.5.0	1.5.0	Menambahkan dukungan untuk reservasi persisten Small Computer System Interface (SCSI) untuk instans yang menjalankan Windows Server 2016 dan setelahnya. Alat ebsnvme-id (`ebsnvme-id.exe`) sekarang diinstal secara default.	31 Agustus 2023

Versi Package	Versi Driver	Detail	Tanggal rilis
1.4.2	1.4.2	Memperbaiki bug yang Driver AWS NVMe tidak mendukung volume penyimpanan instans pada instans D3.	16 Maret 2023
1.4.1	1.4.1	Laporan Namespace Preferred Write Granularity (NPGW) untuk volume EBS yang mendukung fitur opsional ini. NVMe Untuk informasi selengkapnya, lihat bagian 8.25, “Meningkatkan Kinerja melalui Ukuran I/O dan Kepatuhan Penyelarasan,” di Spesifikasi NVMe Dasar, versi 1.4.	20 Mei 2022
1.4.0	1.4.0	• Menambahkan dukungan untuk IOCTLs itu memungkinkan aplikasi untuk berinteraksi dengan NVMe perangkat. Dukungan ini memungkinkan aplikasi untuk mendapatkan `IdentifyController` `IdentifyNamespace` ,, dan `NameSpace` daftar dari NVMe perangkat. Untuk informasi selengkapnya, lihat Kueri spesifik protokol di dokumentasi Microsoft. • Versi driver 1.4.0 dan alat `ebsnvme-id` terbaru (`ebsnvme-id.exe`) digabungkan dalam satu paket. Kombinasi ini memungkinkan Anda untuk menginstal driver dan alat dari satu paket. Untuk detail selengkapnya, lihat AWS NVMe driver. • Perbaikan bug dan peningkatan keandalan.	23 November 2021

Versi Package	Versi Driver	Detail	Tanggal rilis
1.3.2 1.3.2	1.3.2	Memperbaiki masalah pengubahan volume EBS yang secara aktif memproses IO, yang dapat mengakibatkan kerusakan data. Pelanggan yang tidak memodifikasi volume EBS online (misalnya, mengubah ukuran atau mengubah tipe) tidak akan terpengaruh. Ini adalah versi terakhir yang dapat berjalan pada Windows Server 2008 dan 2008 R2. Versi ini tersedia untuk diunduh tetapi tidak lagi didukung. Windows Server 2008 dan 2008 R2 telah mencapai end-of-life, dan tidak lagi didukung oleh Microsoft.	10 September 2019
1.3.1	1.3.1	Peningkatan keandalan.	21 Mei 2019
1.3.0	1.3.0	Peningkatan pengoptimalan perangkat.	31 Agustus 2018
1.2.0	1.2.0	Peningkatan kinerja dan keandalan untuk AWS NVMe perangkat pada semua instans yang didukung, termasuk instans bare metal.	13 Juni 2018
> 1.0.0	> 1.0.0	AWS NVMe driver untuk jenis instans yang didukung yang menjalankan Windows Server.	12 Februari 2018

Berlangganan notifikasi

Amazon SNS dapat memberi Anda notifikasi saat EC2 Windows Drivers versi baru dirilis. Gunakan prosedur berikut untuk berlangganan notifikasi ini.

Untuk berlangganan notifikasi EC2 dari konsol

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah ini karena notifikasi SNS langganan Anda ada di Wilayah ini.

3. Di panel navigasi, pilih Langganan.
4. Pilih Buat langganan.
5. Di kotak dialog Create subscription (Buat langganan), lakukan hal berikut:
   a. Untuk TopicARN, salin Amazon Resource Name (ARN) berikut:

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Untuk Protokol, pilih `Email`.
   c. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi.
   d. Pilih Buat langganan.
6. Anda akan menerima email konfirmasi. Buka email dan ikuti petunjuk untuk menyelesaikan langganan Anda.

Setiap kali driver EC2 Windows baru dirilis, kami mengirimkan notifikasi ke pelanggan. Jika Anda tidak ingin lagi menerima notifikasi ini, gunakan prosedur berikut untuk berhenti berlangganan.

Untuk berhenti berlangganan dari notifikasi driver Windows Amazon EC2

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di panel navigasi, pilih Berlangganan.
3. Pilih kotak centang untuk langganan lalu pilih Tindakan, Hapus langganan. Ketika diminta konfirmasi, pilih Hapus.

Untuk berlangganan notifikasi EC2 menggunakan AWS CLI

Untuk berlangganan pemberitahuan EC2 dengan AWS CLI, gunakan perintah berikut.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Untuk berlangganan notifikasi EC2 menggunakan AWS Tools for Windows PowerShell

Untuk berlangganan notifikasi EC2 dengan AWS Tools for Windows PowerShell, gunakan perintah berikut.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Konfigurasikan instans Windows Amazon EC2 Anda

Setelah meluncurkan instance Windows, Anda dapat masuk sebagai administrator untuk melakukan konfigurasi tambahan untuk fitur Windows dan pengaturan sistem. Utilitas pemecahan masalah Windows EC2dapat membantu Anda memecahkan masalah pada instans Anda.

Anda dapat mengonfigurasi agen peluncuran Windows dan fitur khusus Windows lainnya sebagai berikut.

Agen peluncuran Windows

Setiap AWS Windows AMI (dan banyak lainnya AMIs yang tersedia di AWS Marketplace) menyertakan agen peluncuran Windows yang telah dikonfigurasi sebelumnya dengan pengaturan default. Agen peluncuran melakukan tugas selama startup instance dan dijalankan jika instance dihentikan dan kemudian dimulai, atau dimulai ulang.

Peluncuran Cepat EC2 untuk Windows

Setiap instans Windows Amazon EC2 harus melalui langkah-langkah peluncuran sistem operasi Windows standar (OS), yang mencakup beberapa boot ulang, dan seringkali membutuhkan waktu 15 menit atau lebih lama untuk menyelesaikannya. Amazon EC2 Windows Server AMI yang mengaktifkan fitur Peluncuran Cepat EC2, selesaikan beberapa langkah tersebut dan reboot terlebih dahulu untuk mengurangi waktu yang diperlukan untuk meluncurkan instans.

Pengaturan sistem khusus Windows

Daftar berikut mencakup beberapa pengaturan sistem yang hanya berlaku untuk sistem operasi Windows:

Ubah kata sandi Administrator Windows

Saat Anda terhubung ke instans Windows, Anda harus menentukan akun pengguna dan kata sandi yang memiliki izin untuk mengakses instans. Pertama kali Anda terhubung ke sebuah instans, Anda harus menggunakan akun Administrator dan memberikan kata sandi default. Saat Anda terhubung ke sebuah instans untuk pertama kalinya, kami menyarankan Anda untuk mengubah kata sandi Administrator dari nilai default-nya.

Tambahkan komponen Sistem Windows

Sistem operasi Windows Server mencakup banyak komponen opsional. Menyertakan semua komponen opsional di setiap AWS Windows Server AMI tidak praktis. Sebagai gantinya,

kami menyediakan snapshot EBS media instalasi yang memiliki file yang diperlukan untuk mengkonfigurasi atau menginstal komponen pada instance Windows Anda.

Instal WSL di Windows

Windows Subsystem for Linux (WSL) adalah unduhan gratis yang dapat Anda instal di instans Windows Anda. Dengan menginstal WSL, Anda dapat menjalankan alat baris perintah Linux native secara langsung di instans Windows Anda dan menggunakan alat Linux untuk membuat skrip, di samping desktop Windows tradisional Anda. Anda dapat dengan mudah bertukar antara Linux dan Windows pada satu instans Windows, yang mungkin berguna bagi Anda dalam lingkungan pengembangan.

AWS driver perangkat untuk instance Windows

Anda dapat memperbarui driver AWS perangkat untuk instance Windows Anda. Untuk informasi selengkapnya, lihat the section called “Kelola driver perangkat”.

Tabel berikut merangkum driver yang didukung untuk instance berbasis Nitro menurut versi Windows.

Versi	Driver penyimpanan	Driver jaringan yang ditingkat kan
Windows Server 2025	AWS NVMe versi terbaru	ENA versi terbaru
Windows Server 2022	AWS NVMe versi terbaru	ENA versi terbaru
Windows Server 2019	AWS NVMe versi terbaru	ENA versi terbaru
Windows Server 2016	AWS NVMe versi terbaru	ENA versi terbaru
Windows Server 2012 R2	AWS NVMe versi 1.5.1	ENA versi 2.6.0
Windows Server 2008 R2	AWS NVMe versi 1.3.2	ENA versi 2.2.3

Tabel berikut merangkum driver yang didukung untuk instance berbasis Xen menurut versi Windows.

Versi	Driver penyimpanan	Driver jaringan yang ditingkatkan
Windows Server 2022	AWS PV versi terbaru	• ENA versi terbaru [1] • Intel VF 2 • AWS PV versi terbaru [3]
Windows Server 2019	AWS PV versi terbaru	• ENA versi terbaru [1] • Intel VF 2 • AWS PV versi terbaru [3]
Windows Server 2016	AWS PV versi terbaru	• ENA versi terbaru [1] • Intel VF 2 • AWS PV versi terbaru [3]
Windows Server 2012 R2	AWS PV versi 8.4.3	• ENA versi 2.6.0 1 • Intel VF 2 • AWS PV versi 8.4.3 3
Windows Server 2008 R2	AWS PV versi 8.3.5	• ENA versi 2.2.3 1 • Intel VF 2 • AWS PV versi 8.3.5 3

[1] Misalnya tipe G3, H1, I3,, P2, P3`m4.16xlarge`, P3dn, dan R4.

[2] Misalnya jenis C3, C4, D2, I2, M4 (tidak termasuk`m4.16xlarge`), dan R3.

[3] Misalnya jenis C1, M1, M2, M3, T1, T2, X1, dan X1e.

Agen peluncuran Windows di instans Amazon EC2 Windows

Setiap AMI AWS Windows menyertakan agen peluncuran Windows yang telah dikonfigurasi sebelumnya dengan pengaturan default. Agen peluncuran melakukan tugas selama startup instance

dan dijalankan jika instance dihentikan dan kemudian dimulai, atau dimulai ulang. Untuk informasi tentang agen tertentu, lihat halaman detail dalam daftar berikut.

Untuk informasi selengkapnya tentang AWS Windows AMIs, lihat referensi AWS Windows AMI.

- Gunakan agen EC2launch v2 untuk melakukan tugas selama peluncuran instans Windows EC2
- Gunakan agen EC2launch v1 untuk melakukan tugas selama peluncuran instans Windows EC2
- Gunakan layanan EC2config untuk melakukan tugas selama peluncuran instans sistem operasi Windows lama EC2

Daftar isi

- Bandingkan agen EC2 peluncuran Amazon
- Konfigurasikan DNS Suffix untuk agen peluncuran EC2 Windows
- Berlangganan pemberitahuan agen peluncuran EC2 Windows
- Administrasi Layanan Windows untuk agen EC2 Launch v2 dan EC2 Config

Bandingkan agen EC2 peluncuran Amazon

Tabel berikut menunjukkan perbedaan fungsional utama antara EC2 Config, EC2 Launch v1, dan EC2 Launch v2.

Fitur	EC2Config	EC2Luncurkan v1	EC2Luncurkan v2
Jalankan sebagai	Layanan Windows	PowerShell Skrip	Layanan Windows
Mendukung	Hanya OS warisan	Versi Windows Server: • 2016 • 2019 (LTSC dan SAC)	Versi Windows Server: • 2016 • 2019 (LTSC dan SAC) • 2022 • 2025
File konfigurasi	XML	JSON	JSON/YAML

Fitur	EC2Config	EC2Luncurkan v1	EC2Luncurkan v2
Tetapkan nama pengguna Administrator	Tidak	Tidak	Ya
Data pengguna terkompresi	Tidak	Tidak	Ya
Data pengguna lokal dibuat di AMI	Tidak	Tidak	Ya, dapat dikonfigurasi
Konfigurasi tugas dalam data pengguna	Tidak	Tidak	Ya
Wallpaper yang dapat dikonfigurasi	Tidak	Tidak	Ya
Sesuaikan urutan jalannya tugas	Tidak	Tidak	Ya
Tugas yang dapat dikonfigurasi	15	9	20 saat peluncuran
Mendukung Windows Event Viewer	Ya	Tidak	Ya
Jumlah tipe peristiwa Penampil Peristiwa	2	0	30

> **Note**
>
> EC2Dokumentasi Config disediakan hanya untuk referensi historis. Versi sistem operasi yang dijalankannya tidak lagi didukung oleh Microsoft. Kami sangat menyarankan Anda meningkatkan ke layanan peluncuran terbaru.

Konfigurasikan DNS Suffix untuk agen peluncuran EC2 Windows

Dengan agen EC2 peluncuran Amazon, Anda dapat mengonfigurasi daftar sufiks DNS yang digunakan instance Windows untuk resolusi nama domain. Agen peluncuran mengganti pengaturan Windows standar di kunci `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` registri dengan menambahkan nilai berikut ke daftar pencarian akhiran DNS:

- Domain dari instance
- Sufiks yang dihasilkan dari devolusi domain instance
- Domain NV
- Domain yang ditentukan oleh setiap kartu antarmuka jaringan

Semua agen peluncuran mendukung konfigurasi akhiran DNS. Untuk informasi selengkapnya, lihat versi agen peluncuran spesifik Anda:

- Untuk informasi tentang `setDnsSuffix` tugas dan cara mengkonfigurasi sufiks DNS di EC2 Launch v2, lihat. setDnsSuffix
- Untuk informasi tentang pengaturan daftar akhiran DNS dan cara mengaktifkan atau menonaktifkan devolusi untuk EC2 Peluncuran v1, lihat. Konfigurasikan agen EC2 Launch v1 pada instance Windows Anda
- Untuk informasi tentang pengaturan daftar akhiran DNS dan cara mengaktifkan atau menonaktifkan devolusi untuk EC2 Config, lihat. EC2File pengaturan Config

Devolusi nama domain

Devolusi nama domain adalah perilaku Direktori Aktif yang memungkinkan komputer dalam domain anak untuk mengakses sumber daya di domain induk tanpa menggunakan nama domain yang sepenuhnya memenuhi syarat. Secara default, devolusi nama domain berlanjut hingga hanya ada dua node yang tersisa dalam perkembangan nama domain.

Agen peluncuran melakukan devolusi pada nama domain jika instance terhubung ke domain, dan menambahkan hasilnya ke daftar pencarian akhiran DNS yang dipertahankan dalam kunci registri. **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`** Agen menggunakan pengaturan dari kunci registri berikut, untuk menentukan perilaku devolusi.

- **`System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution`**

  - Ketika tidak diatur, menonaktifkan devolusi
  - Saat disetel ke`1`, aktifkan devolusi (default)
  - Ketika diatur ke`0`, menonaktifkan devolusi
- **`System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`**
  - Bila tidak disetel, gunakan level of 2 (default)
  - Saat disetel ke `3` atau lebih besar, gunakan nilai untuk mengatur level

Ketika Anda menonaktifkan devolusi atau mengubah pengaturan devolusi Anda ke tingkat yang lebih tinggi, kunci `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` registri stil berisi sufiks yang ditambahkan sebelumnya. Mereka tidak dihapus secara otomatis. Anda dapat memperbarui daftar secara manual, atau Anda dapat menghapus daftar dan membiarkan agen Anda menjalankan proses untuk mengatur daftar baru.

> **Note**
>
> Untuk menghapus daftar akhiran DNS dari registri, Anda dapat menjalankan perintah berikut.
>
> ```
> PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
> MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
>  $null } | Out-Null
> ```

Contoh devolusi

Contoh berikut menunjukkan perkembangan nama domain melalui proses devolusi.

`corp.example.com`

- Berlanjut ke `example.com`

`locale.region.corp.example.com`

1. Berlanjut ke `region.corp.example.com`
2. Berlanjut ke `corp.example.com`
3. Berlanjut ke `example.com`

`locale.region.corp.example.com`dengan pengaturan `DomainNameDevolutionLevel=3`

1. Berlanjut ke `region.corp.example.com`
2. Berkembang ke`corp.example.com`. Perkembangan berhenti di sini, karena pengaturan level.

Berlangganan pemberitahuan agen peluncuran EC2 Windows

Amazon SNS dapat memberi tahu Anda saat versi baru agen EC2 peluncuran dirilis. Gunakan prosedur berikut untuk berlangganan notifikasi ini.

Berlangganan EC2 notifikasi Config

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah ini karena notifikasi SNS tempat Anda berlangganan dibuat di Wilayah ini.
3. Di panel navigasi, pilih Langganan.
4. Pilih Buat langganan.
5. Di kotak dialog Create subscription (Buat langganan), lakukan hal berikut:
   a. Untuk Topik ARN, gunakan Nama Sumber Daya Amazon (ARN) berikut yang cocok dengan agen yang ingin Anda terima notifikasi:
      - EC2Luncurkan v2:

        ```
        arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2
        ```

      - EC2Luncurkan atau EC2 Config:

        ```
        arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
        ```

   b. Untuk Protokol, pilih `Email`.
   c. Untuk Endpoint, masukkan alamat email tempat Anda ingin menerima notifikasi.
   d. Pilih Buat langganan.
6. Anda akan menerima email yang meminta Anda untuk mengonfirmasi langganan Anda. Buka email dan ikuti petunjuk untuk menyelesaikan langganan Anda.

Setiap kali versi baru dari agen peluncuran dirilis, kami mengirimkan pemberitahuan kepada pelanggan. Jika Anda tidak ingin lagi menerima notifikasi ini, gunakan prosedur berikut untuk berhenti berlangganan.

Berhenti berlangganan pemberitahuan agen peluncuran

1. Buka konsol Amazon SNS.
2. Di panel navigasi, pilih Langganan.
3. Pilih langganan lalu pilih Tindakan, Hapus langganan. Ketika diminta untuk mengonfirmasi, pilih Hapus.

Administrasi Layanan Windows untuk agen EC2 Launch v2 dan EC2 Config

Jika Anda telah masuk ke instans Anda sebagai pengguna dengan hak administratif, Anda dapat mengelola agen EC2 peluncuran Launch v2 dan EC2 Config seperti halnya layanan Windows lainnya. EC2Launch v1 adalah sekumpulan PowerShell skrip yang dikelola melalui tugas terjadwal secara default. Bagian ini mencakup administrasi layanan untuk EC2 Launch v2 dan EC2 Config.

Untuk menerapkan pengaturan yang diperbarui ke instans Anda, Anda dapat menghentikan dan memulai ulang agen EC2 Launch v2 atau agen peluncuran layanan EC2 Config dari antarmuka Microsoft Management Console (MMC) untuk Layanan. Demikian pula, ketika Anda menginstal versi baru agen peluncuran, Anda harus menghentikan agen terlebih dahulu, kemudian restart ketika instalasi selesai.

> **Note**
>
> Anda harus membuka antarmuka Layanan MMC sebagai administrator untuk memilih tindakan ini. Untuk melakukan ini, Anda dapat memilih Jalankan sebagai administrator dari menu konteks. Atau, untuk membuka antarmuka menggunakan keyboard Anda, ikuti langkah-langkah ini:
>
> 1. Menggunakan `Tab` tombol atau tombol panah, pilih item menu Layanan dari menu Alat Administratif.
> 2. Gunakan kombinasi keyboard berikut untuk membuka sebagai administrator: `Ctrl + Shift +Enter`.

Prosedur berikut mencantumkan langkah-langkah untuk menghentikan dan memulai agen peluncuran pada instans Anda.

Hentikan agen peluncuran

1. Jalankan dan hubungkan ke instans Windows Anda.
2. Pilih Alat Administratif dari menu Start Windows.
3. Buka konsol Layanan sebagai administrator, seperti yang dijelaskan di awal bagian ini.
4. Dalam daftar layanan, pilih agen yang berjalan pada instance Anda (EC2Launch atau EC2Config), lalu pilih Stop dari menu Action. Atau, Anda dapat menggunakan menu konteks untuk menghentikan agen.

Mulai ulang agen peluncuran

1. Jalankan dan hubungkan ke instans Windows Anda.
2. Pilih Alat Administratif dari menu Start Windows.
3. Buka konsol Layanan sebagai administrator, seperti yang dijelaskan di awal bagian ini.
4. Dalam daftar layanan, pilih agen yang berjalan pada instans Anda (EC2Luncurkan atau EC2Konfigurasi), lalu pilih Mulai atau Mulai Ulang dari menu Tindakan. Atau, Anda dapat menggunakan menu konteks untuk memulai ulang agen.

Jika Anda tidak perlu memperbarui pengaturan konfigurasi, membuat AMI Anda sendiri, atau menggunakan AWS Systems Manager, Anda dapat menghapus atau menghapus instalan agen peluncuran.

Hapus

Menghapus layanan akan menghapus subkunci registrinya.

Copot pemasangan

Menghapus instalasi layanan akan menghapus file, subkunci registri, dan pintasan apa pun ke layanan tersebut.

Hapus agen peluncuran

1. Jalankan dan hubungkan ke instans Windows Anda.

2. Mulai jendela Prompt Perintah Windows.
3. Jalankan salah satu perintah berikut untuk menghapus agen peluncuran.

   - Jalankan perintah berikut untuk menghapus EC2 Launch atau EC2 Launch v2:

     ```
     sc delete ec2launch
     ```

   - Jalankan perintah berikut untuk menghapus layanan EC2 Config:

     ```
     sc delete ec2config
     ```

Copot pemasangan agen peluncuran

1. Jalankan dan hubungkan ke instans Windows Anda.
2. Pilih Sistem Windows, lalu Control Panel dari menu Start Windows.
3. Pilih Program dan Fitur untuk membuka daftar program yang diinstal pada instans Anda.
4. Pilih agen peluncuran Anda dari daftar (Amazon EC2 Launch atau EC2ConfigService), lalu pilih Uninstall dari menu File. Atau, Anda dapat menggunakan menu konteks.

   > **Note**
   >
   > Anda dapat melihat versi agen peluncuran apa yang diinstal di kolom Versi.

Gunakan agen EC2launch v2 untuk melakukan tugas selama peluncuran instans Windows EC2

Semua instans Amazon EC2 yang didukung yang diluncurkan AWS dari Windows Server 2022 dan Windows Server AMIs 2025 menyertakan EC2 agen peluncuran Launch v2 `EC2Launch.exe` () secara default. Kami juga menyediakan Windows Server 2016 dan 2019 AMIs dengan EC2 Launch v2 diinstal sebagai agen peluncuran default. Ini AMIs disediakan selain Windows Server 2016 dan 2019 AMIs yang mencakup EC2 Launch v1. Anda dapat mencari Windows AMIs yang menyertakan EC2 Launch v2 secara default dengan memasukkan awalan berikut dalam pencarian Anda dari AMIshalaman di konsol Amazon EC2:. `EC2LaunchV2-Windows_Server-*`

Untuk membandingkan fitur versi agen peluncuran, lihatBandingkan agen EC2 peluncuran Amazon.

EC2Launch v2 melakukan tugas selama startup instance dan berjalan jika instance dihentikan dan kemudian dimulai, atau dimulai ulang. EC2Launch v2 juga dapat melakukan tugas sesuai permintaan. Beberapa dari tugas ini diaktifkan secara otomatis, sementara yang lainnya harus diaktifkan secara manual. Layanan EC2 Launch v2 mendukung semua fitur EC2 Config dan EC2 Launch.

Layanan ini menggunakan file konfigurasi untuk mengontrol operasinya. Anda dapat memperbarui file konfigurasi dengan menggunakan alat grafis atau dengan mengeditnya secara langsung sebagai file .yml tunggal (`agent-config.yml`). Untuk informasi selengkapnya tentang lokasi file, lihatEC2Luncurkan struktur direktori v2.

EC2Launch v2 menerbitkan log peristiwa Windows untuk membantu Anda memecahkan masalah kesalahan dan mengatur pemicu. Untuk informasi selengkapnya, lihat Log peristiwa Windows.

Versi OS yang didukung

Agen EC2 Launch v2 mendukung versi sistem operasi (OS) Windows Server berikut:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019 (Saluran Layanan Jangka Panjang dan Saluran Semi-Tahunan)
- Windows Server 2016

Tugas yang dijalankan secara default

Agen EC2 Launch v2 menjalankan tugas-tugas berikut hanya satu kali secara default selama peluncuran instance awal. Tugas diatur sesuai dengan urutan di mana mereka berjalan dalam tahap peluncuran mereka.

`Bootpanggung`

- extendRootPartition

`PreReadypanggung`

- activateWindows
- setDnsSuffix
- setAdminAccount

- setWallpaper

`PostReady`panggung

- startSsm

EC2Luncurkan konsep v2

Konsep-konsep berikut berguna untuk dipahami saat mempertimbangkan EC2 Peluncuran v2.

agen-konfigurasi

`agent-config`adalah file yang terletak di folder konfigurasi untuk EC2 Launch v2. Ini termasuk konfigurasi untuk boot, jaringanPreReady, dan PostReady tahapan. File ini digunakan untuk menentukan konfigurasi instans untuk tugas-tugas yang harus dijalankan saat AMI di-boot untuk pertama kali atau untuk waktu-waktu berikutnya.

Secara default, instalasi EC2 Launch v2 menginstal `agent-config` file yang menyertakan konfigurasi yang direkomendasikan yang digunakan di Amazon Windows standar. AMIs Anda dapat memperbarui file konfigurasi untuk mengubah pengalaman boot default untuk AMI Anda yang ditentukan oleh EC2 Launch v2. Untuk informasi selengkapnya tentang lokasi file, lihatEC2Luncurkan struktur direktori v2.

Frekuensi

Frekuensi tugas menentukan kapan tugas harus dijalankan, tergantung pada konteks boot. Sebagian besar tugas hanya memiliki satu frekuensi yang diizinkan. Anda dapat menentukan frekuensi untuk tugas `executeScript`.

Anda akan melihat frekuensi berikut di EC2Luncurkan konfigurasi tugas v2.

- Once - Tugas dijalankan sekali, saat AMI telah boot untuk pertama kali (selesai Sysprep).
- Selalu — Tugas berjalan setiap kali agen peluncuran berjalan. Agen peluncuran berjalan saat:
  - sebuah instans dimulai atau dimulai ulang
  - Layanan EC2 Peluncuran berjalan
  - `EC2Launch.exe run` diinvokasi

Panggung

Tahap adalah pengelompokan tugas logis yang dijalankan agen EC2 Launch v2. Beberapa tugas hanya dapat dijalankan dalam tahap tertentu. Yang lain dapat berjalan dalam beberapa tahap.

Saat menggunakan `agent-config.yml`, Anda harus menentukan daftar tahapan, dan daftar tugas untuk dijalankan dalam setiap tahap.

Layanan berjalan tahapan dalam urutan sebagai berikut:

Tahap 1: Boot

Tahap 2: Jaringan

Tahap 3: PreReady

Windows sudah siap

Setelah PreReady tahap selesai, layanan mengirimkan `Windows is ready` pesan ke konsol Amazon EC2.

Tahap 4: PostReady

Data pengguna berjalan selama PostReadytahap. Beberapa versi skrip berjalan sebelum PostReadytahap `agent-config.yml` file, dan beberapa berjalan setelahnya, sebagai berikut:

Sebelum `agent-config.yml`

- Data pengguna YAML versi 1.1
- Data pengguna XML

Setelah `agent-config.yml`

- Data pengguna YAMB versi 1.0 (versi warisan untuk kompatibilitas mundur)

Untuk contoh tahapan dan tugas, lihat Contoh: `agent-config.yml`.

Saat Anda menggunakan data pengguna, Anda harus menentukan daftar tugas agar agen peluncuran dijalankan. Panggung tersirat. Untuk contoh tugas, lihat Contoh: data pengguna.

EC2Launch v2 menjalankan daftar tugas dalam urutan yang Anda tentukan dalam `agent-config.yml` dan dalam data pengguna. Tahapan berjalan secara berurutan. Tahap selanjutnya dimulai setelah tahap sebelumnya selesai. Tugas juga berjalan secara berurutan.

Tugas

Anda dapat menginvokasi tugas untuk melakukan tindakan pada sebuah instans. Anda dapat mengonfigurasi tugas dalam file `agent-config.yml` atau melalui data pengguna. Untuk daftar

tugas yang tersedia untuk EC2 Luncurkan v2, lihat EC2Meluncurkan tugas v2. Untuk skema konfigurasi tugas dan detailnya, lihat EC2Luncurkan konfigurasi tugas v2.

Data pengguna

Data pengguna adalah data yang dapat dikonfigurasi saat Anda meluncurkan sebuah instans. Anda dapat memperbarui data pengguna untuk secara dinamis mengubah cara kustom AMIs atau quickstart AMIs dikonfigurasi. EC2Launch v2 mendukung panjang input data pengguna 60 kB. Data pengguna hanya mencakup UserData tahap, dan karena itu berjalan setelah `agent-config` file. Anda dapat memasukkan data pengguna ketika Anda meluncurkan sebuah instans menggunakan wizard peluncuran instans, atau Anda dapat memodifikasi data pengguna dari konsol EC2. Untuk informasi lebih lanjut tentang bekerja dengan data pengguna, lihat Bagaimana Amazon EC2 menangani data pengguna untuk instans Windows.

EC2Luncurkan ikhtisar tugas v2

EC2Launch v2 dapat melakukan tugas-tugas berikut di setiap boot:

- Siapkan wallpaper baru dan yang disesuaikan secara opsional yang menyajikan informasi tentang instans.
- Setel atribut untuk akun administrator yang dibuat di mesin lokal.
- Tambahkan sufiks DNS ke daftar sufiks pencarian. Hanya sufiks yang belum ada yang ditambahkan ke daftar.
- Atur huruf drive untuk volume tambahan dan perluas untuk menggunakan ruang yang tersedia.
- Tulis file dari konfigurasi ke disk.
- Jalankan skrip yang ditentukan dalam file konfigurasi EC2 Launch v2 atau dari. `user-data` Skrip dari `user-data` dapat berupa teks biasa atau zip dan disediakan sebagai format base64.
- Jalankan program dengan argumen yang diberikan.
- Tetapkan nama komputer.
- Kirim informasi instans ke konsol Amazon EC2.
- Kirim sidik jari sertifikat RDP ke konsol Amazon EC2.
- Secara dinamis, perluas partisi sistem operasi untuk menyertakan ruang yang tidak dipartisi.
- Jalankan data pengguna. Untuk informasi selengkapnya tentang menentukan data pengguna, lihat EC2Luncurkan konfigurasi tugas v2.
- Setel rute statis non-persisten untuk menjangkau layanan metadata dan server. AWS KMS
- Setel partisi non-boot ke `mbr` atau. `gpt`

- Mulai layanan Systems Manager setelah Sysprep.
- Optimalkan pengaturan ENA.
- Aktifkan OpenSSH untuk versi Windows yang lebih baru.
- Aktifkan Jumbo Frame.
- Setel Sysprep untuk dijalankan dengan EC2 Launch v2.
- Publikasikan log peristiwa Windows.

EC2Luncurkan struktur direktori v2

EC2Peluncuran v2 harus diinstal di direktori berikut:

- Biner layana: `%ProgramFiles%\Amazon\EC2Launch`
- Data layanan (pengaturan, file log, dan file statu): `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> Secara default, Windows menyembunyikan file dan folder dalam `C:\ProgramData`. Untuk melihat direktori dan file EC2 Launch v2, Anda harus memasukkan jalur di Windows Explorer atau mengubah properti folder untuk menampilkan file dan folder tersembunyi.

Direktori `%ProgramFiles%\Amazon\EC2Launch` berisi binari dan pustaka pendukung. Ini mencakup subdirektori berikut:

- `settings`
  - `EC2LaunchSettingsUI.exe`— antarmuka pengguna untuk memodifikasi file `agent-config.yml`
  - `YamlDotNet.dll`— DLL untuk mendukung beberapa operasi di antarmuka pengguna
- `tools`
  - `ebsnvme-id.exe`— alat untuk memeriksa metadata volume EBS pada instance
  - `AWSAcpiSpcrReader.exe`— alat untuk menentukan port COM yang benar untuk digunakan
  - `EC2LaunchEventMessage.dll`- DLL untuk mendukung pencatatan peristiwa Windows untuk EC2 Peluncuran
- `service`

  - `EC2LaunchService.exe`— Layanan Windows yang dapat dieksekusi yang diluncurkan ketika agen peluncuran berjalan sebagai layanan
- `EC2AgentTelemetry.dll`- DLL untuk mendukung telemetri agen EC2
- `EC2Launch.exe`— EC2 Peluncuran utama yang dapat dieksekusi
- `EC2LaunchAgentAttribution.txt`— atribusi untuk kode yang digunakan dalam Peluncuran EC2

Direktori `%ProgramData%\Amazon\EC2Launch` berisi subdirektori berikut. Semua data yang dihasilkan oleh layanan, termasuk log, konfigurasi, dan status, disimpan di direktori ini.

- `config`— Konfigurasi

  File konfigurasi layanan disimpan dalam direktori ini sebagai `agent-config.yml`. File ini dapat diperbarui untuk mengubah, menambah, atau menghapus tugas default yang dijalankan oleh layanan. Izin untuk membuat file di direktori ini dibatasi untuk akun administrator untuk mencegah eskalasi hak istimewa.
- `log`— Log contoh

  Log untuk service (`agent.log`), performance (`bench.log`), dan telemetry (`telemetry.log`) disimpan di direktori ini. Ketika `agent.log` mencapai ukuran 1 MB, itu secara otomatis diputar dan file cadangan dibuat dengan format stempel waktu (misalnya,). `agent-2026-03-02T18-56-39.188.log` Hanya satu file log cadangan yang dipertahankan pada satu waktu.
- `state`— Data status layanan

  Status yang digunakan layanan untuk menentukan tugas mana yang harus dijalankan disimpan di sini. Ada sebuah file `.run-once` yang menunjukkan apakah layanan telah dijalankan setelah Sysprep (jadi tugas dengan frekuensi sekali akan dilewati pada proses berikutnya). Subdirektori ini mencakup `state.json` dan `previous-state.json` untuk melacak status setiap tugas.
- `sysprep`— Sysprep

  Direktori ini berisi file yang digunakan untuk menentukan operasi mana yang akan dilakukan oleh Sysprep saat membuat AMI Windows kustom yang dapat digunakan kembali.
- `wallpaper`— Wallpaper

  Gambar wallpaper ini disimpan di direktori ini.

Telemetri

Telemetri adalah informasi tambahan yang membantu AWS untuk lebih memahami kebutuhan Anda, mendiagnosis masalah, dan memberikan fitur untuk meningkatkan pengalaman Anda. Layanan AWS

EC2Luncurkan versi v2 `2.1.592` dan kemudian kumpulkan telemetri, seperti metrik penggunaan dan kesalahan. Data ini dikumpulkan dari instans Amazon EC2 tempat EC2 Launch v2 berjalan. Ini termasuk semua Windows yang AMIs dimiliki oleh AWS.

Jenis telemetri berikut dikumpulkan oleh EC2 Launch v2:

- Informasi penggunaan — perintah agen, metode penginstalan, dan frekuensi eksekusi terjadwal.
- Kesalahan dan informasi diagnostik - kode kesalahan instalasi agen, jalankan kode kesalahan, dan tumpukan panggilan kesalahan.

Contoh data yang dikumpulkan dari versi 2.0.592 hingga 2.1.1:

```
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AdminPasswordTypeCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IpConflictDetectionCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentErrorLocation=addroutes.go:49
```

Dimulai dengan versi 2.2.63, data telemetri Agen EC2 diformat sebagai objek JSON:

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2" ... }
```

Telemetri tidak diaktifkan secara default. Anda dapat menonaktifkan kumpulan telemetri kapan saja.

Menonaktifkan telemetri pada sebuah instans

Untuk menonaktifkan telemetri untuk satu instans, Anda dapat mengatur variabel lingkungan sistem, atau menggunakan MSI untuk memodifikasi instalasi.

Untuk menonaktifkan telemetri dengan menyetel variabel lingkungan sistem, jalankan perintah berikut sebagai administrator.

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Untuk menonaktifkan telemetri menggunakan MSI, jalankan perintah berikut setelah Anda mengunduh MSI.

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Topik lainnya untuk EC2 Launch v2

- Instal versi terbaru EC2 Launch v2
- Konfigurasikan pengaturan EC2 Launch v2 untuk instance Windows
- Definisi tugas untuk tugas startup EC2 Launch v2
- Memecahkan masalah dengan agen EC2 Launch v2
- EC2Luncurkan riwayat versi v2

Instal versi terbaru EC2 Launch v2

Anda dapat menggunakan salah satu metode berikut untuk menginstal agen EC2Launch v2 pada instans EC2 Anda:

- Unduh agen dari Amazon S3 dan instal dengan Windows. PowerShell Untuk mengunduh URLs, lihatEC2Luncurkan unduhan v2 di Amazon S3.
- Instal dengan Distributor SSM.
- Instal dari komponen EC2 Image Builder saat Anda membuat gambar kustom.
- Luncurkan instans Anda dari AMI yang telah diinstal sebelumnya EC2 Launch v2.

> **Warning**
>
> AmazonEC2Launch.msi menghapus versi sebelumnya dari layanan peluncuran EC2, seperti EC2 Launch (v1) dan Config. EC2

Untuk langkah penginstalan, pilih tab yang cocok dengan metode pilihan Anda.

PowerShell

Untuk menginstal versi terbaru dari agen EC2 Launch v2 dengan Windows PowerShell, ikuti langkah-langkah ini.

1. Buat direktori lokal Anda.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Tetapkan URL untuk lokasi unduhan Anda. Jalankan perintah berikut dengan URL Amazon S3 yang akan Anda gunakan. Untuk mengunduh URLs, lihat EC2Luncurkan unduhan v2 di Amazon S3

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Gunakan perintah majemuk berikut untuk mengunduh agen dan menjalankan penginstalan

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016 atau sebelumnya, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. msiexecPerintah menginstal EC2 Launch v2 di lokasi berikut pada instance Windows Server:. `%ProgramFiles%\Amazon\EC2Launch` Untuk memverifikasi bahwa instalasi berjalan, Anda dapat memeriksa sistem file lokal pada instance Anda.

AWS Systems Manager Distributor

Untuk mengonfigurasi pembaruan otomatis untuk EC2 Launch v2 dengan AWS Systems Manager Quick Setup, lihatInstal dan perbarui secara otomatis dengan Pengaturan Cepat Distributor.

Anda juga dapat melakukan instalasi satu kali `AWSEC2Launch-Agent` paket dari AWS Systems Manager Distributor. Untuk instruksi tentang cara menginstal paket dari Systems Manager

Distributor, lihat Menginstal atau memperbarui paket di Panduan Pengguna AWS Systems Manager .

EC2 Image Builder component

Anda dapat menginstal komponen `ec2launch-v2-windows` saat membuat gambar kustom dengan EC2 Image Builder. Untuk petunjuk tentang cara membuat gambar kustom dengan EC2 Image Builder, lihat Buat pipeline gambar menggunakan wizard konsol EC2 Image Builder di Panduan Pengguna EC2 Image Builder.

AMI

EC2Launch v2 sudah diinstal sebelumnya secara default AMIs untuk sistem operasi Windows Server 2022 dan di atasnya:

- Windows_Server- -Bahasa Inggris-Basis Penuh *version*
- Windows_Server- -Bahasa Inggris-Core-Base *version*
- Windows_Server- -Bahasa Inggris-Core-EKS_Optimized *version*
- Windows Server *version* AMIs dengan semua bahasa lainnya
- Windows Server *version* AMIs dengan SQL diinstal

EC2Launch v2 sudah diinstal sebelumnya di AMI Windows Server berikut. Anda dapat menemukan AMI ini dari konsol Amazon EC2, atau dengan menggunakan prefiks pencarian berikut: `EC2LaunchV2-` di AWS CLI.

- EC2LaunchV2-Windows_Server-2019-Inggris-core-base
- EC2LaunchV2-Windows_Server-2019-Inggris-basis penuh
- EC2LaunchV2-Windows_Server-2016-Inggris-core-base
- EC2LaunchV2-Windows_Server-2016-Bahasa Inggris-basis penuh

Secara otomatis menginstal dan memperbarui EC2 Launch v2 dengan AWS Systems Manager Distributor Quick Setup

Dengan Pengaturan Cepat AWS Systems Manager Distributor, Anda dapat mengatur pembaruan otomatis untuk EC2 Launch v2. Proses berikut menyiapkan Systems Manager Association pada instans Anda yang secara otomatis memperbarui agen EC2 Launch v2 pada frekuensi yang Anda tentukan. Asosiasi yang dibuat oleh Penyiapan Cepat Distributor dapat menyertakan instance dalam

Wilayah Akun AWS dan, atau instans dalam Organisasi. AWS Untuk informasi selengkapnya tentang menyiapkan organisasi, lihat Tutorial: Membuat dan mengonfigurasi organisasi di Panduan AWS Organizations Pengguna.

Sebelum Anda mulai, pastikan bahwa contoh Anda memenuhi semua prasyarat.

Prasyarat

Untuk mengatur pembaruan otomatis dengan Penyiapan Cepat Distributor, instans Anda harus memenuhi prasyarat berikut.

- Anda memiliki setidaknya satu instance berjalan yang mendukung EC2 Launch v2. Lihat sistem operasi yang didukung untukEC2Luncurkan v2.
- Anda telah melakukan tugas penyiapan Systems Manager pada instans Anda. Untuk informasi selengkapnya, lihat Menyiapkan Systems Manager di Panduan AWS Systems Manager Pengguna.
- EC2Launch v2 harus menjadi satu-satunya agen peluncuran yang diinstal pada instans Anda. Jika Anda memiliki lebih dari satu agen peluncuran yang diinstal, konfigurasi Pengaturan Cepat Distributor Anda akan gagal. Sebelum Anda mengonfigurasi EC2 Launch v2 dengan Distributor Quick Setup, hapus instalan EC2 Config EC2 atau Launch v1 launch agent, jika ada.

Konfigurasikan Pengaturan Cepat Distributor untuk EC2 Peluncuran v2

Untuk membuat konfigurasi EC2 Launch v2 dengan Penyiapan Cepat Distributor, gunakan pengaturan berikut saat Anda menyelesaikan langkah-langkah penerapan paket Distributor:

- Paket perangkat lunak: Amazon EC2 Launch v2 agent.
- Frekuensi pembaruan: Pilih frekuensi dari daftar.
- Target: Pilih dari opsi penerapan yang tersedia.

Untuk memeriksa status konfigurasi Anda, navigasikan ke tab Systems Manager Quick Setup Configurations di Konsol Manajemen AWS.

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Pengaturan Cepat.
3. Di tab Konfigurasi, pilih baris yang terkait dengan konfigurasi yang Anda buat. Tab Konfigurasi mencantumkan konfigurasi Anda, dan menyertakan ringkasan detail utama, seperti Region, status Deployment, dan status Asosiasi.

> **Note**
>
> Nama asosiasi untuk setiap konfigurasi EC2 Launch v2 Distributor dimulai dengan awalan berikut:`AWS-QuickSetup-Distributor-EC2Launch-Agent-`.

4. Untuk melihat detail, pilih konfigurasi dan pilih Lihat detail.

Untuk informasi selengkapnya dan langkah pemecahan masalah, lihat Memecahkan Masalah hasil Pengaturan Cepat di Panduan Pengguna.AWS Systems Manager

EC2Luncurkan unduhan v2 di Amazon S3

Untuk menginstal versi terbaru EC2 Launch v2, unduh penginstal dari lokasi berikut:

- https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi

Konfigurasikan opsi instalasi

Saat Anda menginstal atau memutakhirkan EC2 Launch v2, Anda dapat mengonfigurasi opsi instalasi dengan dialog EC2 Launch v2 install atau dengan msiexec perintah di shell baris perintah.

Pertama kali installer EC2 Launch v2 berjalan pada sebuah instance, ini menginisialisasi pengaturan agen peluncuran pada instance Anda sebagai berikut:

- Ini menciptakan jalur lokal dan menulis file agen peluncuran ke sana. Hal ini terkadang disebut sebagai instalasi bersih.
- Ini menciptakan variabel `EC2LAUNCH_TELEMETRY` lingkungan jika belum ada, dan menetapkannya berdasarkan konfigurasi Anda.

Untuk detail konfigurasi, pilih tab yang cocok dengan metode konfigurasi yang akan Anda gunakan.

Amazon EC2Launch Setup dialog

Saat Anda menginstal atau memutakhirkan EC2 Launch v2, Anda dapat mengonfigurasi opsi instalasi berikut melalui dialog EC2 Launch v2 install.

Opsi Instal Dasar

Kirim Telemetri

Saat Anda menyertakan fitur ini dalam dialog penyiapan, penginstal mengatur variabel lingkungan `EC2LAUNCH_TELEMETRY` ke nilai `1`. Jika Anda menonaktifkan Kirim Telemetri, penginstal menetapkan variabel lingkungan ke nilai. `0`

Saat agen EC2 Launch v2 berjalan, ia membaca variabel `EC2LAUNCH_TELEMETRY` lingkungan untuk menentukan apakah akan mengunggah data telemetri. Jika nilainya sama dengan 1, agen menggunggah data. Jika tidak, itu tidak mengunggah.

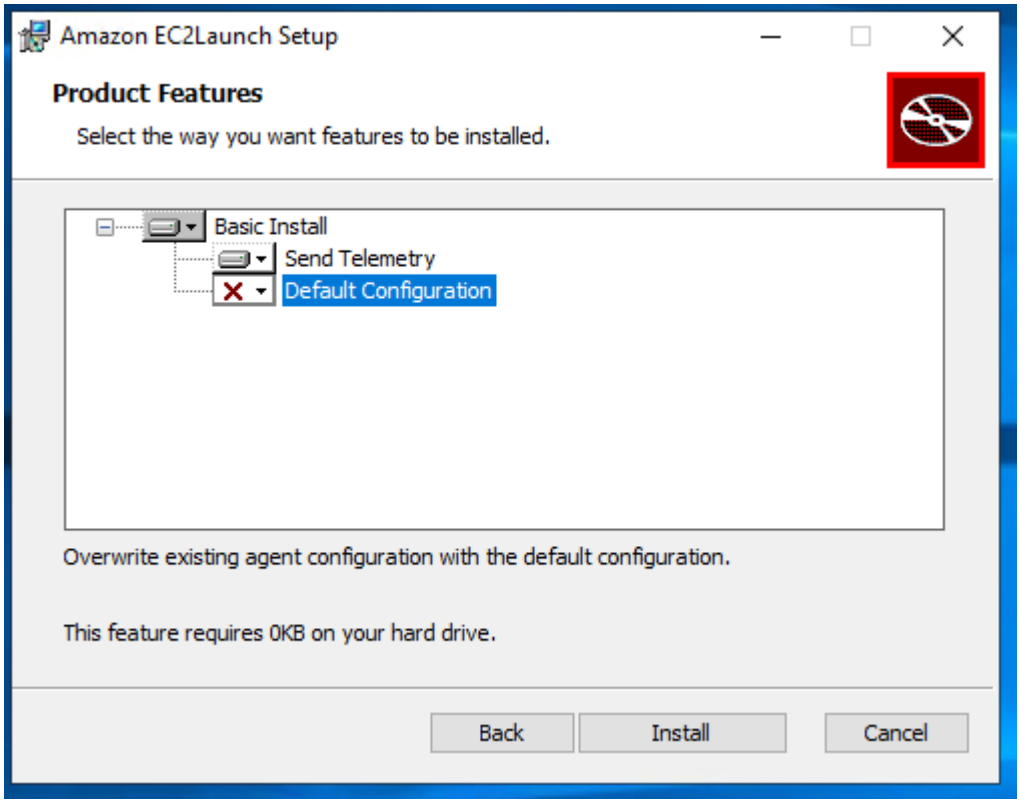
Konfigurasi default

Konfigurasi default untuk EC2 Launch v2 adalah menimpa agen peluncuran lokal jika sudah ada. Pertama kali Anda menjalankan instalasi pada sebuah instans, konfigurasi default melakukan instalasi bersih. Jika Anda menonaktifkan konfigurasi default pada instalasi awal, instalasi gagal.

Jika Anda menjalankan instalasi lagi pada instans, Anda dapat menonaktifkan konfigurasi default untuk melakukan pemutakhiran yang tidak menggantikan file `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`.

Contoh: Tingkatkan EC2 Peluncuran v2 dengan telemetri

Contoh berikut menunjukkan dialog setup EC2 Launch v2 yang dikonfigurasi untuk meng-upgrade instalasi saat ini dan mengaktifkan telemetri. Konfigurasi ini melakukan instalasi tanpa mengganti file konfigurasi agen, dan menetapkan variabel lingkungan `EC2LAUNCH_TELEMETRY` ke nilai `1`.



Command line

Saat Anda menginstal atau memutakhirkan EC2 Launch v2, Anda dapat mengonfigurasi opsi instalasi berikut dengan msiexec perintah di shell baris perintah.

Nilai parameter **`ADDLOCAL`**

Dasar (wajib)

Instal agen peluncuran. Jika nilai ini tidak ada dalam `ADDLOCAL` parameter, instalasi berakhir.

Bersih

Saat Anda menyertakan nilai `Clean` dalam parameter `ADDLOCAL`, penginstal menuliskan file konfigurasi agen ke lokasi berikut: `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Jika file konfigurasi agen sudah ada, file tersebut akan menimpa file.

Saat Anda membiarkan nilai `Clean` keluar dari parameter `ADDLOCAL`, penginstal melakukan pemutakhiran yang tidak menggantikan file konfigurasi agen.

Telemetri

Ketika Anda memasukkan nilai `Telemetry` dalam parameter `ADDLOCAL`, pengisntal mengatur variabel lingkungan `EC2LAUNCH_TELEMETRY` ke nilai `1`.

Ketika Anda membiarkan nilai `Telemetry` keluar dari parameter `ADDLOCAL`, pengintal menetapkan variabel lingkungan ke nilai `0`.

Saat agen EC2 Launch v2 berjalan, ia membaca variabel `EC2LAUNCH_TELEMETRY` lingkungan untuk menentukan apakah akan mengunggah data telemetri. Jika nilainya sama dengan 1, agen menggunggah data. Jika tidak, itu tidak mengunggah.

Contoh: instal EC2 Launch v2 dengan telemetri

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Verifikasi versi EC2 Launch v2

Gunakan salah satu prosedur berikut untuk memverifikasi versi EC2 Launch v2 yang diinstal pada instans Anda.

PowerShell

Verifikasi versi EC2 Launch v2 yang diinstal dengan Windows PowerShell, sebagai berikut.

1. Luncurkan sebuah instans dari AMI dan hubungkan diri Anda dengan instans tersebut.
2. Jalankan perintah berikut PowerShell untuk memverifikasi versi EC2 Launch v2 yang diinstal:

   ```
   & "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
   ```

Windows Control Panel

Verifikasi versi EC2 Launch v2 yang diinstal di Panel Kontrol Windows, sebagai berikut.

1. Luncurkan sebuah instans dari AMI dan hubungkan diri Anda dengan instans tersebut.
2. Buka Panel Kontrol Windows dan pilih Program dan Fitur.
3. Cari `Amazon EC2Launch` dalam daftar program yang diinstal. Nomor versinya muncul di kolom Versi.

Untuk melihat pembaruan terbaru untuk AWS Windows AMIs, lihat riwayat versi Windows AMI di Referensi AMI AWS Windows.

Untuk versi terbaru dari EC2 Launch v2, lihatEC2Luncurkan riwayat versi v2.

Anda dapat menerima pemberitahuan ketika versi baru dari layanan EC2 Launch v2 dirilis. Lihat informasi yang lebih lengkap di Berlangganan pemberitahuan agen peluncuran EC2 Windows.

Konfigurasikan pengaturan EC2 Launch v2 untuk instance Windows

Bagian ini berisi informasi tentang cara mengkonfigurasi pengaturan untuk EC2 Launch v2.

Topiknya mencakup:

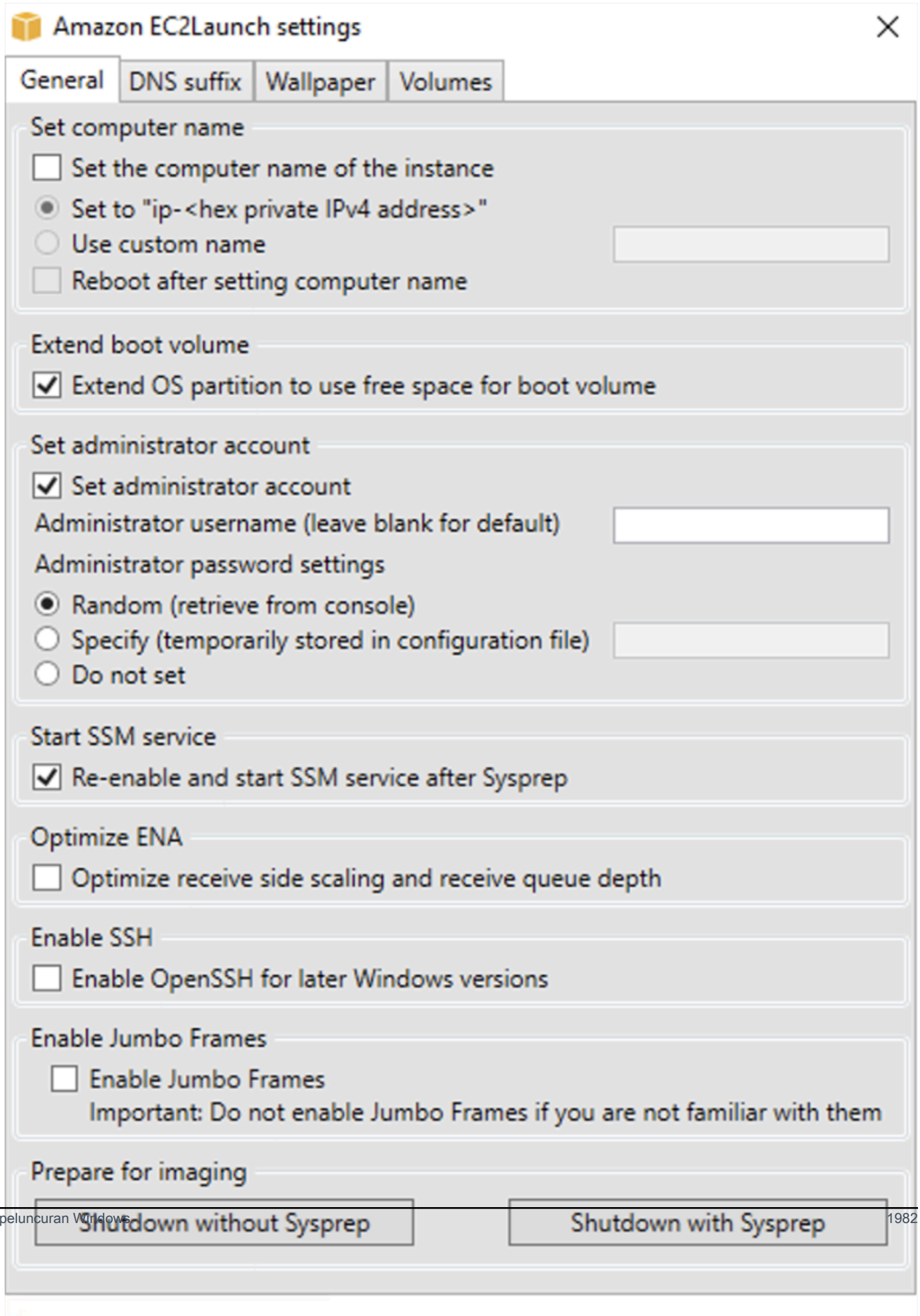
- Ubah pengaturan menggunakan kotak dialog EC2 Launch v2 settings
- Konfigurasikan EC2 Launch v2 menggunakan CLI
- EC2Luncurkan konfigurasi tugas v2
- EC2Luncurkan kode keluar v2 dan reboot
- EC2Luncurkan v2 dan Sysprep

Ubah pengaturan menggunakan kotak dialog EC2 Launch v2 settings

Prosedur berikut menjelaskan cara menggunakan kotak dialog pengaturan EC2 Launch v2 untuk mengaktifkan atau menonaktifkan pengaturan.

> **Note**
>
> Jika Anda mengonfigurasi tugas khusus secara tidak benar di file agent-config.yml. dan Anda mencoba membuka kotak dialog pengaturan EC2 Peluncuran Amazon, Anda akan menerima kesalahan. Untuk contoh skema, lihat Contoh: `agent-config.yml`.

1. Jalankan dan hubungkan ke instans Windows Anda.
2. Dari menu Start, pilih All Programs, lalu navigasikan ke EC2Launch settings. Sebelum Anda memilih Shutdown dengan Sysprep atau Shutdown tanpa Sysprep, pastikan bahwa Anda menyimpan setiap perubahan yang ingin Anda terapkan ketika Anda menjalankan shutdown.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set computer name
Set the computer name of the instance
Set to "ip-<hex private IPv4 address>"
Use custom name
Reboot after setting computer name
Extend boot volume
Extend OS partition to use free space for boot volume
Set administrator account
Set administrator account
Administrator username (leave blank for default)
Administrator password settings
Random (retrieve from console)
Specify (temporarily stored in configuration file)
Do not set
Start SSM service
Re-enable and start SSM service after Sysprep
Optimize ENA
Optimize receive side scaling and receive queue depth
Enable SSH
Enable OpenSSH for later Windows versions
Enable Jumbo Frames
Enable Jumbo Frames
Important: Do not enable Jumbo Frames if you are not familiar with them
Prepare for imaging
Shutdown without Sysprep
Shutdown with Sysprep

3. Pada tab Umum dari kotak dialog Pengaturan EC2 peluncuran, Anda dapat mengaktifkan atau menonaktifkan pengaturan berikut.

   a. Atur Nama Komputer

      Jika pengaturan ini diaktifkan (dinonaktifkan secara default), maka nama host saat ini dibandingkan dengan nama host yang diinginkan di setiap boot. Jika nama host tidak cocok, maka nama host disetel ulang, dan sistem kemudian secara opsional melakukan boot ulang untuk mengambil nama host baru. Jika nama host kustom tidak ditentukan, itu dihasilkan menggunakan alamat pribadi IPv4 berformat heksadesimal, misalnya,. `ip-AC1F4E6` Untuk mencegah perubahan nama host yang ada, jangan aktifkan pengaturan ini.

   b. Perpanjang Volume Boot

      Pengaturan ini secara dinamis memperluas `Disk 0`/`Volume 0` untuk memasukkan ruang yang tidak dipartisi. Ini dapat berguna ketika instance di-boot dari volume root yang memiliki ukuran khusus.

   c. Atur Akun Administrator

      Saat diaktifkan, Anda dapat mengatur atribut nama pengguna dan kata sandi untuk akun administrator yang dibuat di mesin lokal Anda. Jika fitur ini tidak diaktifkan, akun administrator tidak dibuat di sistem setelah Sysprep. Berikan kata sandi dalam`adminPassword` hanya jika`adminPasswordtype` adalah`Specify`.

      Jenis kata sandi ditentukan sebagai berikut:

      i. `Random`

         EC2Peluncuran menghasilkan kata sandi dan mengenkripsi menggunakan kunci pengguna. Sistem akan menonaktifkan pengaturan ini setelah instans dijalankan sehingga kata sandi ini akan tetap ada jika instans tersebut di-boot ulang atau dihentikan dan dimulai.

      ii. `Specify`

         EC2Peluncuran menggunakan kata sandi yang Anda tentukan`adminPassword`. Jika kata sandi tidak memenuhi persyaratan sistem, EC2 Launch menghasilkan kata sandi acak sebagai gantinya. Kata sandi disimpan di `agent-config.yml` sebagai teks polos dan dihapus setelah Sysprep mengatur kata sandi administrator. EC2Luncurkan mengenkripsi kata sandi menggunakan kunci pengguna.

iii. `Do not set`

EC2Peluncuran menggunakan kata sandi yang Anda tentukan dalam file unattend.xml. Jika Anda tidak menentukan kata sandi di unattend.xml, akun administrator dinonaktifkan.

d. Mulai Layanan SSM

Ketika dipilih, layanan Systems Manager diaktifkan untuk mulai mengikuti Sysprep. EC2Launch v2 melakukan semua tugas yang dijelaskan sebelumnya, dan Agen SSM memproses permintaan untuk kemampuan Systems Manager, seperti Run Command dan State Manager.

Anda dapat menggunakan Run Command untuk memutakhirkan instans yang ada untuk menggunakan versi terbaru dari layanan EC2 Launch v2 dan Agen SSM. Untuk informasi selengkapnya, lihat Memperbarui Agen SSM menggunakan Run Command di Panduan Pengguna AWS Systems Manager.

e. Optimalkan ENA

Saat dipilih, pengaturan ENA dikonfigurasi untuk memastikan bahwa pengaturan ENA Receive Side Scaling dan Receive Queue Depth dioptimalkan. AWS Untuk informasi selengkapnya, lihat Konfigurasikan afinitas CPU penskalaan sisi Terima.

f. Aktifkan SSH

Pengaturan ini memungkinkan OpenSSH untuk versi Windows yang lebih baru untuk memungkinkan administrasi sistem jarak jauh.

g. Aktifkan Jumbo Frame

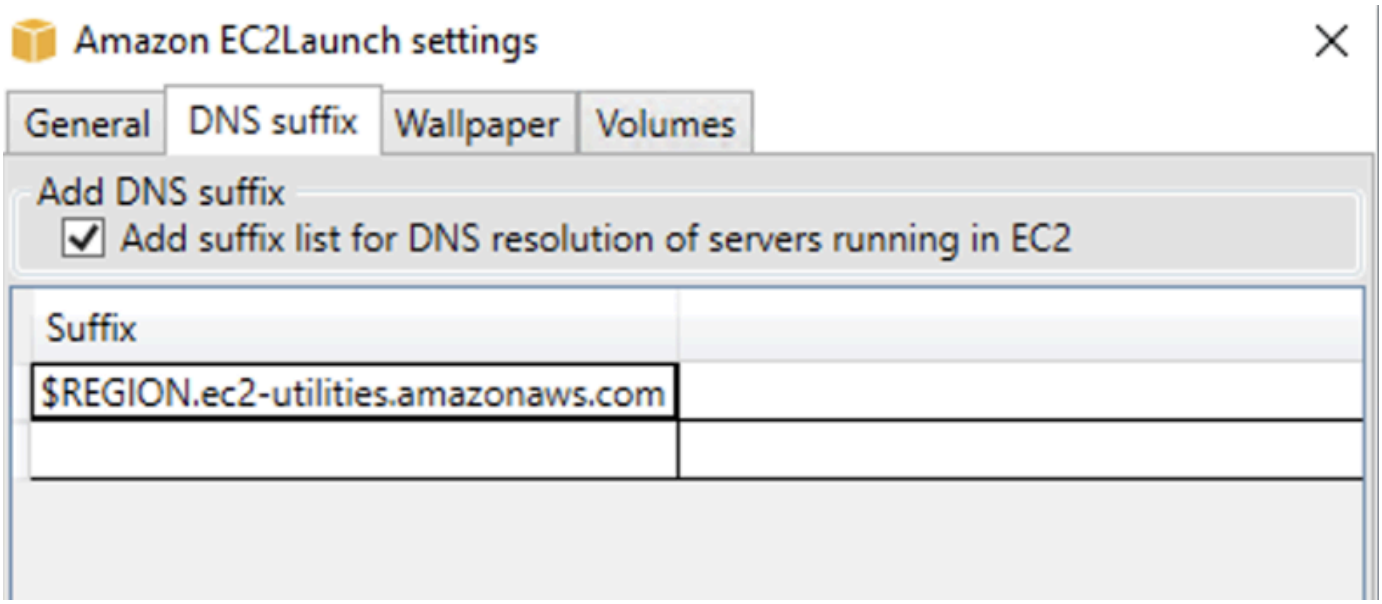
Pilih untuk mengaktifkan Jumbo Frames. Jumbo Frames dapat memiliki efek yang tidak diinginkan pada komunikasi jaringan Anda, jadi pastikan Anda memahami bagaimana Jumbo Frames akan memengaruhi sistem Anda sebelum mengaktifkan. Untuk informasi selengkapnya tentang Jumbo Frames, lihat Frame jumbo (9001 MTU).

h. Persiapkan untuk Pencitraan

Pilih apakah Anda ingin instans EC2 Anda dimatikan dengan atau tanpa Sysprep. Ketika Anda ingin menjalankan Sysprep dengan EC2 Launch v2, pilih Shutdown with Sysprep.

4. Pada tab Sufiks DNS, Anda dapat memilih apakah Anda ingin menambahkan daftar sufiks DNS untuk resolusi DNS dari server yang berjalan di EC2, tanpa memberikan nama domain yang

memenuhi syarat. Sufiks DNS dapat berisi variabel `$REGION` dan `$AZ`. Hanya sufiks yang belum ada yang akan ditambahkan ke daftar.

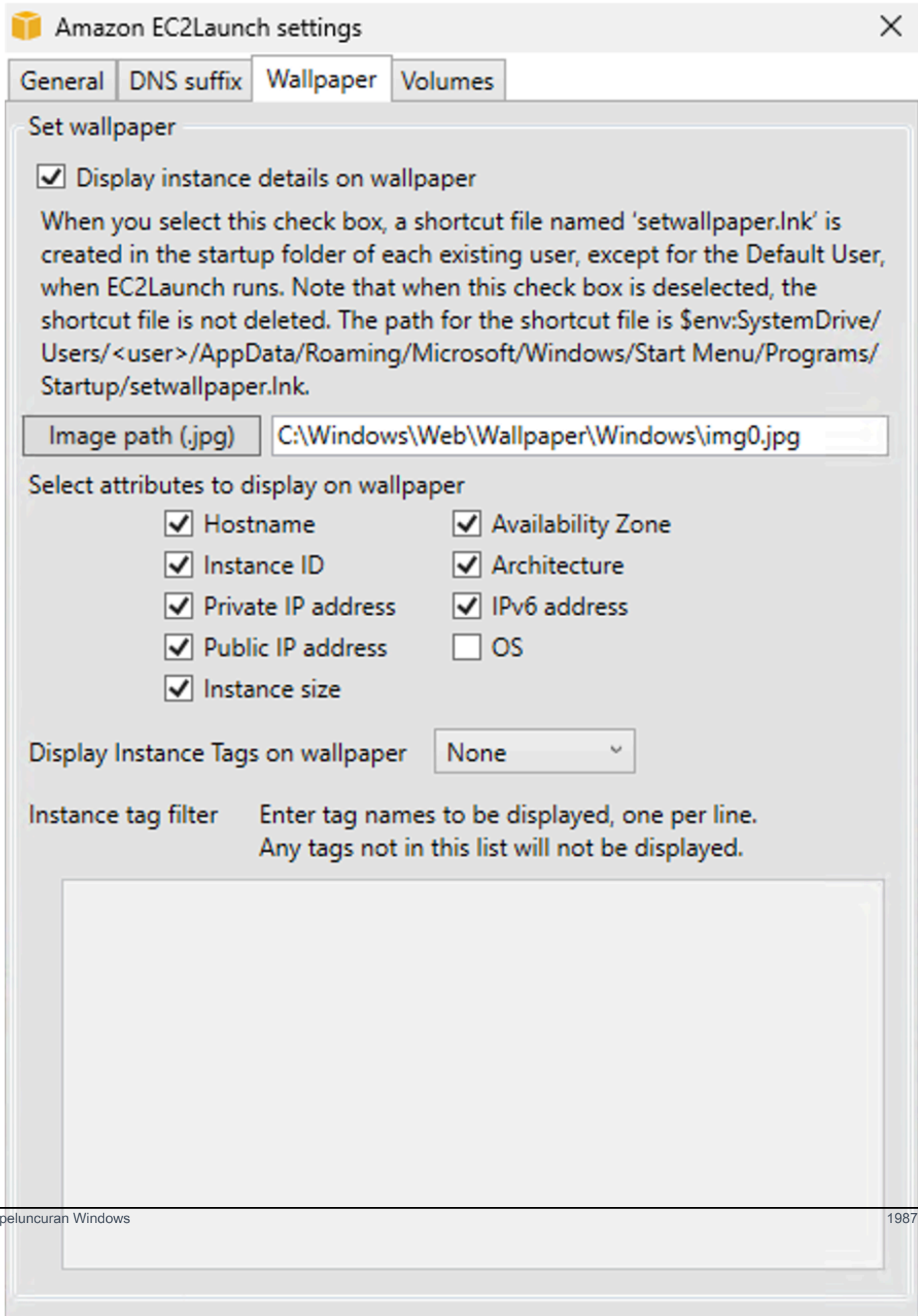


5. Pada tab Wallpaper, Anda dapat mengonfigurasi wallpaper instans Anda dengan gambar latar belakang, dan menentukan detail instans untuk wallpaper yang akan ditampilkan. Amazon EC2 menghasilkan detail setiap kali Anda masuk.

   Anda dapat mengonfigurasi wallpaper Anda dengan kontrol berikut.

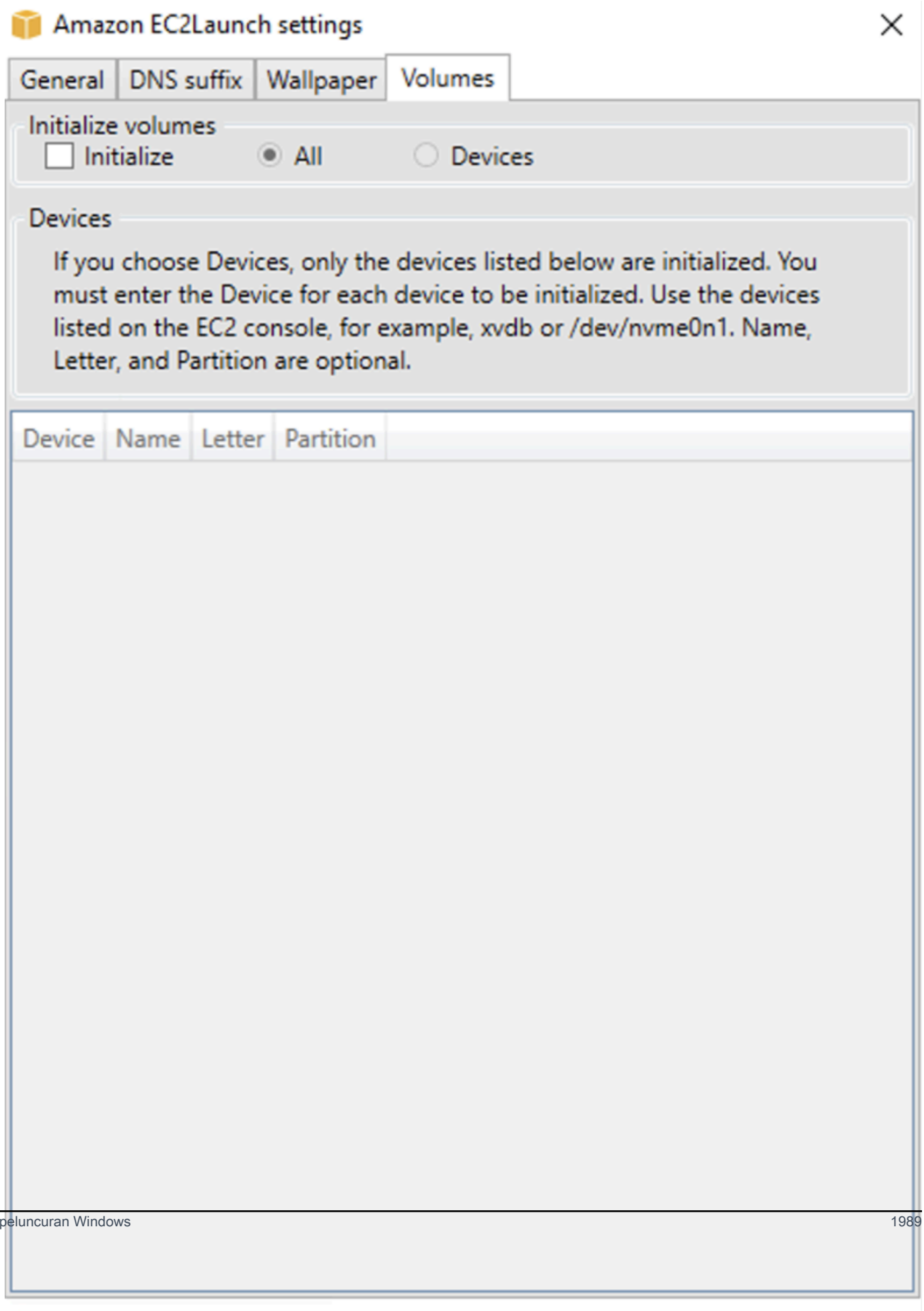
   - Tampilkan detail instans pada wallpaper — Kotak centang ini mengaktifkan atau menonaktifkan tampilan detail instans pada wallpaper.
   - Jalur gambar (.jpg) - Tentukan jalur ke gambar yang akan digunakan sebagai latar belakang wallpaper.
   - Pilih atribut yang akan ditampilkan di wallpaper — Pilih kotak centang untuk detail instans yang ingin Anda tampilkan di wallpaper. Hapus kotak centang untuk detail instans yang dipilih sebelumnya yang akan Anda hapus dari wallpaper.
   - Tampilkan Tanda Instans pada wallpaper - Pilih salah satu pengaturan berikut untuk menampilkan tanda instans pada wallpaper:
     - Tidak ada - Jangan tampilkan tanda instans apa pun di wallpaper.
     - Tampilkan semua — Tampilkan semua tanda instans pada wallpaper.
     - Tampilkan difilter - Tampilkan tanda instans tertentu pada wallpaper. Saat memilih pengaturan ini, Anda dapat menambahkan tanda instans yang ingin ditampilkan di wallpaper di kotak filter tanda instans.

> **Note**
>
> Anda harus mengaktifkan tanda dalam metadata untuk menampilkan tanda pada wallpaper. Untuk informasi selengkapnya tentang tanda instans dan metadata, lihat Lihat tag untuk instans EC2 Anda menggunakan metadata instans.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set wallpaper
Display instance details on wallpaper
When you select this check box, a shortcut file named 'setwallpaper.lnk' is created in the startup folder of each existing user, except for the Default User, when EC2Launch runs. Note that when this check box is deselected, the shortcut file is not deleted. The path for the shortcut file is $env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk.
Image path (.jpg)
C:\Windows\Web\Wallpaper\Windows\img0.jpg
Select attributes to display on wallpaper
Hostname
Instance ID
Private IP address
Public IP address
Instance size
Availability Zone
Architecture
IPv6 address
OS
Display Instance Tags on wallpaper
None
Instance tag filter
Enter tag names to be displayed, one per line.
Any tags not in this list will not be displayed.

6. Pada tab Volume, pilih apakah Anda ingin menginisialisasi volume yang dilampirkan ke instans. Mengaktifkan set huruf drive untuk volume tambahan dan memperluasnya untuk menggunakan ruang yang tersedia. Jika Anda memilih Semua, semua volume penyimpanan diinisialisasi. Jika Anda memilih Perangkat, hanya perangkat yang ditentukan dalam daftar yang diinisialisasi. Anda harus memasukkan perangkat untuk setiap perangkat yang akan diinisialisasi. Gunakan peranti yang terdaftar pada konsol EC2, sebagai contoh, `xvdb` atau `/dev/nvme0n1`. Daftar dropdown menampilkan volume penyimpanan yang dilampirkan pada instans. Untuk memasukkan perangkat yang tidak terpasang ke instans, masukkan perangkat itu di bidang teks.

   Nama, Huruf, dan Partisi adalah bidang opsional. Jika tidak ada nilai yang ditentukan untuk Partisi, volume penyimpanan yang lebih besar dari 2 TB diinisialisasi dengan jenis `gpt` partisi, dan yang lebih kecil dari 2 TB diinisialisasi dengan jenis `mbr` partisi. Jika perangkat dikonfigurasi, dan perangkat non-NTFS berisi tabel partisi, atau 4 KB pertama dari disk berisi data, maka disk akan dilewati dan tindakan dicatat.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Initialize volumes
Initialize
All
Devices
Devices
If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.
Device
Name
Letter
Partition

Konfigurasikan EC2 Launch v2 menggunakan CLI

Anda dapat menggunakan Command Line Interface (CLI) untuk mengonfigurasi pengaturan EC2 Peluncuran Anda dan mengelola layanan. Bagian berikut berisi deskripsi dan informasi penggunaan untuk perintah CLI yang dapat Anda gunakan untuk EC2 mengelola Launch v2.

Commands

- collect-logs
- get-agent-config
- list-volumes
- atur ulang
- run
- status
- sysprep
- validasi
- versi
- wallpaper

collect-logs

Mengumpulkan file log untuk EC2 Launch, zip file, dan menempatkannya di direktori tertentu.

Contoh

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Penggunaan

```
ec2launch collect-logs [flags]
```

Bendera

`-h, --help`

bantuan untuk `collect-logs`

`-o, --output string`

jalur ke file log output zip

get-agent-config

Mencetak `agent-config.yml` dalam format yang ditentukan (JSON atau YAML). Jika tidak ada format yang ditentukan, `agent-config.yml` dicetak dalam format yang ditentukan sebelumnya.

Contoh

```
ec2launch get-agent-config -f json
```

Penggunaan

`ec2launch get-agent-config [flags]`

Bendera

`-h, --help`

bantuan untuk `get-agent-config`

`-f, --format string`

format output file `agent-config`: `json`, `yaml`

list-volumes

Mencantumkan semua volume penyimpanan yang dilampirkan ke instans, termasuk volume singkat dan EBS.

Contoh

```
ec2launch list-volumes
```

Penggunaan

`ec2launch list-volumes`

Bendera

`-h, --help`

bantuan untuk `list-volumes`

atur ulang

Tujuan utama dari tugas ini adalah untuk mengatur ulang agen untuk waktu berikutnya yang dijalankan. Untuk melakukan itu, reset perintah menghapus semua data status agen untuk EC2 Launch v2 dari `EC2Launch` direktori lokal (lihatEC2Luncurkan struktur direktori v2). Reset opsional menghapus layanan dan log Sysprep.

Perilaku skrip tergantung pada mode apa agen menjalankan skrip — inline, atau terpisah.

Inline (default)

Agen EC2 Launch v2 menjalankan skrip satu per satu (`detach: false`). Ini adalah pengaturan default.

> **Note**
>
> Ketika skrip inline Anda mengeluarkan perintah reset atau sysprep, skrip tersebut segera berjalan dan mengatur ulang agen. Tugas saat ini selesai, kemudian agen dimatikan tanpa menjalankan tugas lebih lanjut.
> Misalnya, jika tugas yang mengeluarkan perintah akan diikuti oleh `startSsm` tugas (disertakan secara default setelah data pengguna berjalan), tugas tidak berjalan dan layanan Systems Manager tidak pernah dimulai.

Terlepas

Agen EC2 Launch v2 menjalankan skrip bersamaan dengan tugas lain ()`detach: true`.

> **Note**
>
> Saat skrip terpisah Anda mengeluarkan reset atau sysprep, perintah tersebut menunggu agen selesai sebelum dijalankan. Tugas setelah executeScript masih akan berjalan.

Contoh

```
ec2launch reset -c
```

Penggunaan

`ec2launch reset [flags]`

Bendera

`-c`, `--clean`

membersihkan log instans sebelum `reset`

`-h`, `--help`

bantuan untuk `reset`

run

Menjalankan EC2 Peluncuran v2.

Contoh

```
ec2launch run
```

Penggunaan

`ec2launch run [flags]`

Bendera

`-h`, `--help`

bantuan untuk `run`

status

Mendapat status agen EC2 Launch v2. Memblokir proses secara opsional sampai agen selesai. Kode keluar proses menentukan status agen:

- `0` – agen berjalan dan berhasil.
- `1` – agen berjalan dan gagal.
- `2` – agen masih berjalan.
- `3` – agen dalam status yang tidak diketahui. Status agen tidak berjalan atau berhenti.
- `4` – kesalahan terjadi ketika mencoba untuk mengambil status agen.
- `5` – agen tidak berjalan dan status berjalan terakhir yang diketahui tidak diketahui. Ini bisa berarti salah satu dari berikut ini:

- kedua `state.json` dan `previous-state.json` dihapus.
- `previous-state.json` rusak.

Ini adalah status agen setelah menjalankan perintah `reset`.

Contoh:

```
ec2launch status -b
```

Penggunaan

`ec2launch status [flags]`

Bendera

`-b,--block`

memblokir proses sampai agen selesai berjalan

`-h,--help`

bantuan untuk `status`

sysprep

Tujuan utama dari tugas ini adalah untuk mengatur ulang agen untuk waktu berikutnya yang dijalankan. Untuk melakukan itu, perintah sysprep mengatur ulang status agen, memperbarui file `unattend.xml`, menonaktifkan RDP, dan menjalankan Sysprep.

Perilaku skrip tergantung pada mode apa agen menjalankan skrip — inline, atau terpisah.

Inline (default)

Agen EC2 Launch v2 menjalankan skrip satu per satu (`detach: false`). Ini adalah pengaturan default.

> **Note**
>
> Ketika skrip inline Anda mengeluarkan perintah reset atau sysprep, skrip tersebut segera berjalan dan mengatur ulang agen. Tugas saat ini selesai, kemudian agen dimatikan tanpa menjalankan tugas lebih lanjut.

Misalnya, jika tugas yang mengeluarkan perintah akan diikuti oleh `startSsm` tugas (disertakan secara default setelah data pengguna berjalan), tugas tidak berjalan dan layanan Systems Manager tidak pernah dimulai.

Terlepas

Agen EC2 Launch v2 menjalankan skrip bersamaan dengan tugas lain ()`detach: true`.

> **Note**
>
> Saat skrip terpisah Anda mengeluarkan reset atau sysprep, perintah tersebut menunggu agen selesai sebelum dijalankan. Tugas setelah executeScript masih akan berjalan.

Contoh:

```
ec2launch sysprep
```

Penggunaan

`ec2launch sysprep [flags]`

Bendera

`-c,--clean`

membersihkan log instans sebelum `sysprep`

`-h,--help`

bantuan untuk Sysprep

`-s,--shutdown`

mematikan instans setelah `sysprep`

validasi

Memvalidasi `agent-config` file `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Contoh

```
ec2launch validate
```

Penggunaan

`ec2launch validate [flags]`

Bendera

-h , `--help`

bantuan untuk `validate`

versi

Mendapatkan versi yang dapat dieksekusi.

Contoh

```
ec2launch version
```

Penggunaan

`ec2launch version [flags]`

Bendera

`-h`, `--help`

bantuan untuk `version`

wallpaper

Menyetel wallpaper baru ke jalur wallpaper yang disediakan (file.jpg), dan menampilkan detail instans yang dipilih.

Sintaksis

```
ec2launch wallpaper ^
```

```
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,ipv6Address,instanceSize,availa
```

Masukan

Parameter

--allowed-tag [,] ***tag-name-1 tag-name-n***

(Opsional) Base64 mengenkode array JSON dari nama tanda instans untuk ditampilkan di wallpaper. Anda dapat menggunakan tanda ini atau `--all-tags`, tetapi tidak keduanya.

--atribut***attribute-string-1***, ***attribute-string-n***

(Opsional) Daftar string atribut `wallpaper` yang dipisahkan dengan koma untuk menerapkan pengaturan ke wallpaper.

[--jalur | -p] ***path-string***

(Wajib) Menentukan jalur file gambar latar belakang `wallpaper`.

Bendera

--all-tags

(Opsional) Menampilkan semua tanda instans pada wallpaper. Anda dapat menggunakan tanda ini atau `--allowed-tags`, tetapi tidak keduanya.

[--help | -h]

Menampilkan bantuan untuk perintah wallpaper.

EC2Luncurkan konfigurasi tugas v2

Bagian ini mencakup skema, tugas, detail, dan contoh konfigurasi untuk `agent-config.yml` dan data pengguna.

Tugas dan contoh

- Skema: agent-config.yml

- Konfigurasikan skrip data pengguna EC2 Luncurkan v2 yang berjalan selama peluncuran atau reboot

Skema: **agent-config.yml**

Struktur `agent-config.yml` file ditunjukkan di bawah ini. Perhatikan bahwa tugas tidak dapat diulang dalam tahap yang sama. Untuk properti tugas, lihat deskripsi tugas yang mengikuti.

Struktur dokumen: agent-config.yml

JSON

```
{
 "version": "1.1",
 "config": [
  {
   "stage": "string",
   "tasks": [
    {
     "task": "string",
     "inputs": {
      ...
     }
    },
    ...
   ]
  },
  ...
 ]
}
```

YAML

```
version: 1.1
config:
- stage: string
  tasks:
  - task: string
 inputs:
   ...
  ...
...
```

Contoh: **`agent-config.yml`**

Contoh berikut menunjukkan pengaturan untuk file konfigurasi `agent-config.yml`.

```
version: 1.1
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
- stage: postReady
  tasks:
  - task: startSsm
```

Konfigurasikan skrip data pengguna EC2 Luncurkan v2 yang berjalan selama peluncuran atau reboot

Contoh JSON dan YAMG berikut menunjukkan struktur dokumen untuk data pengguna. Amazon EC2 mengurai setiap tugas yang dinamai dalam array `tasks` yang Anda tentukan dalam dokumen. Setiap

tugas memiliki set properti dan persyaratan sendiri. Untuk detailnya, lihat Definisi tugas untuk tugas startup EC2 Launch v2.

> **Note**
>
> Tugas hanya boleh muncul sekali dalam array tugas data pengguna.

Struktur dokumen: data pengguna

JSON

```
{
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
   },
  },
  ...
 ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
...
```

Contoh: data pengguna

Untuk informasi selengkapnya tentang data pengguna, lihat Bagaimana Amazon EC2 menangani data pengguna untuk instans Windows.

Contoh dokumen YAMB berikut menunjukkan PowerShell skrip yang EC2 Launch v2 berjalan sebagai data pengguna untuk membuat file.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

Anda dapat menggunakan format XMLuntuk data pengguna yang kompatibel dengan versi agen peluncuran sebelumnya. EC2Launch v2 menjalankan skrip sebagai `executeScript` tugas di `UserData` panggung. Agar sesuai dengan perilaku EC2 Launch v1 dan EC2 Config, skrip data pengguna berjalan sebagai attached/inline proses secara default.

Anda dapat menambahkan tanda opsional untuk menyesuaikan cara skrip Anda berjalan. Misalnya, untuk menjalankan skrip data pengguna saat instans di-boot ulang selain satu kali saat instans diluncurkan, Anda dapat menggunakan tanda berikut:

`<persist>true</persist>`

Contoh:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Anda dapat menentukan satu atau lebih PowerShell argumen dengan `<powershellArguments>` tag. Jika tidak ada argumen yang diteruskan, EC2 Launch v2 menambahkan argumen berikut secara default:`-ExecutionPolicy Unrestricted`.

Contoh:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Untuk menjalankan skrip data pengguna XML sebagai proses yang terpisah, tambahkan tanda berikut ke data pengguna Anda.

```
<detach>true</detach>
```

Contoh:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

> **Note**
>
> Tanda lepas tidak didukung pada agen peluncuran sebelumnya.

Log perubahan: data pengguna

Tabel berikut mencantumkan perubahan untuk data pengguna, dan referensi silang ke versi agen EC2 Launch v2 yang berlaku.

Versi data pengguna	Detail	Diperkenalkan di
1.1	• Tugas data pengguna berjalan sebelum tahap `PostReady` dalam file konfigurasi agen. • Menjalankan data pengguna sebelum memulai Agen Systems Manager (perilaku yang sama seperti EC2 Launch v1 dan EC2 Config) . *	EC2Luncurkan v2 versi 2.0.1245
1.0	• Akan usang. • Tugas data pengguna berjalan sebelum tahap `PostReady` dalam file konfigurasi agen. Ini tidak kompatibel ke belakang dengan EC2 Launch v1.	EC2Luncurkan v2 versi 2.0.0

Versi data pengguna	Detail	Diperkenalkan di
	• Dipengaruhi oleh kondisi balapan antara start Systems Manager Agent dan tugas data pengguna.	

* Bila digunakan dengan file `agent-config.yml` default.

EC2Luncurkan kode keluar v2 dan reboot

Anda dapat menggunakan EC2 Launch v2 untuk menentukan bagaimana kode keluar ditangani oleh skrip Anda. Secara default, kode keluar dari perintah terakhir yang dijalankan dalam skrip dilaporkan sebagai kode keluar untuk seluruh skrip. Sebagai contoh, jika skrip mencakup tiga perintah dan perintah pertama gagal tetapi perintah yang berikutnya berhasil, maka status berjalan dilaporkan sebagai `success` karena perintah akhir berhasil.

Jika Anda ingin skrip untuk me-reboot sebuah instance, maka Anda harus menentukan `exit 3010` dalam skrip Anda, bahkan ketika reboot adalah langkah terakhir dalam skrip Anda. `exit 3010`menginstruksikan EC2 Launch v2 untuk me-reboot instance dan memanggil skrip lagi sampai mengembalikan kode keluar yang tidak`3010`, atau sampai jumlah reboot maksimum tercapai. EC2Luncurkan v2 memungkinkan maksimal 5 reboot per tugas. Jika Anda mencoba untuk me-reboot instans dari skrip dengan menggunakan mekanisme yang berbeda, seperti, `Restart-Computer`maka status berjalan skrip akan menjadi tidak konsisten. Sebagai contoh, skrip mungkin terjebak dalam loop mulai ulang atau tidak melakukan restart.

Jika Anda menggunakan format data pengguna XMLyang kompatibel dengan agen sebelumnya, maka data pengguna dapat berjalan lebih banyak daripada yang Anda inginkan. Untuk informasi selengkapnya, lihat Layanan menjalankan data pengguna lebih dari satu kali di bagian Pemecahan Masalah.

EC2Luncurkan v2 dan Sysprep

Layanan EC2 Launch v2 menjalankan Sysprep, alat Microsoft yang memungkinkan Anda membuat AMI Windows yang disesuaikan yang dapat digunakan kembali. Ketika EC2 Launch v2 memanggil Sysprep, ia menggunakan file `%ProgramData%\Amazon\EC2Launch` untuk menentukan operasi mana yang harus dilakukan. Anda dapat mengedit file-file ini secara tidak langsung menggunakan kotak dialog EC2Launch settings, atau langsung menggunakan editor YAMM atau editor teks.

Namun, ada beberapa pengaturan lanjutan yang tidak tersedia di kotak dialog Pengaturan EC2 peluncuran, jadi Anda harus mengedit entri tersebut secara langsung.

Jika Anda membuat AMI dari sebuah instans setelah memperbarui pengaturannya, pengaturan baru tersebut diterapkan ke setiap instans yang diluncurkan dari AMI baru. Untuk informasi tentang membuat grafik, lihat Buat AMI yang didukung Amazon EBS-Backed.

Definisi tugas untuk tugas startup EC2 Launch v2

Setiap tugas yang dijalankan EC2 Launch v2 selama peluncuran atau startup memiliki seperangkat properti dan persyaratannya sendiri. Detail tugas mencakup pengaturan untuk seberapa sering tugas berjalan — sekali, atau selalu, tahap proses boot agen apa yang dijalankannya, sintaks, dan contoh dokumen YAMAL. Untuk informasi selengkapnya, tinjau detail tugas yang ditunjukkan dalam referensi ini.

EC2Luncurkan Tugas v2

- activateWindows
- enableJumboFrames
- enableOpenSsh
- executeProgram
- executeScript
- extendRootPartition
- initializeVolume
- optimizeEna
- setAdminAccount
- setDnsSuffix
- setHostName
- setWallpaper
- startSsm
- sysprep
- writeFile

activateWindows

Mengaktifkan Windows terhadap satu set AWS KMS server. Aktivasi dilewati jika instance terdeteksi sebagai Bring-Your-Own-License (BYOL).

Frekuensi - sekali

AllowedStages — `[PreReady]`

Masukan —

`activation`: (peta)

`type`: (string) tipe aktivasi yang akan digunakan, diatur ke `amazon`

Contoh

```
task: activateWindows
  inputs:
    activation:
    type: amazon
```

enableJumboFrames

Mengaktifkan Jumbo Frames, yang meningkatkan unit transmisi maksimum (MTU) dari adaptor jaringan. Untuk informasi selengkapnya, lihat Frame jumbo (9001 MTU).

Frekuensi - selalu

AllowedStages — `[PostReady, UserData]`

Masukan - tidak ada

Contoh

```
task: enableJumboFrames
```

enableOpenSsh

Mengaktifkan Windows OpenSSH dan menambahkan kunci publik untuk instans tersebut ke folder kunci resmi.

Frekuensi — sekali

AllowedStages — `[PreReady, UserData]`

Masukan - tidak ada

Contoh

Contoh berikut menunjukkan cara mengaktifkan OpenSSH pada sebuah instans, dan untuk menambahkan kunci publik untuk instans tersebut ke folder kunci resmi. Konfigurasi ini hanya berfungsi pada instans yang menjalankan Windows Server 2019 dan versi setelahnya.

```
task: enableOpenSsh
```

executeProgram

Menjalankan program dengan argumen opsional dan frekuensi tertentu.

Tahapan: Anda dapat menjalankan tugas `executeProgram` selama tahapan `PreReady`, `PostReady`, dan `UserData`

Frekuensi: dapat dikonfigurasi, lihat Input.

Masukan

Bagian ini berisi satu atau lebih program untuk menjalankan executeProgram tugas (input). Setiap input dapat mencakup pengaturan yang dapat dikonfigurasi berikut:

frekuensi (string)

(Wajib) Tentukan dengan tepat satu dari nilai-nilai berikut:

- `once`
- `always`

jalur (string)

(Wajib) Jalur file untuk menjalankan executable.

argumen (daftar string)

(Opsional) Daftar argumen yang dipisahkan koma untuk diberikan kepada program sebagai input.

runAs (string)

(Wajib) Harus diatur ke `localSystem`

Output

Semua tugas menulis entri logfile ke file `agent.log`. Output tambahan dari tugas `executeProgram` disimpan secara terpisah dalam folder bernama dinamis, sebagai berikut:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.tmp`*

Jalur yang tepat ke file output disertakan dalam `agent.log` file, misalnya:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

File keluaran untuk **`executeProgram`** tugas tersebut

`ExecuteProgramInputs.tmp`

Berisi jalur untuk executable, dan semua parameter input yang diteruskan tugas `executeProgram` padanya saat dijalankan.

`Output.tmp`

Berisi output runtime dari program yang dijalankan tugas `executeProgram`.

`Err.tmp`

Berisi pesan kesalahan runtime dari program yang dijalankan tugas `executeProgram`.

Contoh

Contoh berikut menunjukkan cara menjalankan file yang dapat dieksekusi dari direktori lokal pada instans dengan tugas `executeProgram`.

Contoh 1: File setup yang dapat dieksekusi dengan satu argumen

Contoh ini menunjukkan tugas `executeProgram` yang menjalankan setup yang dapat dieksekusi dalam mode senyap.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\Users\Administrator\Desktop\setup.exe
      arguments: ['-quiet']
```

Contoh 2: VLC dapat dieksekusi dengan dua argumen

Contoh ini menunjukkan tugas `executeProgram` yang menjalankan file VLC yang dapat dieksekusi dengan dua argumen yang diteruskan sebagai parameter input.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\vlc-3.0.11-win64.exe
      arguments: ['/L=1033','/S']
      runAs: localSystem
```

executeScript

Menjalankan skrip dengan argumen opsional dan frekuensi tertentu. Perilaku skrip tergantung pada mode apa agen menjalankan skrip — inline, atau terpisah.

Inline (default)

Agen EC2 Launch v2 menjalankan skrip satu per satu (`detach: false`). Ini adalah pengaturan default.

> **Note**
>
> Ketika skrip inline Anda mengeluarkan perintah reset atau sysprep, skrip tersebut segera berjalan dan mengatur ulang agen. Tugas saat ini selesai, kemudian agen dimatikan tanpa menjalankan tugas lebih lanjut.
> Misalnya, jika tugas yang mengeluarkan perintah akan diikuti oleh `startSsm` tugas (disertakan secara default setelah data pengguna berjalan), tugas tidak berjalan dan layanan Systems Manager tidak pernah dimulai.

Terlepas

Agen EC2 Launch v2 menjalankan skrip secara bersamaan dengan tugas lain ()`detach: true`.

> **Note**
>
> Saat skrip terpisah Anda mengeluarkan reset atau sysprep, perintah tersebut menunggu agen selesai sebelum dijalankan. Tugas setelah executeScript masih akan berjalan.

Tahapan: Anda dapat menjalankan tugas `executeScript` selama tahapan `PreReady`, `PostReady`, dan `UserData`

Frekuensi: dapat dikonfigurasi, lihat Input.

Masukan

Bagian ini berisi satu atau lebih skrip untuk executeScript tugas yang akan dijalankan (input). Setiap input dapat mencakup pengaturan yang dapat dikonfigurasi berikut:

frekuensi (string)

(Wajib) Tentukan dengan tepat satu dari nilai-nilai berikut:

- `once`
- `always`

tipe (string)

(Wajib) Tentukan dengan tepat satu dari nilai-nilai berikut:

- `batch`
- `powershell`

argumen (daftar string)

(Opsional) Daftar argumen string untuk diteruskan ke shell (bukan ke PowerShell skrip). Parameter ini tidak didukung untuk `type: batch`. Jika tidak ada argumen yang diteruskan, EC2 Launch v2 menambahkan argumen berikut secara default:`-ExecutionPolicy Unrestricted`.

konten (string)

(Wajib) Konten skrip.

runAs (string)

(Wajib) Tentukan dengan tepat satu dari nilai-nilai berikut:

- `admin`
- `localSystem`

lepas (Boolean)

(Opsional) Agen EC2 Launch v2 default untuk menjalankan skrip satu per satu (). `detach: false` Untuk menjalankan skrip secara bersamaan dengan tugas lain, atur nilainya ke `true` (`detach: true`).

> **Note**
>
> Kode keluar skrip (termasuk `3010`) tidak berpengaruh jika `detach` diatur ke `true`.

Output

Semua tugas menulis entri logfile ke file `agent.log`. Output tambahan dari skrip yang dijalankan tugas `executeScript` disimpan secara terpisah dalam folder bernama dinamis, sebagai berikut:

`%LocalAppData%\Temp\`*`EC2Launch#########`*`\`*`outputfilename.ext`*

Jalur yang tepat ke file output disertakan dalam `agent.log` file, misalnya:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

File keluaran untuk **`executeScript`** tugas tersebut

`UserScript.`*`ext`*

Berisi skrip yang dijalankan tugas `executeScript`. Ekstensi file tergantung pada jenis skrip yang Anda tentukan dalam `type` parameter untuk `executeScript` tugas, sebagai berikut:

- Jika tipenya adalah `batch`, maka ekstensi file adalah `.bat`.
- Jika tipenya adalah `powershell`, maka ekstensi file adalah `.ps1`.

`Output.tmp`

Berisi output runtime dari skrip yang dijalankan tugas `executeScript`.

`Err.tmp`

Berisi pesan kesalahan runtime dari skrip yang dijalankan tugas `executeScript`.

Contoh

Contoh berikut menunjukkan cara menjalankan skrip inline dengan tugas `executeScript`.

Contoh 1: File teks output Hello world

Contoh ini menunjukkan `executeScript` tugas yang menjalankan PowerShell skrip untuk membuat file teks “Hello world” di `C:` drive.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: admin
      content: |-
        New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
        Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Contoh 2: Jalankan dua skrip

Contoh ini menunjukkan bahwa tugas `executeScript` dapat menjalankan lebih dari satu skrip, dan tipe skrip tidak harus cocok.

Script pertama (`type: powershell`) menulis ringkasan proses yang saat ini berjalan pada instans ke file teks yang terletak di `C:` drive.

Script kedua (`batch`) menulis informasi sistem ke `Output.tmp` file.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: localSystem
      content: |
```

```
        Get-Process | Out-File -FilePath C:\Process.txt
    - frequency: always
      type: batch
      runAs: localSystem
      content: |
        systeminfo
```

Contoh 3: Konfigurasi sistem idempotensi dengan boot ulang

Contoh ini menunjukkan tugas `executeScript` yang menjalankan skrip idempotensi untuk melakukan konfigurasi sistem berikut dengan boot ulang di antara setiap langkah:

- Ganti nama komputer.
- Bergabunglah dengan komputer ke domain.
- Aktifkan Telnet.

Skrip memastikan bahwa setiap operasi berjalan satu kali saja. Ini mencegah loop reboot dan membuat skrip idempoten.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: localSystem
      content: |-
        $name = $env:ComputerName
        if ($name -ne $desiredName) {
          Rename-Computer -NewName $desiredName
          exit 3010
        }
        $domain = Get-ADDomain
        if ($domain -ne $desiredDomain)
        {
          Add-Computer -DomainName $desiredDomain
          exit 3010
        }
        $telnet = Get-WindowsFeature -Name Telnet-Client
        if (-not $telnet.Installed)
        {
          Install-WindowsFeature -Name "Telnet-Client"
          exit 3010
        }
```

extendRootPartition

Memperluas volume root untuk menggunakan semua ruang yang tersedia di disk.

Frekuensi - sekali

AllowedStages — `[Boot]`

Masukan - tidak ada

Contoh

```
task: extendRootPartition
```

initializeVolume

Menginisialisasi volume kosong yang dilampirkan ke instans sehingga mereka diaktifkan dan dipartisi. Agen peluncuran melewatkan inisialisasi jika mendeteksi bahwa volume tidak kosong. Volume dianggap kosong jika 4 KiB pertama dari volume adalah kosong, atau jika volume tidak memiliki tata letak hard disk yang dapat dikenali Windows.

Parameter `letter` input selalu diterapkan saat tugas ini berjalan, terlepas dari apakah drive sudah diinisialisasi.

Tugas `initializeVolume` melakukan tindakan berikut.

- Atur atribut disk `offline` dan `readonly` ke false.
- Buat sebuah partisi. Jika tidak ada jenis partisi yang ditentukan dalam parameter `partition` input, default berikut berlaku:
  - Jika ukuran disk lebih kecil dari 2 TB, atur tipe partisi ke `mbr`.
  - Jika ukuran disk 2 TB atau lebih besar, atur tipe partisi ke `gpt`.
- Format volume sebagai NTFS.
- Atur label volume sebagai berikut:
  - Gunakan nilai parameter input `name`, jika ditentukan.
  - Jika volumenya fana, dan tidak ada nama yang ditentukan, atur label volume ke. `Temporary Storage Z`
- Jika volumenya singkat (SSD atau HDD - bukan Amazon EBS), buat `Important.txt` file di root volume dengan konten berikut:

```
This is an 'Instance Store' disk and is provided at no additional charge.

*This disk offers increased performance since it is local to the host
*The number of Instance Store disks available to an instance vary by instance type
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
 PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY

For more information, please refer to: Instans menyimpan penyimpanan blok sementara
 untuk instans EC2.
```

- Atur huruf drive ke nilai yang ditentukan dalam parameter `letter` input.

Tahapan: Anda dapat menjalankan `initializeVolume` tugas selama `PostReady` dan `UserData` tahapan.

Frekuensi: selalu.

Masukan

Anda dapat mengonfigurasi parameter runtime sebagai berikut:

perangkat (daftar peta)

(Bersyarat) Konfigurasi untuk setiap perangkat yang dimulai agen peluncuran. Ini diperlukan jika parameter input `initialize` diatur ke `devices`.

- perangkat (string, wajib) - Mengidentifikasi perangkat selama pembuatan instans. Sebagai contoh, `xvdb`, `xvdf`, atau `\dev\nvme0n1`.
- huruf (string, opsional) - Satu karakter. Surat drive untuk ditetapkan.
- nama (string, opsional) - Nama volume yang akan ditetapkan.
- partisi (string, opsional) – Tentukan salah satu nilai berikut untuk tipe partisi yang akan dibuat, atau biarkan agen peluncuran menentukan default berdasarkan ukuran volume:
  - mbr
  - gpt

inisialisasi (string)

(Wajib) Tentukan dengan tepat satu dari nilai-nilai berikut:

- `all`
- `devices`

Contoh

Contoh berikut menampilkan konfigurasi input sampel untuk tugas `initializeVolume` tersebut.

Contoh 1: Inisialisasi dua volume pada sebuah instans

Contoh ini menunjukkan tugas `initializeVolume` yang menginisialisasi dua volume sekunder pada sebuah instans. Perangkat yang bernama `DataVolume2` dalam contoh tersebut bersifat sementara.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Contoh 2: Inisialisasi volume EBS yang dilampirkan ke sebuah instans

Contoh ini menunjukkan tugas `initializeVolume` yang menginisialisasi semua volume EBS kosong yang dilampirkan ke instans.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Mengoptimalkan pengaturan ENA berdasarkan tipe instans saat ini; mungkin mem-boot ulang instans.

Frekuensi - selalu

AllowedStages — `[PostReady, UserData]`

Masukan - tidak ada

Contoh

```
task: optimizeEna
```

setAdminAccount

Set atribut untuk akun administrator default yang dibuat di mesin lokal.

Frekuensi - sekali

AllowedStages — `[PreReady]`

Masukan —

`name`: (string) nama akun administrator

`password`: (peta)

`type`: (string) strategi untuk mengatur kata sandi, baik sebagai `static`, `random`, atau `doNothing`

`data`: (string) menyimpan data jika bidang `type` statis

Contoh

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
  type: random
```

setDnsSuffix

Menambahkan sufiks DNS ke daftar sufiks pencarian. Hanya sufiks yang belum ada yang ditambahkan ke daftar. Untuk informasi selengkapnya tentang cara agen peluncuran menyetel sufiks DNS, lihat. Konfigurasikan DNS Suffix untuk agen peluncuran EC2 Windows

Frekuensi - selalu

AllowedStages — `[PreReady]`

Masukan —

`suffixes`: (daftar string) daftar satu atau lebih sufiks DNS yang valid; variabel substitusi yang valid adalah `$REGION` dan `$AZ`

Contoh

```
task: setDnsSuffix
inputs:
  suffixes:
  - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Menetapkan nama host komputer ke string kustom atau, jika tidak `hostName` ditentukan, IPv4 alamat pribadi.

Frekuensi - selalu

AllowedStages — `[PostReady, UserData]`

Masukan —

`hostName`: (string) nama host opsional, yang harus diformat sebagai berikut.

- Harus 15 karakter atau kurang
- Harus hanya berisi karakter alfanumerik (a-z, A-Z, 0-9) dan tanda hubung (-).
- Tidak boleh seluruhnya terdiri dari karakter numerik.

`reboot`: (boolean) menunjukkan apakah booti ulang diizinkan saat nama host diubah

Contoh

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Membuat file pintasan `setwallpaper.lnk` di folder startup setiap pengguna yang ada kecuali untuk `Default User`. File pintasan ini berjalan saat pengguna masuk untuk pertama kalinya setelah boot instans. File ini menyiapkan instans dengan wallpaper kustom yang menampilkan atribut instans.

Jalur file pintasan adalah:

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> Saat Anda menghapus tugas `setWallpaper`, file pintasan ini tidak akan terhapus. Untuk informasi selengkapnya, lihat Tugas `setWallpaper` tidak diaktifkan tetapi wallpaper diatur ulang saat reboot.

Tahapan: Anda dapat mengonfigurasi wallpaper selama tahapan `PreReady` dan `UserData`.

Frekuensi: `always`

Konfigurasi wallpaper

Anda dapat menggunakan pengaturan berikut untuk mengonfigurasi wallpaper Anda.

Masukan

Parameter masukan yang Anda berikan, dan atribut yang dapat Anda atur untuk mengonfigurasi wallpaper Anda:

jalur (string)

(Wajib) Jalur nama file dari file gambar format .jpg lokal yang akan digunakan untuk gambar wallpaper Anda.

atribut (daftar string)

(Opsional) Anda dapat menambahkan satu atau lebih atribut berikut ke wallpaper Anda:

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `privateIpAddress`
- `publicIpAddress`

- `ipv6Address`

instanceTags

(Opsional) Anda dapat menggunakan salah satu opsi berikut untuk pengaturan ini.

- AllTags(string) — Tambahkan semua tag instance ke wallpaper Anda.

```
instanceTags: AllTags
```

- instanceTags (daftar string) - Tentukan daftar nama tanda instans untuk ditambahkan ke wallpaper Anda. Contoh:

```
instanceTags:
  - Tag 1
  - Tag 2
```

Contoh

Contoh berikut menunjukkan input konfigurasi wallpaper yang mengatur jalur file untuk gambar latar belakang wallpaper, bersama dengan tanda instans bernama `Tag 1` dan `Tag 2`, serta atribut yang menyertakan nama host, ID instans, dan alamat IP privat serta publik untuk instans tersebut.

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
  - privateIpAddress
  - publicIpAddress
  instanceTags:
  - Tag 1
  - Tag 2
```

> **Note**
>
> Anda harus mengaktifkan tanda dalam metadata untuk menampilkan tanda pada wallpaper. Untuk informasi selengkapnya tentang tanda instans dan metadata, lihat Lihat tag untuk instans EC2 Anda menggunakan metadata instans.

startSsm

Memulai layanan Systems Manager (SSM) setelah Sysprep.

Frekuensi - selalu

AllowedStages — `[PostReady, UserData]`

Masukan - tidak ada

Contoh

```
task: startSsm
```

sysprep

Mereset status layanan, update `unattend.xml`, menonaktifkan RDP, dan menjalankan Sysprep. Tugas ini berjalan hanya setelah semua tugas lainnya selesai.

Frekuensi - sekali

AllowedStages — `[UserData]`

Masukan —

`clean`: (boolean) membersihkan log instans sebelum menjalankan Sysprep

`shutdown`: (boolean) menutup instans setelah menjalankan Sysprep

Contoh

```
task: sysprep
inputs:
clean: true
shutdown: true
```

writeFile

Menuliskan file ke tujuan.

Frekuensi - lihat Input

AllowedStages — `[PostReady, UserData]`

Masukan —

`frequency`: (string) salah satu `once` atau `always`

`destination`: (string) jalur tempat menulis konten

`content`: (string) teks untuk ditulis ke tujuan

Contoh

```
task: writeFile
inputs:
  - frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Memecahkan masalah dengan agen EC2 Launch v2

Bagian ini menunjukkan skenario pemecahan masalah umum untuk EC2 Launch v2, informasi tentang melihat log peristiwa Windows, dan keluaran log konsol dan pesan.

Topik pemecahan masalah

- Skenario pemecahan masalah umum
- Log peristiwa Windows
- EC2Luncurkan keluaran log konsol v2

Skenario pemecahan masalah umum

Bagian ini menunjukkan skenario pemecahan masalah umum dan langkah-langkah penyelesaiannya.

Skenario

- Layanan gagal menyetel wallpaper
- Layanan gagal menjalankan data pengguna
- Layanan menjalankan tugas hanya satu kali
- Layanan gagal menjalankan tugas

- Layanan menjalankan data pengguna lebih dari satu kali
- Tugas terjadwal dari EC2 Launch v1 gagal dijalankan setelah migrasi ke EC2 Launch v2
- Layanan menginisialisasi volume EBS yang tidak kosong
- Tugas setWallpaper tidak diaktifkan tetapi wallpaper diatur ulang saat reboot
- Layanan macet dalam status berjalan
- Tidak valid agent-config.yml mencegah membuka kotak dialog pengaturan EC2 Launch v2
- task:executeScript should be unique and only invoked once

Layanan gagal menyetel wallpaper

Resolusi

1. Periksa apakah `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs \Startup\setwallpaper.lnk` ada.
2. Periksa `%ProgramData%\Amazon\EC2Launch\log\agent.log` untuk melihat apakah ada kesalahan yang terjadi.

Layanan gagal menjalankan data pengguna

Penyebab potensial: Layanan mungkin gagal sebelum menjalankan data pengguna.

Resolusi

1. Periksa `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.
2. Lihat jika `boot`, `network`, `preReady`, dan `postReadyLocalData` semuanya telah ditandai sebagai sukses.
3. Jika salah satu tahapan gagal, periksa `%ProgramData%\Amazon\EC2Launch\log \agent.log` jika ada kesalahan tertentu.

Layanan menjalankan tugas hanya satu kali

Resolusi

1. Periksa frekuensi tugas.
2. Jika layanan sudah berjalan setelah Sysprep, dan frekuensi tugas diatur ke `once`, tugas tidak akan dijalankan lagi.

3. Atur frekuensi tugas ke `always` jika Anda ingin menjalankan tugas setiap kali EC2 Launch v2 berjalan.

Layanan gagal menjalankan tugas

Resolusi

1. Periksa entri terbaru di `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Jika tidak ada kesalahan yang terjadi, coba jalankan layanan secara manual dari `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` untuk melihat apakah tugas berhasil.

Layanan menjalankan data pengguna lebih dari satu kali

Resolusi

Data pengguna ditangani secara berbeda antara EC2 Launch v1 dan EC2 Launch v2. EC2Launch v1 menjalankan data pengguna sebagai tugas terjadwal pada instance saat `persist` disetel ke`true`. Jika `persist` diatur ke, `false`maka tugas tidak dijadwalkan bahkan saat keluar dengan reboot atau terganggu saat berjalan.

EC2Launch v2 menjalankan data pengguna sebagai tugas agen dan melacak status jalanannya. Jika masalah data pengguna me-restart komputer atau jika data pengguna terganggu saat berjalan, maka status berjalan-nya masih tetap ada sebagai `pending` dan data pengguna akan berjalan lagi pada boot instans berikutnya. Jika Anda ingin mencegah skrip data pengguna berjalan lebih dari sekali, buat skrip menjadi idempoten.

Contoh skrip idempotensi berikut mengatur nama komputer dan bergabung dengan domain.

```
<powershell>
  $name = $env:computername
  if ($name -ne $desiredName) {
 Rename-Computer -NewName $desiredName
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
```

```
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
</powershell>
<persist>false</persist>
```

Tugas terjadwal dari EC2 Launch v1 gagal dijalankan setelah migrasi ke EC2 Launch v2

Resolusi

Alat migrasi tidak mendeteksi tugas terjadwal yang ditautkan ke skrip EC2 Launch v1; oleh karena itu, alat ini tidak secara otomatis mengatur tugas-tugas tersebut di EC2 Launch v2. Untuk mengonfigurasi tugas-tugas ini, edit `agent-config.yml`file, atau gunakan kotak dialog EC2 Launch v2 settings. Misalnya, jika sebuah instance memiliki tugas terjadwal yang berjalan`InitializeDisks.ps1`, maka setelah Anda menjalankan alat migrasi, Anda harus menentukan volume yang ingin Anda inisialisasi di kotak dialog EC2 Launch v2 settings. Lihat Langkah 6 prosedur untuk Ubah pengaturan menggunakan kotak dialog EC2 Launch v2 settings.

Layanan menginisialisasi volume EBS yang tidak kosong

Resolusi

Sebelum menginisialisasi volume, EC2 Launch v2 mencoba mendeteksi apakah itu kosong. Jika volume tidak kosong, maka ia melewatkan inisialisasi. Setiap volume yang terdeteksi sebagai tidak kosong tidak akan diinisialisasi. Volume dianggap kosong jika 4 KiB pertama dari volume adalah kosong, atau jika volume tidak memiliki tata letak hard disk yang dapat dikenali Windows. Volume yang diinisialisasi dan diformat pada sistem Linux tidak memiliki tata letak hard disk yang dikenali Windows, misalnya MBR atau GPT. Oleh karena itu, volume tersebut akan dianggap sebagai volume kosong dan diinisialisasi. Jika Anda ingin menyimpan data ini, jangan mengandalkan deteksi drive kosong EC2 Luncurkan v2. Sebagai gantinya, tentukan volume yang ingin Anda inisialisasi di kotak dialog EC2 Launch v2 settings (lihat langkah 6) atau di `agent-config.yml`.

Tugas **`setWallpaper`** tidak diaktifkan tetapi wallpaper diatur ulang saat reboot

`setWallpaper`Tugas membuat file `setwallpaper.lnk` pintasan di folder startup setiap pengguna yang ada. File pintasan ini berjalan saat pengguna masuk untuk pertama kalinya setelah boot instans. File ini menyiapkan instans dengan wallpaper kustom yang menampilkan atribut instans. Menghapus `setWallpaper` tugas tidak menghapus file pintasan ini. Anda harus menghapus file ini secara manual atau menghapusnya menggunakan skrip.

Jalur pintasnya adalah:

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Resolusi

Hapus file ini secara manual, atau hapus menggunakan skrip.

Contoh PowerShell skrip untuk menghapus file pintasan

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Layanan macet dalam status berjalan

Deskripsi

EC2Luncurkan v2 diblokir, dengan pesan log (`agent.log`) mirip dengan berikut ini:

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Kemungkinan penyebab

SAC diaktifkan dan menggunakan port serial. Untuk informasi selengkapnya, lihat Gunakan SAC untuk memecahkan masalah instans Windows Anda.

Resolusi

Coba langkah-langkah berikut untuk mengatasi masalah ini:

- Nonaktifkan layanan yang menggunakan port serial.
- Jika Anda ingin layanan terus menggunakan port serial, tulis skrip khusus untuk melakukan tugas agen peluncuran dan menginvokasinya sebagai tugas terjadwal.

Tidak valid **`agent-config.yml`** mencegah membuka kotak dialog pengaturan EC2 Launch v2

Deskripsi

EC2Luncurkan pengaturan v2 mencoba mengurai `agent-config.yml` file sebelum membuka kotak dialog. Jika file konfigurasi YAMB tidak mengikuti skema yang didukung, kotak dialog akan menampilkan kesalahan berikut:

```
Unable to parse configuration file agent-config.yml. Review configuration file. Exiting application.
```

Resolusi

1. Verifikasi bahwa file konfigurasi mengikuti skema yang didukung.
2. Jika Anda ingin memulai dari awal, salin file konfigurasi default ke `agent-config.yml`. Anda dapat menggunakan contoh `agent-config.yml` yang disediakan di bagian Konfigurasi Tugas.
3. Anda juga dapat memulai dari awal dengan menghapus `agent-config.yml`. EC2Luncurkan pengaturan v2 menghasilkan file konfigurasi kosong.

`task:executeScript should be unique and only invoked once`

Deskripsi

Tugas tidak dapat diulang dalam tahap yang sama.

Resolusi

Beberapa tugas harus dimasukkan sebagai array, seperti executeScript dan executeProgram. Untuk contoh cara menulis skrip sebagai array, lihat executeScript.

Log peristiwa Windows

EC2Launch v2 menerbitkan log peristiwa Windows untuk acara penting, seperti memulai layanan, Windows siap, dan keberhasilan dan kegagalan tugas. Pengidentifikasi peristiwa secara unik mengidentifikasi peristiwa tertentu. Setiap acara berisi informasi tahapan, tugas, dan level, serta deskripsi. Anda dapat mengatur pemicu untuk peristiwa tertentu menggunakan pengenal peristiwa.

Acara IDs memberikan informasi tentang suatu peristiwa dan secara unik mengidentifikasi beberapa peristiwa. Digit paling signifikan dari ID peristiwa menunjukkan tingkat keparahan suatu peristiwa.

Peristiwa	Digit paling tidak signifikan
`Success`	`. . .0`
`Informational`	`. . .1`
`Warning`	`. . .2`
`Error`	`. . .3`

Peristiwa terkait layanan yang dihasilkan ketika layanan dimulai atau berhenti termasuk satu digit pengenal peristiwa.

Peristiwa	Pengenal digit tunggal
`Success`	`0`
`Informational`	`1`
`Warning`	`2`
`Error`	`3`

Pesan peristiwa untuk peristiwa `EC2LaunchService.exe` dimulai dengan `Service:`. Pesan peristiwa untuk peristiwa `EC2Launch.exe` tidak dimulai dengan `Service:`.

Acara empat digit IDs mencakup informasi tentang tahap, tugas, dan tingkat keparahan suatu peristiwa.

Topik

- Format ID Peristiwa
- Contoh ID Peristiwa
- Skema log peristiwa Windows

Format ID Peristiwa

Tabel berikut menunjukkan format pengenal peristiwa EC2 Launch v2.

3	2 1	0
D	T	L

Huruf dan angka dalam tabel mewakili tipe dan definisi peristiwa berikut.

Tipe peristiwa	Definisi
S (Panggung)	0 - Pesan tingkat layanan 1 - Boot 2 - Jaringan 3 - PreReady 5 - Windows sudah Siap 6 - PostReady 7 - Data Pengguna
T (Tugas)	Tugas yang diwakili oleh dua nilai yang sesuai berbeda untuk setiap tahap. Untuk melihat daftar lengkap peristiwa, lihat Skema log Peristiwa Windows.

Tipe peristiwa	Definisi
L (Level peristiwa)	0 - Sukses 1 - Informasi 2 - Peringatan 3 - Kesalahan

Contoh ID Peristiwa

Berikut ini adalah contoh peristiwa IDs.

- `5000` - Windows siap digunakan
- `3010`- Aktifkan tugas windows di PreReady panggung berhasil
- `6013`- Mengatur tugas wallpaper di tahap Data PostReady Lokal mengalami kesalahan

Skema log peristiwa Windows

MessageId/ Id Acara	Pesan peristiwa
`. . .0`	`Success`
`. . .1`	`Informational`
`. . .2`	`Warning`
`. . .3`	`Error`
`x`	`EC2Launch service-level logs`
`0`	`EC2Launch service exited successfully`
`1`	`EC2Launch service informational logs`

MessageId/ Id Acara	Pesan peristiwa
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix

MessageId/ Id Acara	Pesan peristiwa
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file

MessageId/ Id Acara	Pesan peristiwa
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

EC2Luncurkan keluaran log konsol v2

Bagian ini berisi contoh keluaran log konsol untuk EC2 Launch v2 dan mencantumkan semua pesan kesalahan log konsol EC2 Luncurkan v2 untuk membantu Anda memecahkan masalah. Untuk informasi selengkapnya tentang keluaran konsol instance dan cara mengaksesnya, lihatthe section called “Output konsol instans”.

Output

- EC2Luncurkan keluaran log konsol v2
- EC2Luncurkan pesan log konsol v2

EC2Luncurkan keluaran log konsol v2

Berikut ini adalah contoh keluaran log konsol untuk EC2 Launch v2. Beberapa nilai dalam contoh ini diganti dengan teks representatif yang dikelilingi oleh kurawal kurawal.

```
2025/07/22 21:26:53Z: Windows sysprep configuration complete.
2025/07/22 21:26:53Z: Message: Waiting for access to metadata...
2025/07/22 21:26:53Z: Message: Meta-data is now available.
2025/07/22 21:26:53Z: AMI Origin Version: 2024.12.13
2025/07/22 21:26:53Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2025/07/22 21:26:53Z: OS: Microsoft Windows NT 10.0.20348
2025/07/22 21:26:53Z: OsVersion: 10.0
2025/07/22 21:26:53Z: OsProductName: Windows Server 2022 Datacenter
2025/07/22 21:26:53Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2025/07/22 21:26:53Z: OsCurrentBuild: 20348
2025/07/22 21:26:53Z: OsReleaseId: 2009
2025/07/22 21:26:53Z: Language: en-US
```

```
2025/07/22 21:26:53Z: TimeZone: UTC
2025/07/22 21:26:53Z: Offset: UTC +0000
2025/07/22 21:26:53Z: Launch: EC2 Launch v2.2.63
2025/07/22 21:26:53Z: AMI-ID: ami-1234567890abcdef1
2025/07/22 21:26:53Z: Instance-ID: i-1234567890abcdef0
2025/07/22 21:26:54Z: Instance Type: t3.xlarge
2025/07/22 21:26:54Z: Driver: AWS NVMe Driver v1.6.0.35
2025/07/22 21:26:54Z: SubComponent: 1.6.0.35; EnableSCSIPersistentReservations: 0
2025/07/22 21:26:54Z: Driver: AWS PV Driver Package v8.5.0
2025/07/22 21:26:55Z: Driver: Amazon Elastic Network Adapter v2.8.0.0
2025/07/22 21:26:55Z: HOSTNAME: EC2AMAZ-9FJG5CC
2025/07/22 21:26:55Z: RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
2025/07/22 21:26:55Z: RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
2025/07/22 21:26:56Z: SSM: Amazon SSM Agent v3.3.2746.0
2025/07/22 21:26:57Z: User data format: no_user_data
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentCommandErrorCode=1
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AdminPasswordTypeCode=0
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentErrorLocation=execute_windows.go:410
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IpConflictDetectionCode=0
2025/07/22 21:26:57Z: Message: Windows is Ready to use
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2", ...}
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2", ...}
```

EC2Luncurkan pesan log konsol v2

Berikut ini adalah daftar semua pesan log konsol EC2 Launch v2.

```
Error EC2Launch service is stopping. {error message}
```

Detail kesalahan layanan yang dihentikan:

- `Error setting up EC2Launch agent folders`
- `See instance logs for detail`
- `Error stopping service`
- `Error initializing service`

```
Windows sysprep configuration complete
```

```
Invalid administrator username: {invalid username}
```

```
Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
```

Pesan berikut adalah blok informasi yang berisi detail AMI:

```
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
HOSTNAME: {computer name}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
SSM: Amazon SSM Agent {version}
AWS VSS Version: {version}
```

```
Windows sysprep configuration complete.
Windows is being configured. 'SysprepState is {state}'
Windows is still being configured. 'SysprepState is {state}'
Windows is Ready to use
Waiting for access to metadata...
Meta-data is now available.
Metadata is not available for this instance.
```

```
Timed out waiting for access to metadata.
User data format: {format}
```

Pesan telemetri EC2launch v2 menyertakan nilai properti telemetri peluncuran. Dimulai dengan versi 2.2.63, data telemetri agen EC2 diformat sebagai objek JSON.

```
EC2LaunchTelemetry: {telemetry property}
```

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2" ... }
```

EC2Luncurkan riwayat versi v2

Riwayat versi

- EC2Luncurkan riwayat versi v2

EC2Luncurkan riwayat versi v2

Untuk memastikan bahwa Anda telah menginstal agen peluncuran terbaru, lihatInstal versi terbaru EC2 Launch v2. Anda dapat menerima pemberitahuan saat versi baru agen EC2 Launch v2 dirilis. Untuk informasi selengkapnya, lihat Berlangganan pemberitahuan agen peluncuran EC2 Windows.

Tabel berikut menjelaskan versi rilis EC2 Launch v2.

Versi	Detail	Tanggal rilis
2.4.0	• Pencatatan agen yang disederhanakan dengan menghapus file yang berlebihan`console.log` `.err.log` • Meningkatkan kemampuan pencatatan agen dengan menambahkan rotasi log, membatasi ukuran log hingga 1 MB dan meningkatkan presisi waktu hingga milidetik. • Mengurangi waktu ke Windows Siap dengan menghapus kueri status Hyper-V.	Maret 5, 2026
2.3.237	•	Februari 25, 2026

Versi	Detail	Tanggal rilis
	Memperbaiki masalah kerusakan agen yang disebabkan oleh ketidakcocokan antara versi runtime Visual C++ tertentu dan fungsi telemetri agen.	
2.3.108	• Menambahkan tampilan IPv6 alamat ke wallpaper. Untuk atribut Memori dan Jaringan, lihat AWS Dokumentasi.	Desember 29, 2025
2.3.56	• Memperbaiki masalah di mana rute jaringan persisten yang telah dikonfigurasi sebelumnya tidak ditangani dengan benar oleh EC2 Launch v2.	November 4, 2025
2.3.5	• Peningkatan deteksi antarmuka jaringan primer menggunakan IMDS saat menambahkan rute.	September 15, 2025
2.2.63	• Agen peluncuran yang diperbarui untuk meningkat kanTelemetri.	Juli 29, 2025
2.1.1	• Ditambahkan dukungan penuh untuk IPv6.	14 Mei 2025
2.0.2107	• Penambahan rute yang disempurnakan untuk menangani skenario saat IPv4 atau IPv6 alamat tidak tersedia di antarmuka.	Maret 27, 2025
2.0.2081	• Memperbaiki masalah di mana informasi sertifikat RDP tidak diambil atau divalidasi dengan benar. Menambahk an fungsionalitas untuk secara otomatis memulai Layanan Desktop Jarak Jauh jika diperlukan. • Izin layanan EC2 Luncurkan v2 yang disesuaikan untuk memperbaiki masalah yang terjadi saat menanyakan status layanan.	Februari 4, 2025

Versi	Detail	Tanggal rilis
2.0.2046	• Memperbarui jalur wallpaper dalam `agent-config.yml` file untuk menggunakan jalur wallpaper sistem operasi default. • Menambahkan telemetri untuk memantau lokasi di mana kesalahan agen terjadi. • Diperbarui pesan log agen.	Oktober 3, 2024
2.0.1981	• Pesan kesalahan perintah `EC2Launch.exe` CLI yang diperbarui untuk pengguna non-Administrator.	Agustus 6, 2024
2.0.1948	• Ditambahkan telemetri untuk memantau penggunaan pilihan password admin. • Izin EC2 Peluncuran yang Dimodifikasi.	Juli 1, 2024
2.0.1924	• Memperbarui UI Pengaturan EC2 Peluncuran. • Memperbarui perintah CLI wallpaper. • Memperbarui installer EC2 Launch.	Juni 10, 2024
2.0.1914	• Tambahkan rute dengan alamat gateway yang tidak ditentukan (`0.0.0.0`untuk IPv4 atau `::` untukIPv6). • Selalu tambahkan keduanya IPv4 dan IPv6 rute. • Memperbaiki masalah saat `Administrator` nama pengguna ditambahkan ke `agent-config.yml` file saat tidak ditentukan. • Izin EC2 Luncurkan v2 yang dimodifikasi.	Juni 5, 2024

Versi	Detail	Tanggal rilis
2.0.1881	• Menambahkan opsi kata sandi terenkripsi ke `setAdminAccount` tugas. • Menambahkan perintah CLI untuk mengenkripsi kata sandi statis di agent-config.yml. • Memperbaiki masalah di mana data pengguna XMLtidak menambahkan PowerShell argumen saat dijalankan dengan izin Administrator. Untuk detail selengkapnya, lihat Bagaimana Amazon EC2 menangani data pengguna untuk instans Windows. • PowerShell Argumen yang disesuaikan untuk `executeScript` tugas dan skrip data pengguna saat dijalankan dengan `LocalSystem` izin. Ketika argumen kosong, agen menggunakan nilai default berikut:`-ExecutionPolicy Unrestricted` . • Mencegah pencetakan versi driver duplikat ke log konsol.	8 Mei 2024

Versi	Detail	Tanggal rilis
2.0.1815	• Penanganan kesalahan yang disesuaikan agar gagal pada masalah penyiapan kritis sebelum sysprep. • Memperbaiki masalah di mana tugas wallpaper dan nama host dapat menggunakan alamat IP yang salah pada instance dengan beberapa alamat IP yang ditetapkan ke antarmuka jaringan utama. • Tugas wallpaper dan nama host diubah untuk mendapatkan IP pribadi dari IMDS terlebih dahulu, kemudian gagal kembali ke WMI jika IMDS dinonaktifkan. • Memperbaiki masalah dengan `initializeVolume` tugas di mana `sc1` volume gagal diinisialisasi karena kesalahan sementara.	Maret 6, 2024
2.0.1739	• Memperbaiki masalah yang mencegah kode keluar ditangkap oleh `executeScript` tugas yang dijalankan sebagai pengguna Administrator Windows.	Januari 17, 2024

Versi	Detail	Tanggal rilis
2.0.1702	• Membatasi izin `Telemetry.log` menjadi `read-execute` saja untuk pengguna standar. • Mengkonfigurasi layanan EC2 Luncurkan Windows untuk memulai kembali pada kegagalan start-up. • Membuat kegagalan `add-routes` dapat ditindaklanjuti dengan melakukan logging output `route.exe stderr`. • Memperbaiki masalah yang terjadi saat metrik rute berada di luar jangkauan [1, 9999]. • Menambahkan dukungan wallpaper ke beberapa tipe instans baru. • Memperbaiki masalah yang disebabkan oleh skrip data pengguna yang berjalan sebagai pengguna Administrator Windows dan mengirim output ke `stderr`.	4 Januari 2024

Versi	Detail	Tanggal rilis
2.0.1643	• Memperbarui alat `ebsnvme-id.exe` ke versi 1.1.0.7. • Memperbaiki masalah dengan menerima penskalaan sisi (RSS) dan menerima pengaturan kedalaman antrean pada tipe instans logam yang dimulai dengan 'logam-*', seperti logam-48x1. • Peristiwa telemetri yang dihapus yang melaporkan perintah data pengguna XML yang memblokir agen. • Tugas `setDnsSuffix` yang diperbarui untuk membatasi devolusi nama domain berdasarkan entri registri: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Menambahkan tugas publik dan CLI yang menambahkan rute jaringan. • Catatan — Ini adalah versi terakhir yang secara resmi mendukung Windows Server 2012. • Catatan — Ini adalah versi terakhir yang secara resmi mendukung sistem operasi 32-bit.	4 Oktober 2023
2.0.1580	• Cara agen peluncuran menangani kesalahan saat Anda mengubah izin file log diubah. • Menambahkan batas waktu habis untuk menghubungkan ke port serial. Batas waktu memungkinkan agen peluncuran untuk terus berjalan jika port serial sedang digunakan.	5 September 2023

Versi	Detail	Tanggal rilis

2.0.1521	• Bendera –block usang dari EC2Launch.exe reset dan perintah sysprep.
	• EC2Launch.exe yang diperbarui untuk mendeteksi dan menangani perintah reset dan sysprep yang digunakan dalam tugas executeScript inline. Perintah tersebut menyebabkan agen berhenti berjalan setelah executeScript tugas menjalankannya.
	• Skrip data pengguna XML yang diperbarui untuk menjalankan inline secara default.
	• Aktifkan skrip data pengguna XML untuk berjalan terpisah dengan tanda baru detach. Untuk detail selengkapnya, lihat Skrip data pengguna.
	• Membuat perubahan berikut ini pada log agen.
	  • Pesan log agen yang diperbarui.
	  • Menghapus executeScript konten dan output dari log agen.
	  • Argumen executeProgram dan output yang dihapus dari log agen.
	• Membuat perubahan berikut pada log konsol.
	  • Menambahkan nilai EnableSCSIPersistentReservations ke log konsol.
		3 Juli 2023

Versi	Detail	Tanggal rilis
2.0.1303	• Menambahkan penanganan kesalahan tambahan dan baris log saat menambahkan rute jaringan. • Diizinkan `executeScript` dan `executeProgram` tugas di PreReady panggung. • Tugas `executeProgram` yang diperbarui untuk menghasilkan file output yang mirip dengan output dari tugas executeScript. Untuk informasi selengkapnya, lihat executeProgram. • Menambahkan telemetri untuk memantau penggunaan perintah agen pemblokiran dalam data pengguna XML.	3 Mei 2023
2.0.1245	• Peningkatan visibilitas tentang kerusakan dengan mencatat tumpukan panggilan rusak dalam teks yang jelas. • Menambahkan EventLog layanan sebagai dependensi startup untuk memperbaiki kerusakan saat layanan EC2 Peluncuran Amazon dimulai lebih cepat daripada EventLog layanan. • Membuat data pengguna XHTML berjalan sebelum PostReady tahap dari file konfigurasi agen (seperti EC2 Launch v1 dan Config EC2). • Menambahkan data pengguna YAMB versi 1.1 untuk membuat data pengguna berjalan sebelum PostReady tahap dari file konfigurasi agen (data pengguna YAMB versi 1.0 berjalan setelah PostReady tahap dari file konfigurasi agen).	8 Maret 2023

Versi	Detail	Tanggal rilis
2.0.1173	• Menambahkan fitur opsional untuk menampilkan tanda instans pada wallpaper. Untuk informasi selengkapnya, lihat setWallpaper. • Menambahkan penanganan kesalahan saat grup keamanan untuk Elastic Graphics tidak disiapkan dengan benar. • Memperbaiki batas waktu saat Layanan Metadata Instans tidak diaktifkan.	6 Februari 2023
2.0.1121	• Memperbaiki masalah saat kesalahan 404 dicetak ke wallpaper saat tidak ada IPv4 alamat publik yang ditetapkan. • Memperbaiki masalah saat sistem file volume diformat sebagai `RAW` ganti `NTFS` saat huruf drive perangkatnya disetel ke. `D` • Memperbaiki masalah di mana volume NVMe SSD salah diidentifikasi sebagai volume EBS. • Memperbaiki kesalahan saat mengaktifkan Windows saat IMDS dinonaktifkan.	4 Januari 2023

Versi	Detail	Tanggal rilis
2.0.1082	• Memperbaiki masalah di mana bidang `setWallpaper : privateIpAddress` kosong saat IMDS dinonaktifkan. • Memperbaiki masalah dengan pengaturan nama host ke IPv4 alamat pribadi saat IMDS dinonaktifkan. • Memperbaiki masalah dengan menginisialisasi volume pada Windows Server 2012. • Memperbaiki masalah dengan pengaturan bingkai jumbo. • Memperbaiki kesalahan ketika tidak ada kunci SSH yang ditentukan pada peluncuran instans. • Memperbaiki kesalahan pada Windows Server 2012 ketika Windows tidak memiliki ReleaseId 'kunci registri.	7 Desember 2022
2.0.1011	• Memperbaiki logika untuk menemukan adaptor jaringan saat PDevice ID Pn kosong.	11 November 2022
2.0.1009	• Menggunakan informasi segmen PCI untuk memilih port konsol.	8 November 2022

Versi	Detail	Tanggal rilis
2.0.982	• Menambahkan logika coba lagi untuk mendapatkan informasi RDP. • Memperbaiki kesalahan selama inisialisasi volume pada `d2.8xlarge` instans. • Memperbaiki masalah di mana adaptor jaringan yang salah dapat dipilih setelah reboot. • Menghapus pesan kesalahan alarm palsu saat ACPI SPCR tidak tersedia.	31 Oktober 2022
2.0.863	• Pembaruan IMDS menunggu logika untuk hanya membuat IMDSv2 permintaan. • Menambahkan logika untuk menetapkan huruf drive ke volume yang sudah diinisialisasi tetapi tidak dipasang. • Mencetak pesan kesalahan yang lebih spesifik ketika jenis key pair tidak didukung. • Memperbaiki bug kode reboot 3010. • Menambahkan pemeriksaan untuk data pengguna yang dengan enkode base64 tidak valid.	6 Juli 2022
2.0.698	• Memperbaiki kesalahan ketik dalam output log saat menjalank an skrip.	30 Januari 2022
2.0.674	• Telemetri mengunggah kontrol privasi. enabled/disabled • Memperbaiki `index out of bounds` bug. • Menghapus pintasan wallpaper selama `sysprep`.	15 November 2021

Versi	Detail	Tanggal rilis
2.0.651	• Menambahkan logika untuk menghapus instalan agen lama selama instalasi EC2 Launch v2. • Memperbaiki masalah `list-volume` CLI saat volume root tidak terdaftar sebagai volume 0.	7 Oktober 2021
2.0.592	• Memperbaiki bug untuk melaporkan status tahap dengan benar. • Menghapus pesan kesalahan alarm palsu saat file log ditutup. • Menambahkan telemetri.	31 Agustus 2021
2.0.548	• Menambahkan angka nol di depan untuk nama host IP hex. • Memperbaiki izin file untuk `enableOpenSsh` tugas. • Memperbaiki crash perintah sysprep.	4 Agustus 2021
2.0.470	• Memperbaiki bug di tahap jaringan untuk menunggu DHCP menetapkan IP ke instans. • Memperbaiki bug dengan `setDnsSuffix` ketika kunci `SearchList` registri tidak ada. • Memperbaiki bug dalam logika devolusi DNS di. `setDnsSuffix` • Menambahkan rute jaringan setelah reboot perantara. • Mengizinkan `initializeVolume` untuk menulis ulang volume yang ada. • Menghapus informasi tambahan dari subperintah versi.	20 Juli 2021

Versi	Detail	Tanggal rilis
2.0.285	• Menambahkan opsi untuk menjalankan skrip pengguna dalam proses terpisah. • Userdata warisan (userdata XML) sekarang berjalan dalam proses terpisah, yang merupakan perilaku yang sama dengan agen peluncuran sebelumnya. • Menambahkan bendera CLI ke perintah `sysprep` dan `reset`, yang memungkinkannya untuk memblokir sampai layanan berhenti. • Membatasi izin folder konfigurasi.	8 Maret 2021
2.0.207	• Menambahkan bidang `hostName` opsional ke tugas `setHostName` . • Memperbaiki bug reboot. Reboot tugas `executeScript` dan `executeProgram` akan ditandai sebagai berjalan. • Menambahkan lebih banyak kode kembali untuk perintah status. • Menambahkan layanan bootstrap untuk memperbaiki masalah startup saat menjalankan tipe instans `t2.nano`. • Memperbaiki mode instalasi bersih untuk menghapus file yang tidak terlacak oleh installer.	2 Februari 2021

Versi	Detail	Tanggal rilis
2.0.160	• Memperbaiki perintah `validate` untuk mendeteksi nama tahap yang tidak valid. • Menambahkan perintah `w32tm resync` di tugas `addroutes` . • Memperbaiki masalah dengan mengubah urutan pencarian akhiran DNS. • Menambahkan syarat pemeriksaan agar bisa melaporkan data pengguna yang tidak valid dengan lebih baik.	4 Desember 2020
2.0.153	Menambahkan fungsionalitas Sysprep di. UserData	3 November 2020
2.0.146	• Memperbaiki masalah dengan RootExtend AMIs non-Inggris. • Memberi izin menulis grup pengguna ke file log. • Membuat partisi MS Reserved untuk volume GPT. • Menambahkan perintah daftar-volume dan dropdown volume di pengaturan Amazon EC2 Launch. • Menambahkan get-agent-config perintah untuk mencetak file agent-config.ymldalam format yaml atau json. • Hapus kata sandi statis jika tidak ada kunci publik yang terdeteksi.	6 Oktober 2020

Versi	Detail	Tanggal rilis
2.0.124	• Menambahkan opsi untuk menampilkan versi OS pada wallpaper. • Menginisialisasi volume EBS yang dienkripsi. • Menambahkan rute untuk VPCs tanpa nama DNS lokal.	10 September 2020
2.0.104	• Membuat daftar pencarian sufiks DNS jika tidak ada. • Lewati mode Hibernasi jika tidak diminta.	12 Agustus 2020
2.0.0	Pelepasan awal.	Selasa, Selasa, 30 Juni 2020

Gunakan agen EC2launch v1 untuk melakukan tugas selama peluncuran instans Windows EC2

Amazon dikelola AMIs untuk Windows Server 2016 dan 2019 termasuk satu set skrip Windows Powershell yang disebut EC2 Launch. EC2Peluncuran melakukan tugas selama boot instance awal. Untuk informasi tentang versi EC2 peluncuran yang disertakan dalam AWS Windows AMIs, lihat Referensi AMI AWS Windows.

> **Note**
>
> Agen peluncuran terbaru untuk Windows Server 2016 dan versi sistem operasi yang lebih baru adalah EC2 Launch v2, yang menggantikan EC2 Config EC2 dan Launch, dan sudah diinstal sebelumnya AWS pada Windows Server 2016 dan AMIs 2019 dengan nama yang dimulai. `EC2LaunchV2-Windows_Server-*` Anda juga dapat menginstal dan mengonfigurasi agen secara manual di Windows Server 2016 dan 2019. Untuk informasi selengkapnya, lihat Instal EC2 Launch v2.
> Untuk menggunakan EC2 Launch with IMDSv2, versi harus 1.3.2002730 atau yang lebih baru.

Anda dapat menggunakan PowerShell perintah Windows berikut untuk memverifikasi versi EC2 Launch yang diinstal.

```
Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

EC2Luncurkan tugas

EC2Peluncuran melakukan tugas-tugas berikut secara default selama boot instance awal:

- Siapkan wallpaper baru yang menampilkan informasi tentang instans.
- Menetapkan nama komputer ke IPv4 alamat pribadi instance.
- Mengirimkan informasi instans ke konsol Amazon EC2.
- Mengirim sidik jari sertifikat RDP ke konsol EC2.
- Mengatur kata sandi acak untuk akun administrator.
- Menambahkan sufiks DNS.
- Secara dinamis memperluas partisi sistem operasi untuk menyertakan ruang yang tidak dipartisi.
- Menjalankan data pengguna (jika ditentukan). Untuk informasi selengkapnya tentang menentukan data pengguna, lihat Jalankan perintah saat Anda meluncurkan instans EC2 dengan input data pengguna.
- Mengatur rute statis persisten untuk menjangkau layanan metadata dan server AWS KMS .

> **Important**
>
> Jika AMI kustom dibuat dari instans ini, rute ini diambil sebagai bagian dari konfigurasi OS dan setiap instans baru yang diluncurkan dari AMI akan mempertahankan rute yang sama, terlepas dari penempatan subnet. Untuk memperbarui rute, lihat Perbarui metadata/KMS rute untuk Server 2016 dan yang lebih baru saat meluncurkan AMI khusus.

Tugas berikut membantu menjaga kompatibilitas mundur dengan layanan EC2 Config. Anda juga dapat mengonfigurasi EC2 Peluncuran untuk melakukan tugas-tugas ini selama startup:

- Inisialisasi volume EBS sekunder.
- Kirim log Peristiwa Windows ke log konsol EC2.
- Kirim pesan siap digunakan Windows ke konsol EC2.

EC2Luncurkan struktur direktori

EC2Peluncuran diinstal secara default pada Windows Server 2016 dan kemudian AMIs di direktori root`C:\ProgramData\Amazon\EC2-Windows\Launch`.

> **Note**
>
> Secara default, Windows menyembunyikan file dan folder dalam `C:\ProgramData`. Untuk melihat direktori dan file EC2 Luncurkan, Anda harus mengetikkan jalur di Windows Explorer atau mengubah properti folder untuk menampilkan file dan folder tersembunyi.

Direktori `Launch` berisi subdirektori berikut.

- `Scripts`— Berisi PowerShell skrip yang membentuk EC2 Peluncuran.
- `Module` — Berisi modul untuk membangun skrip yang terkait dengan Amazon EC2.
- `Config` — Berisi file konfigurasi skrip yang dapat Anda sesuaikan.
- `Sysprep` — Berisi sumber daya Sysprep.
- `Settings` — Berisi aplikasi untuk antarmuka pengguna grafis Sysprep.
- `Library` — Berisi pustaka bersama untuk agen peluncuran EC2.
- `Log`— Berisi subdirektori untuk skrip dan file log yang dihasilkan oleh skrip.

Telemetri

Telemetri adalah informasi tambahan yang membantu AWS untuk lebih memahami kebutuhan Anda, mendiagnosis masalah, dan memberikan fitur untuk meningkatkan pengalaman Anda dengan AWS layanan.

EC2Luncurkan versi `1.3.2003498` dan kemudian kumpulkan telemetri, seperti metrik penggunaan dan kesalahan. Data ini dikumpulkan dari instans Amazon EC2 tempat EC2 Peluncuran berjalan. Ini termasuk semua Windows yang AMIs dimiliki oleh AWS.

Jenis telemetri berikut dikumpulkan oleh EC2 Peluncuran:

- Informasi penggunaan — perintah agen, metode penginstalan, dan frekuensi eksekusi terjadwal.
- Kesalahan dan informasi diagnostik - instalasi agen dan menjalankan kode kesalahan.

Contoh data yang dikumpulkan:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

Telemetri tidak diaktifkan secara default. Anda dapat menonaktifkan kumpulan telemetri kapan saja. Jika telemetri diaktifkan, EC2 Launch mengirimkan data telemetri tanpa pemberitahuan pelanggan tambahan.

Pilihan Anda untuk mengaktifkan atau menonaktifkan telemetri dikumpulkan.

Anda dapat memilih masuk atau keluar dari kumpulan telemetri. Pilihan Anda untuk mengikuti atau tidak mengikuti telemetri dikumpulkan untuk memastikan bahwa kami mematuhi opsi telemetri Anda.

Visibilitas telemetri

Saat telemetri diaktifkan, telemetri muncul di output konsol Amazon EC2 sebagai berikut:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Menonaktifkan telemetri pada sebuah instans

Untuk menonaktifkan telemetri dengan menyetel variabel lingkungan sistem, jalankan perintah berikut sebagai administrator:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Untuk menonaktifkan telemetri selama instalasi, jalankan `install.ps1` sebagai berikut:

```
. .\install.ps1 -EnableTelemetry:$false
```

Topik lainnya untuk EC2 Peluncuran

- Instal versi terbaru EC2 Launch
- Konfigurasikan agen EC2 Launch v1 pada instance Windows Anda

- EC2Luncurkan riwayat versi

Instal versi terbaru EC2 Launch

Gunakan prosedur berikut untuk mengunduh dan menginstal versi terbaru EC2 Peluncuran pada instans Anda.

Untuk mengunduh dan menginstal versi terbaru EC2 Launch

1. Jika Anda telah menginstal dan mengkonfigurasi EC2 Launch pada sebuah instance, buat cadangan file konfigurasi EC2 Launch. Proses penginstalan tidak menyimpan perubahan dalam file ini. Secara default, file terletak di direktori `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Unduh EC2-Windows-Launch.zip ke direktori pada instans.
3. Unduh install.ps1 ke direktori yang sama tempat Anda mengunduh `EC2-Windows-Launch.zip`.
4. Jalankan `install.ps1`
5. Jika Anda membuat cadangan file konfigurasi EC2 Launch, salin ke `C:\ProgramData\Amazon\EC2-Windows\Launch\Config` direktori.

Untuk mengunduh dan menginstal versi terbaru EC2 Launch menggunakan PowerShell

Jika Anda telah menginstal dan mengkonfigurasi EC2 Launch pada sebuah instance, buat cadangan file konfigurasi EC2 Launch. Proses penginstalan tidak menyimpan perubahan dalam file ini. Secara default, file terletak di direktori `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Untuk menginstal versi terbaru EC2 Launch menggunakan PowerShell, jalankan perintah berikut dari PowerShell jendela sebagai administrator:

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
```

```
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifikasi instalasi dengan memeriksa agen peluncuran. Jalankan perintah berikut dari PowerShell jendela sebagai administrator:

```
Import-Module C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psm1
Import-LocalizedData -BaseDirectory C:\ProgramData\Amazon\EC2-Windows\Launch\Module\ -
FileName 'Ec2Launch.psd1' -BindingVariable moduleManifest
$moduleManifest.Get_Item('ModuleVersion')
```

Konfigurasikan agen EC2 Launch v1 pada instance Windows Anda

Setelah instans Anda diinisialisasi pertama kali, Anda dapat mengonfigurasi EC2 Peluncuran untuk dijalankan lagi dan melakukan tugas start-up yang berbeda.

Tugas

- Konfigurasikan tugas inisialisasi
- Jadwalkan EC2 Peluncuran untuk berjalan di setiap boot
- Inisialisasi drive dan petakan huruf drive
- Kirim log peristiwa Windows ke log konsol EC2.
- Kirim pesan Windows siap setelah boot berhasil

Konfigurasikan tugas inisialisasi

Tentukan pengaturan di file `LaunchConfig.json` untuk mengaktifkan atau menonaktifkan tugas inisialisasi berikut:

- Atur nama komputer ke IPv4 alamat pribadi instance.
- Atur monitor agar selalu menyala.
- Siapkan wallpaper baru.
- Tambahkan daftar sufiks DNS.

> **Note**
>
> Ini menambahkan pencarian akhiran DNS untuk domain berikut dan mengkonfigurasi sufiks standar lainnya. Untuk informasi selengkapnya tentang cara agen peluncuran mengatur sufiks DNS, lihat. Konfigurasikan DNS Suffix untuk agen peluncuran EC2 Windows
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- Perluas ukuran volume boot.
- Setel kata sandi administrator.

Untuk mengonfigurasi pengaturan inisialisasi

1. Saat ingin mengonfigurasikan instans, buka file berikut ini dalam editor teks: `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json`.
2. Perbarui pengaturan berikut sesuai kebutuhan dan simpan perubahan Anda. Sediakan kata sandi dalam `adminPassword` hanya jika `adminPasswordtype` adalah `Specify`.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
}
```

Jenis kata sandi ditentukan sebagai berikut:

`Random`

EC2Peluncuran menghasilkan kata sandi dan mengenkripsi menggunakan kunci pengguna. Sistem akan menonaktifkan pengaturan ini setelah instans dijalankan sehingga kata sandi ini akan tetap ada jika instans tersebut di-boot ulang atau dihentikan dan dimulai.

`Specify`

EC2Peluncuran menggunakan kata sandi yang Anda tentukan`adminPassword`. Jika kata sandi tidak memenuhi persyaratan sistem, EC2 Launch menghasilkan kata sandi acak sebagai gantinya. Kata sandi disimpan dalam teks `LaunchConfig.json` yang jelas dan dihapus setelah Sysprep menetapkan kata sandi administrator. EC2Luncurkan mengenkripsi kata sandi menggunakan kunci pengguna.

`DoNothing`

EC2Peluncuran menggunakan kata sandi yang Anda tentukan dalam `unattend.xml` file. Jika Anda tidak menentukan kata sandi di `unattend.xml`, akun administrator akan dinonaktifkan.

3. Di Windows PowerShell, jalankan perintah berikut untuk menjadwalkan skrip untuk dijalankan sebagai Tugas Terjadwal Windows. Skrip berjalan satu kali selama boot berikutnya dan kemudian menonaktifkan tugas-tugas ini agar tidak berjalan lagi.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

Jadwalkan EC2 Peluncuran untuk berjalan di setiap boot

Anda dapat menjadwalkan EC2 Peluncuran untuk berjalan di setiap boot, bukan hanya boot awal.

Untuk mengaktifkan EC2 Peluncuran berjalan di setiap boot:

1. Buka Windows PowerShell dan jalankan perintah berikut:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

2. Atau, jalankan executable dengan perintah berikut:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

Kemudian pilih `Run EC2Launch on every boot`. Anda dapat menentukan apakah instans EC2 Anda `Shutdown without Sysprep` atau `Shutdown with Sysprep`.

> **Note**
>
> Saat Anda mengaktifkan EC2 Peluncuran untuk berjalan di setiap boot, hal berikut terjadi saat EC2 Peluncuran berjalan berikutnya:
>
> - Jika `AdminPasswordType` masih diatur ke`Random`, EC2 Launch akan menghasilkan password baru pada boot berikutnya. Setelah boot itu, `AdminPasswordType` secara otomatis diatur `DoNothing` untuk mencegah EC2 Peluncuran menghasilkan kata sandi baru pada boot berikutnya. Untuk mencegah EC2 Launch membuat kata sandi baru pada boot pertama, atur `AdminPasswordType` secara manual `DoNothing` sebelum Anda reboot.
> - `HandleUserData` akan diatur kembali ke `false` kecuali data pengguna mengatur `persist` ke `true`. Untuk informasi selengkapnya, lihat the section called “Skrip data pengguna”.

Inisialisasi drive dan petakan huruf drive

Tentukan pengaturan di file `DriveLetterMappingConfig.json` untuk memetakan huruf drive ke volume pada instans EC2 Anda. Skrip menginisialisasi drive yang belum diinisialisasi dan dipartisi. Untuk informasi selengkapnya tentang mendapatkan detail volume di Windows, lihat Get-Volume di dokumentasi Microsoft.

Untuk memetakan huruf drive ke volume

1. Buka file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` di editor teks.
2. Tentukan pengaturan volume berikut dan simpan perubahan Anda:

```
{
 "driveLetterMapping": [
  {
   "volumeName": "sample volume",
   "driveLetter": "H"
  }
```

```
 ]
}
```

3. Buka Windows PowerShell dan gunakan perintah berikut untuk menjalankan skrip EC2 Launch yang menginisialisasi disk:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Untuk menginisialisasi disk setiap kali booting instans, tambahkan bendera `-Schedule` sebagai berikut:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -Schedule
```

Kirim log peristiwa Windows ke log konsol EC2.

Tentukan pengaturan di file `EventLogConfig.json` untuk mengirim log Peristiwa Windows ke log konsol EC2.

Untuk mengonfigurasi pengaturan untuk mengirim log Peristiwa Windows

1. Pada instans, buka file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` dalam editor teks.
2. Konfigurasikan pengaturan log berikut dan simpan perubahan Anda:

```
{
 "events": [
  {
   "logName": "System",
   "source": "An event source (optional)",
   "level": "Error | Warning | Information",
   "numEntries": 3
  }
 ]
}
```

3. Di Windows PowerShell, jalankan perintah berikut sehingga sistem menjadwalkan skrip untuk dijalankan sebagai Tugas Terjadwal Windows setiap kali instance boot.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -Schedule
```

Log dapat membutuhkan waktu tiga menit atau lebih untuk muncul di log konsol EC2.

Kirim pesan Windows siap setelah boot berhasil

Layanan EC2config mengirim pesan “Windows siap” ke konsol EC2 setelah setiap boot. EC2Peluncuran mengirim pesan ini hanya setelah boot awal. Untuk kompatibilitas mundur dengan layanan EC2 Config, Anda dapat EC2 menjadwalkan Peluncuran untuk mengirim pesan ini setelah setiap boot. Pada contoh, buka Windows PowerShell dan jalankan perintah berikut. Sistem menjadwalkan skrip untuk dijalankan sebagai Tugas Terjadwal Windows.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -Schedule
```

EC2Luncurkan riwayat versi

Untuk mengunduh dan menginstal versi terbaru EC2 Launch, lihatInstal versi terbaru EC2 Launch.

Tabel berikut menjelaskan versi rilis dari EC2 Launch.

Versi	Detail	Tanggal rilis
1.4.299	• Logika yang dioptimalkan untuk mengambil versi EC2 WinUtil driver. • Mengurangi waktu ke Windows Siap dengan menghapus kueri status Hyper-V.	3 Maret 2026
1.4.183	• Logika penginstal yang diperbarui untuk mencegah instalasi yang tidak didukung pada Windows Server 2022. • Diperbarui untuk mencetak versi EC2 WinUtil driver ke log konsol instance.	4 Februari 2026
1.4.6	• Diperbarui pesan log agen.	13 Oktober 2025
1.3.2005119	•	11 Februari 2025

Versi	Detail	Tanggal rilis
	Memperbaiki masalah di mana `Invoke-Userdata` akan gagal saat dipanggil tanpa parameter apa pun.	
1.3.2005065	• Memperbaiki masalah di mana informasi sertifikat RDP tidak diambil atau divalidasi dengan benar. Menambahkan fungsionalitas untuk secara otomatis memulai Layanan Desktop Jarak Jauh jika diperlukan.	22 Oktober 2024
1.3.2005008	• Diperbarui `Set-Wallpaper` untuk kembali ke latar belakang warna solid jika gambar wallpaper default tidak ditemukan.	6 Agustus 2024
1.3.2004959	• Logika penginstal yang diperbarui untuk mencegah instalasi yang tidak didukung pada Windows Server 2025 atau yang lebih baru.	2 Juli 2024
1.3.2004891	• Memperbaiki masalah yang tidak `HandleUserData` disetel `false` seperti yang diharapkan. • Menambahkan opsi `Encrypted` kata sandi ke`LaunchConfig.json` . • Mengubah `Settings UI` perilaku untuk mengenkripsi kata sandi yang ditentukan pengguna secara default. • Ditambahkan `SetAdminPasswordConfig.ps1` untuk mengonversi opsi `Specify` kata `Encrypted` sandi ke opsi kata sandi di file konfigurasi agen.	31 Mei 2024
1.3.2004617	• Memperbaiki kesalahan saat mengatur wallpaper.	15 Januari 2024

Versi	Detail	Tanggal rilis
1.3.2004592	• Izin akses yang diperbarui yang ditetapkan oleh install.ps1 untuk `%ProgramData%\Amazon\EC2-Windows\Launch` . • folder/file Akses EC2 Luncurkan terbatas ke read-execute hanya untuk akun pengguna standar. • Mengubah agen agar berhenti menunggu Layanan Metadata Instans (IMDS) untuk diinisialisasi jika IMDS tidak diaktifkan untuk instans. • Menambahkan batas waktu lima menit saat menunggu IMDS diinisialisasi. • Mengubah agen untuk menulis telemetri ke log konsol instans sebelum pesan `Windows is Ready`, bukan setelahnya. • Menambahkan dukungan wallpaper ke beberapa tipe instans baru. Untuk informasi selengkapnya tentang izin akses dan izin akun pengguna dari direktori EC2 Peluncuran, lihat. the section called “EC2Luncurkan struktur direktori”	2 Januari 2024
1.3.2004491	• Menambahkan telemetri untuk memantau penggunaan opsi Tentukan kata sandi admin.	9 November 2023
1.3.2004462	• Menambahkan flush setelah setiap penulisan ke konsol serial.	18 Oktober 2023

Versi	Detail	Tanggal rilis
1.3.2004438	• Membatasi devolusi nama domain berdasarkan entri registri: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Izin `UserdataExecution.log` terbatas hanya untuk `Administrators` . • Menambahkan pesan kesalahan di Log Peristiwa Windows saat inisialisasi log gagal.	4 Oktober 2023
1.3.2004256	• Menambahkan nilai `EnableSCSIPersistentReservations` ke log konsol. • Menambahkan kemampuan coba lagi untuk Get-ConsolePort.	7 Juli 2023
1.3.2004052	• Memperbaiki kesalahan yang terjadi saat tidak ada kunci SSH yang ditentukan saat peluncuran instans. • Diperbarui untuk mencoba lagi memulai layanan Amazon SSMAgent Windows pada kegagalan. • Diperbarui untuk SysprepInstance gagal.ps1 jika BeforeSysprep .cmd gagal dengan kode keluar bukan nol.	8 Maret 2023
1.3.2003975	• Memperbaiki masalah yang memengaruhi build Packer AMI di mana `SysprepInstance.ps1` mengembalikan 1. `$LastErrorCode`	24 Desember 2022

Versi	Detail	Tanggal rilis
1.3.2003961	• Memperbaiki masalah di mana kata sandi administrator yang ditentukan secara eksplisit ditimpa dengan kata sandi acak pada instans yang diluncurkan dengan cepat. • Memperbaiki masalah di mana Agen SSM gagal memulai pada tipe instans yang lebih kecil. • Memperbaiki masalah saat log konsol instans berisi, `RDPCERTIFICATE-THUMBPRINT: 0000000 0000000000000000` bukan nilai cap jempol sertifikat RDP yang valid.	6 Desember 2022
1.3.2003923	• Memperbaiki logika untuk menemukan adaptor jaringan saat PDevice ID Pn kosong.	9 November 2022
1.3.2003919	• Diperbarui Get-ConsolePort untuk menggunakan informasi segmen PCI. • Memperbaiki masalah di mana adaptor jaringan yang salah dapat dipilih setelah reboot. • Logika start-SSM-Agent batas waktu tetap. • Memperbaiki kompatibilitas mundur untuk alias AdminCred entials fungsi Kirim.	8 November 2022
1.3.2003857	• Memprioritaskan adaptor dengan gateway default saat adaptor jaringan utama dipilih. • Enkripsi kata sandi dalam memori yang diperluas.	3 Oktober 2022

Versi	Detail	Tanggal rilis
1.3.2003824	• Memperbaiki kesalahan selama `setComputerName` . • Menambahkan logika untuk melewati aktivasi Windows ketika kode penagihan BYOL terdeteksi. • Menambahkan enkripsi kata sandi dalam memori. • Memperbaiki kesalahan selama inisialisasi volume aktif. `m6id.4xlarge`	30 Agustus 2022
1.3.2003691	• Logika tunggu IMDS yang diperbarui untuk hanya membuat IMDSv2 permintaan. • Memperbaiki bug yang memengaruhi instalasi eGPU.	21 Juni 2022
1.3.2003639	• Menambahkan logika tunggu adaptor jaringan untuk mencegah penggunaan sebelum inisialisasi. • Memperbaiki masalah kecil.	10 Mei 2022
1.3.2003498	• Menambahkan telemetri. • Menambahkan pintasan ke UI Pengaturan. • PowerShell Skrip yang diformat. • Memperbaiki masalah dengan shutdown yang terjadi sebelum BeforeSysprep .cmd selesai.	31 Januari 2022
1.3.2003411	Logika pembuatan kata sandi untuk mengecualikan kata sandi dengan kompleksitas rendah diubah.	4 Agustus 2021
1.3.2003364	Diperbarui Instal- EgpuManager dengan IMDSv2 dukungan.	7 Juni 2021

Versi	Detail	Tanggal rilis
1.3.2003312	• Menambahkan baris log sebelum dan sesudah pengaturan `setMonitorAlwaysOn` . • Menambahkan versi paket AWS Nitro Enclave ke log konsol.	4 Mei 2021
1.3.2003284	Peningkatan model izin dengan memperbarui lokasi untuk menyimpan data pengguna ke `LocalAppData` .	23 Maret 2021
1.3.2003236	• Metode yang diperbarui untuk mengatur kata sandi pengguna di `Set-AdminAccount` dan `Randomize-LocalAdminPassword` . • Memperbaiki`InitializeDisks` untuk memeriksa apakah disk diatur untuk membaca hanya sebelum mengaturnya menjadi dapat ditulis.	11 Februari 2021
1.3.2003210	Perbaiki lokalisasi untuk `install.ps1` .	7 Januari 2021
1.3.2003205	Perbaikan keamanan untuk `install.ps1` untuk memperbarui izin di direktori `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` .	28 Desember 2020
1.3.2003189	Menambahkan `w32tm resync` setelah menambahkan rute.	4 Desember 2020
1.3.2003155	Informasi tipe instans yang diperbarui.	25 Agustus 2020
1.3.2003150	Menambahkan `OsCurrentBuild` dan `OsReleaseId` ke output konsol .	22 April 2020
1.3.2003040	Memperbaiki logika fallback IMDS versi 1.	7 April 2020
1.3.2002730	Menambahkan dukungan untuk IMDS V2.	3 Maret 2020

Versi	Detail	Tanggal rilis
1.3.2002240	Memperbaiki masalah kecil.	31 Oktober 2019
1.3.2001660	Memperbaiki masalah login otomatis untuk pengguna tanpa kata sandi setelah pertama kali menjalankan Sysprep.	2 Juli 2019
1.3.2001360	Memperbaiki masalah kecil.	27 Maret 2019
1.3.2001220	Semua PowerShell skrip ditandatangani.	28 Februari 2019
1.3.2001200	Memperbaiki masalah InitializeDisks dengan.ps1 di mana menjalankan skrip pada node di Windows Server Failover Cluster akan memformat drive pada node jarak jauh yang huruf drive-nya cocok dengan huruf drive lokal.	27 Februari 2019
1.3.2001160	Memperbaiki wallpaper yang hilang di Windows 2019.	22 Februari 2019
1.3.2001040	• Menambahkan plugin untuk mengatur monitor agar tidak pernah mati untuk memperbaiki masalah ACPI. • Edisi dan versi SQL Server ditulis ke konsol.	21 Januari 2019
1.3.2000930	Perbaiki untuk menambahkan rute ke metadata pada ipv6-enab led. ENIs	2 Januari 2019
1.3.2000760	• Menambahkan konfigurasi default untuk pengaturan RSS dan Menerima Antrean untuk perangkat ENA. • Hibernasi dinonaktifkan selama Sysprep.	5 Desember 2018

Versi	Detail	Tanggal rilis
1.3.2000630	• Menambahkan rute 169.254.169.253/32 untuk server DNS. • Menambahkan filter pengaturan pengguna Admin. • Perbaikan dilakukan pada hibernasi instans. • Menambahkan opsi untuk menjadwalkan EC2 Peluncuran untuk berjalan di setiap boot.	9 November 2018
1.3.2000430.0	• Menambahkan rute 169.254.169.123/32 ke layanan waktu AMZN. • Menambahkan rute 169.254.169.249/32 ke layanan lisensi GRID. • Menambahkan batas waktu habis 25 detik saat mencoba memulai Systems Manager.	19 September 2018
1.3.200039.0	• Memperbaiki huruf drive yang tidak tepat untuk volume EBS NVME. • Menambahkan logging tambahan untuk versi driver NVME.	15 Agustus 2018
1.3.2000080	Memperbaiki masalah kecil.	
1.3.610	Memperbaiki masalah pengalihan output dan error ke file dari data pengguna.	
1.3.590	• Menambahkan tipe instans yang hilang di wallpaper. • Memperbaiki masalah pemetaan huruf drive dan penginstalan disk.	

Versi	Detail	Tanggal rilis
1.3.580	• Memperbaiki `Get-Metadata` untuk menggunakan pengaturan proxy sistem default untuk permintaan web. • Menambahkan kasus khusus untuk inisialisasi NVMe dalam disk. • Memperbaiki masalah kecil.	
1.3.550	Menambahkan opsi `-NoShutdown` untuk mengaktifkan Sysprep tanpa pematian.	
1.3.540	Memperbaiki masalah kecil.	
1.3.530	Memperbaiki masalah kecil.	
1.3.521	Memperbaiki masalah kecil.	
1.3.0	• Memperbaiki masalah panjang heksadesimal untuk perubahan nama komputer. • Memperbaiki kemungkinan loop reboot untuk perubahan nama komputer. • Memperbaiki masalah dalam pengaturan wallpaper.	
1.2.0	• Perbarui untuk menampilkan informasi tentang sistem operasi (OS) yang diinstal di log sistem EC2. • Perbarui untuk menampilkan versi EC2Launch dan SSM Agent di log sistem EC2. • Memperbaiki masalah kecil.	

Versi	Detail	Tanggal rilis
1.1.2	• Perbarui untuk menampilkan informasi driver ENA di log sistem EC2. • Perbarui untuk mengecualikan Hyper-V dari logika filter NIC utama. • Menambahkan AWS KMS server dan port ke kunci registri untuk aktivasi KMS. • Penyiapan wallpaper yang ditingkatkan untuk banyak pengguna. • Perbarui untuk menghapus rute dari penyimpanan persisten. • Perbarui untuk menghapus z dari zona ketersediaan di daftar sufiks DNS. • Perbarui untuk mengatasi masalah dengan tag < runAsLocal System> dalam data pengguna.	
1.1.1	Pelepasan awal.	

Gunakan layanan EC2config untuk melakukan tugas selama peluncuran instans sistem operasi Windows lama EC2

> **Note**
>
> EC2Config telah mencapai akhir dukungan. Versi sistem operasi yang dijalankannya tidak lagi didukung oleh Microsoft. Kami sangat menyarankan Anda meningkatkan ke agen peluncuran terbaru.
> Agen peluncuran terbaru untuk Windows Server 2022 dan versi sistem operasi yang lebih baru adalah EC2Launch v2, yang menggantikan EC2 Config EC2 dan Launch, dan sudah diinstal sebelumnya AWS pada Windows Server 2022 dan 2025. AMIs Anda juga dapat

menginstal dan mengonfigurasi agen secara manual di Windows Server 2016 dan 2019. Untuk informasi selengkapnya, lihat Instal EC2 Launch v2.

Windows AMIs untuk versi Windows Server sebelum Windows Server 2016 menyertakan layanan opsional, layanan EC2 Config ()`EC2Config.exe`. EC2Config dimulai saat instance melakukan booting dan melakukan tugas selama startup dan setiap kali Anda menghentikan atau memulai instance. EC2Config juga dapat melakukan tugas sesuai permintaan. Beberapa dari tugas ini diaktifkan secara otomatis, sementara yang lainnya harus diaktifkan secara manual. Meskipun opsional, layanan ini menyediakan akses ke fitur lanjutan yang tidak tersedia tanpa layanan ini. Layanan ini berjalan diLocalSystem Akun.

Layanan EC2 Config menjalankan Sysprep, alat Microsoft yang memungkinkan Anda membuat AMI Windows yang disesuaikan yang dapat digunakan kembali. Ketika EC2 Config memanggil Sysprep, ia menggunakan file `%ProgramFiles%\Amazon\EC2ConfigService\Settings` untuk menentukan operasi mana yang akan dilakukan. Anda dapat mengedit file-file ini secara tidak langsung menggunakan dialog sistem Properti Layanan EC2, atau langsung menggunakan editor XHTML atau editor teks. Namun, ada beberapa pengaturan lanjutan yang tidak tersedia di dialog sistem Properti Layanan Ec2, jadi Anda harus mengedit entri tersebut secara langsung.

Jika Anda membuat AMI dari sebuah instans setelah memperbarui pengaturannya, pengaturan baru tersebut diterapkan ke setiap instans yang diluncurkan dari AMI baru. Untuk informasi tentang membuat grafik, lihat Buat AMI yang didukung Amazon EBS-Backed.

EC2Config menggunakan file pengaturan untuk mengontrol operasinya. Anda dapat memperbarui file pengaturan ini dengan menggunakan alat grafis atau dengan mengedit file XML secara langsung. Biner layanan dan file tambahan terdapat dalam direktori `%ProgramFiles%\Amazon\EC2ConfigService`.

Daftar Isi

- EC2Config dan AWS Systems Manager
- EC2Tugas Config
- EC2File pengaturan Config
- Instal EC2 Config versi terbaru
- Konfigurasikan setelan proksi .NET untuk EC2 layanan Config
- Setel properti layanan EC2config dari dialog sistem pada instans Windows EC2 Anda

- Memecahkan masalah dengan agen peluncuran Config EC2
- EC2riwayat versi Config

EC2Config dan AWS Systems Manager

Layanan EC2 Config memproses permintaan Systems Manager pada instance yang dibuat dari AMIs untuk versi Windows Server sebelum Windows Server 2016 yang diterbitkan sebelum November 2016.

Instans yang dibuat dari AMIs untuk versi Windows Server sebelum Windows Server 2016 yang diterbitkan setelah November 2016 termasuk layanan EC2 Config dan Agen SSM. EC2Config melakukan semua tugas yang dijelaskan sebelumnya, dan Agen SSM memproses permintaan untuk kemampuan Systems Manager seperti Run Command dan State Manager.

Anda dapat menggunakan Run Command untuk memutakhirkan instans yang ada untuk digunakan ke versi terbaru dari layanan EC2 Config dan Agen SSM. Untuk informasi selengkapnya, lihat Memperbarui Agen SSM menggunakan Run Command di Panduan AWS Systems Manager Pengguna.

EC2Tugas Config

EC2Config menjalankan tugas startup awal saat instance pertama kali dimulai dan kemudian menonaktifkannya. Untuk menjalankan tugas ini lagi, Anda harus secara eksplisit mengaktifkannya sebelum mematikan instans, atau dengan menjalankan Sysprep secara manual. Tugas-tugas tersebut adalah sebagai berikut:

- Tetapkan kata sandi terenkripsi acak untuk akun administrator.
- Buat dan instal sertifikat host yang digunakan untuk Remote Desktop Connection.
- Secara dinamis, perluas partisi sistem operasi untuk menyertakan ruang yang tidak dipartisi.
- Jalankan data pengguna yang ditentukan (dan Cloud-Init, jika sudah diinstal). Untuk informasi selengkapnya tentang menentukan data pengguna, lihat Jalankan perintah saat Anda meluncurkan instans EC2 dengan input data pengguna.

EC2Config melakukan tugas-tugas berikut setiap kali instance dimulai:

- Ubah nama host agar sesuai dengan alamat IP privat dalam notasi Hex (tugas ini dinonaktifkan secara default dan harus diaktifkan untuk dijalankan saat dimulainya instans).

- Konfigurasikan server manajemen kunci (AWS KMS), periksa status aktivasi Windows, dan aktifkan Windows seperlunya.
- Pasang semua volume Amazon EBS dan volume penyimpanan instans, dan petakan nama volume ke huruf drive.
- Tulis entri log peristiwa ke konsol untuk membantu pemecahan masalah (tugas ini dinonaktifkan secara default dan harus diaktifkan agar dapat dijalankan saat instans dimulai).
- Tulis ke konsol bahwa Windows sudah siap.
- Tambahkan rute khusus ke adaptor jaringan utama untuk mengaktifkan alamat IP berikut ketika satu NIC atau beberapa NICs terpasang:`169.254.169.250`,`169.254.169.251`, dan`169.254.169.254`. Alamat ini digunakan oleh Windows Activation dan ketika Anda mengakses metadata instans.

> **Note**
>
> Jika OS Windows dikonfigurasi untuk digunakan IPv4, alamat IPv4 link-lokal ini dapat digunakan. Jika OS Windows memiliki tumpukan protokol IPv4 jaringan dinonaktifkan dan digunakan IPv6 sebagai gantinya, tambahkan `[fd00:ec2::250]` sebagai pengganti `169.254.169.250` dan`169.254.169.251`. Kemudian, tambahkan `[fd00:ec2::254]` sebagai pengganti `169.254.169.254`.

EC2Config melakukan tugas berikut setiap kali pengguna login:

- Tampilkan informasi wallpaper ke latar belakang desktop.

Saat instance berjalan, Anda dapat meminta EC2 Config melakukan tugas berikut sesuai permintaan:

- Jalankan Sysprep dan matikan instans sehingga Anda dapat membuat AMI darinya. Untuk informasi selengkapnya, lihat Buat Amazon EC2 AMI menggunakan Windows Sysprep.

EC2File pengaturan Config

File pengaturan mengontrol pengoperasian layanan EC2 Config. File-file ini terletak di direktori `C:\Program Files\Amazon\Ec2ConfigService\Settings`:

- `ActivationSettings.xml`—Mengontrol aktivasi produk menggunakan server manajemen kunci (AWS KMS).

- `AWS.EC2.Windows.CloudWatch.json`—Mengontrol penghitung kinerja mana yang akan dikirim CloudWatch dan log mana yang akan dikirim ke CloudWatch Log.
- `BundleConfig.xml`—Mengontrol cara EC2 Config menyiapkan instance yang didukung penyimpanan instance untuk pembuatan AMI.
- `Config.xml`—Mengontrol pengaturan utama.
- `DriveLetterConfig.xml`—Mengontrol pemetaan huruf drive.
- `EventLogConfig.xml`—Mengontrol informasi log peristiwa yang ditampilkan di konsol saat instans sedang booting.
- `WallpaperSettings.xml`—Mengontrol informasi yang ditampilkan di latar belakang desktop.

ActivationSettings.xml

File ini berisi pengaturan yang mengontrol aktivasi produk. Ketika Windows boot, layanan EC2 Config memeriksa apakah Windows sudah diaktifkan. Jika Windows belum diaktifkan, maka Windows mencoba mengaktifkan Windows dengan mencari server AWS KMS yang ditentukan.

- `SetAutodiscover`—Menunjukkan apakah akan mendeteksi AWS KMS secara otomatis.
- `TargetKMSServer`—Menyimpan alamat IP pribadi dari file. AWS KMS AWS KMS harus berada di Wilayah yang sama dengan instans Anda.
- `DiscoverFromZone`—Menemukan AWS KMS server dari zona DNS yang ditentukan.
- `ReadFromUserData`Mendapatkan AWS KMS server dari UserData.
- `LegacySearchZones`—Menemukan AWS KMS server dari zona DNS yang ditentukan.
- `DoActivate`—Mencoba aktivasi menggunakan pengaturan tertentu di bagian. Nilai ini bisa jadi `true` atau `false`.
- `LogResultToConsole`—Menampilkan hasil ke konsol.

BundleConfig.xml

File ini berisi pengaturan yang mengontrol cara EC2 Config menyiapkan instance untuk pembuatan AMI.

- `AutoSysprep`—Menunjukkan apakah akan menggunakan Sysprep secara otomatis. Ubah nilainya menjadi `Yes` untuk menggunakan Sysprep.

- `SetRDPCertificate`—Mengatur sertifikat yang ditandatangani sendiri ke server Remote Desktop. Ini memungkinkan Anda untuk melakukan RDP dengan aman ke dalam instans. Ubah nilainya menjadi `Yes` jika instans baru harus memiliki sertifikat.

  Pengaturan ini tidak digunakan untuk contoh dengan versi sistem operasi sebelum Windows Server 2016, karena mereka dapat menghasilkan sertifikat mereka sendiri.
- `SetPasswordAfterSysprep`—Mengatur kata sandi acak pada instans yang baru diluncurkan, mengenkripsinya dengan kunci peluncuran pengguna, dan menghasilkan kata sandi terenkripsi ke konsol. Ubah nilai pengaturan ini ke `No` jika instans baru tidak boleh diatur ke kata sandi terenkripsi acak.

Config.xml

Plug-in

- `Ec2SetPassword`—Membuat sandi terenkripsi acak setiap kali Anda meluncurkan sebuah instans. Fitur ini dinonaktifkan secara default setelah peluncuran pertama sehingga reboot instans ini tidak mengubah sandi yang ditetapkan oleh pengguna. Ubah pengaturan ini menjadi `Enabled` untuk terus menghasilkan sandi setiap kali Anda meluncurkan sebuah instans.

  Pengaturan ini penting jika Anda berencana membuat AMI dari instans Anda.
- `Ec2SetComputerName`—Mengatur nama host instans menjadi nama unik berdasarkan alamat IP instans dan melakukan boot ulang instans. Untuk mengatur nama host Anda sendiri, atau mencegah perubahan nama host yang ada, jangan aktifkan pengaturan ini.
- `Ec2InitializeDrives`—Menginisialisasi dan memformat semua volume selama startup. Fitur ini diaktifkan secara default.
- `Ec2EventLog`—Menampilkan entri log peristiwa di konsol. Secara default, tiga entri kesalahan terbaru dari log aktivitas sistem akan ditampilkan. Untuk menentukan entri log peristiwa yang akan ditampilkan, edit file `EventLogConfig.xml` yang terletak di direktori `EC2ConfigService\Settings`. Untuk informasi tentang pengaturan dalam file ini, lihat Kunci Eventlog.
- `Ec2ConfigureRDP`—Menyiapkan sertifikat yang ditandatangani sendiri di instans, sehingga pengguna dapat mengakses instans dengan aman menggunakan Remote Desktop. Pengaturan ini tidak digunakan untuk contoh dengan versi sistem operasi sebelum Windows Server 2016, karena mereka dapat menghasilkan sertifikat mereka sendiri.
- `Ec2OutputRDPCert`—Menampilkan informasi sertifikat Remote Desktop ke konsol, sehingga pengguna dapat memverifikasinya dengan sidik jari.

- `Ec2SetDriveLetter`—Mengatur huruf drive dari volume yang terpasang berdasarkan pengaturan yang ditentukan pengguna. Secara default, ketika dilampirkan ke sebuah instans, volume Amazon EBS dapat dipasang menggunakan huruf drive pada instans tersebut. Untuk menentukan pemetaan huruf drive Anda, edit file `DriveLetterConfig.xml` yang terletak di direktori `EC2ConfigService\Settings`.
- `Ec2WindowsActivate`—Plug-in menangani aktivasi Windows. Ia memeriksa untuk melihat apakah Windows diaktifkan. Jika tidak, itu memperbarui pengaturan AWS KMS klien, dan kemudian mengaktifkan Windows.

  Untuk mengubah AWS KMS pengaturan, edit `ActivationSettings.xml` file yang terletak di `EC2ConfigService\Settings` direktori.
- `Ec2DynamicBootVolumeSize`—Memperluas Disk 0/Volume 0 untuk menyertakan ruang yang tidak dipartisi.
- `Ec2HandleUserData`—Membuat dan menjalankan skrip yang dibuat oleh pengguna pada peluncuran pertama instans setelah Sysprep dijalankan. Perintah yang dibungkus dalam tag skrip disimpan ke file batch, dan perintah yang dibungkus PowerShell tag disimpan ke file.ps1 (sesuai dengan kotak centang Data Pengguna pada dialog sistem Properti Layanan Ec2).
- `Ec2ElasticGpuSetup`—Memasang paket perangkat lunak Elastic GPU jika instans dikaitkan dengan GPU elastis.
- `Ec2FeatureLogging`—Mengirimkan instalasi fitur Windows dan status layanan yang sesuai ke konsol. Hanya didukung untuk fitur Microsoft Hyper-V dan layanan vmms yang sesuai.

Pengaturan Global

- `ManageShutdown`Memastikan instans yang diluncurkan dari Amazon S3 yang didukung AMIs tidak berakhir saat menjalankan Sysprep.
- `SetDnsSuffixList`—Mengatur sufiks DNS adaptor jaringan untuk Amazon EC2. Hal ini memungkinkan resolusi DNS server yang berjalan di Amazon EC2 tanpa memberikan nama domain yang sepenuhnya memenuhi syarat.

> **Note**
>
> Ini menambahkan pencarian akhiran DNS untuk domain berikut dan mengkonfigurasi sufiks standar lainnya. Untuk informasi selengkapnya tentang cara agen peluncuran menyetel sufiks DNS, lihat. Konfigurasikan DNS Suffix untuk agen peluncuran EC2 Windows

```
region.ec2-utilities.amazonaws.com
```

- `WaitForMetaDataAvailable`Memastikan bahwa layanan EC2 Config akan menunggu metadata dapat diakses dan jaringan tersedia sebelum melanjutkan boot. Pemeriksaan ini memastikan bahwa EC2 Config dapat memperoleh informasi dari metadata untuk aktivasi dan plug-in lainnya.
- `ShouldAddRoutes`—Menambahkan rute khusus ke adaptor jaringan utama untuk mengaktifkan alamat IP berikut saat beberapa NICs terpasang: 169.254.169.250, 169.254.169.251, dan 169.254.169.254. Alamat ini digunakan oleh Windows Activation dan ketika Anda mengakses metadata instans.
- `RemoveCredentialsfromSyspreponStartup`—Menghapus kata sandi administrator dari `Sysprep.xml` saat layanan dimulai lagi. Untuk memastikan bahwa kata sandi ini tetap ada, edit pengaturan ini.

DriveLetterConfig.xml

File ini berisi pengaturan yang mengontrol pemetaan huruf drive. Secara default, volume dapat dipetakan ke huruf drive yang tersedia. Anda dapat memasang volume ke huruf drive tertentu sebagai berikut.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName`—Label volume. Sebagai conto,*`My Volume`* Untuk menentukan pemetaan untuk volume penyimpanan instans, gunakan label `Temporary Storage X`, di mana `X` adalah angka dari 0 sampai 25.
- `DriveLetter`—Huruf drive. Sebagai conto,*`M:`* Pemetaan gagal jika huruf drive sudah digunakan.

EventLogConfig.xml

File ini berisi pengaturan yang mengontrol informasi log peristiwa yang ditampilkan di konsol saat instans sedang di-boot. Secara default, kami menampilkan tiga entri kesalahan terbaru dari log peristiwa Sistem.

- `Category`—Kunci log peristiwa yang akan dipantau.
- `ErrorType`—Tipe peristiwa (misalnya, `Error`, `Warning`, `Information`)
- `NumEntries`—Jumlah peristiwa yang disimpan untuk kategori ini.
- `LastMessageTime`—Untuk mencegah pesan yang sama didorong berulang kali, layanan memperbarui nilai ini setiap kali mendorong suatu pesan.
- `AppName`—Sumber peristiwa atau aplikasi yang mencatat peristiwa tersebut.

WallpaperSettings.xml

File ini berisi pengaturan yang mengontrol informasi yang ditampilkan di latar belakang desktop. Informasi berikut ini ditampilkan secara default.

- `Hostname`—Menampilkan nama komputer.
- `Instance ID`—Menampilkan ID instans.
- `Public IP Address`—Menampilkan alamat IP publik instans.
- `Private IP Address`—Menampilkan alamat IP privat instans.
- `Availability Zone`—Menampilkan Zona Ketersediaan tempat instans berjalan.
- `Instance Size`—Menampilkan tipe instans.
- `Architecture`—Menampilkan pengaturan variabel lingkungan `PROCESSOR_ARCHITECTURE`.

Anda dapat menghapus informasi apa pun yang ditampilkan secara default dengan menghapus entrinya. Anda dapat menambahkan metadata instans tambahan untuk ditampilkan sebagai berikut.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

Anda dapat menambahkan variabel lingkungan Sistem tambahan untuk ditampilkan sebagai berikut.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

File ini berisi pengaturan yang mengontrol cara EC2 Config menginisialisasi drive.

Secara default, EC2 Config menginisialisasi drive yang tidak dibawa online dengan sistem operasi. Anda dapat menyesuaikan plugin sebagai berikut.

```
<InitializeDrivesSettings>
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Gunakan grup pengaturan untuk menentukan cara Anda ingin memulai drive:

FormatWithMEMANGKAS

Mengaktifkan perintah TRIM saat memformat drive. Setelah drive diformat dan diinisialisasi, sistem mengembalikan konfigurasi TRIM.

Dimulai dengan EC2 Config versi 3.18, perintah TRIM dinonaktifkan selama operasi format disk secara default. Ini meningkatkan waktu pemformatan. Gunakan pengaturan ini untuk mengaktifkan TRIM selama operasi format disk untuk EC2 Config versi 3.18 dan yang lebih baru.

FormatWithoutMEMANGKAS

Menonaktifkan perintah TRIM saat memformat drive dan meningkatkan waktu pemformatan di Windows. Setelah drive diformat dan diinisialisasi, sistem mengembalikan konfigurasi TRIM.

DisableInitializeDrives

Menonaktifkan pemformatan untuk drive baru. Gunakan pengaturan ini untuk memulai drive secara manual.

Instal EC2 Config versi terbaru

> **Note**
>
> Agen peluncuran terbaru untuk Windows Server 2022 dan versi sistem operasi yang lebih baru adalah EC2Launch v2, yang menggantikan EC2 Config EC2 dan Launch. EC2Peluncuran v2 sudah diinstal sebelumnya pada AWS Windows Server 2022 dan 2025 AMIs. Anda juga dapat menginstal dan mengonfigurasi agen secara manual di Windows Server 2016 dan 2019. Untuk informasi selengkapnya, lihat Instal EC2 Launch v2.

Untuk informasi tentang cara menerima notifikasi untuk pembaruan EC2 Config, lihat. Berlangganan pemberitahuan agen peluncuran EC2 Windows Untuk informasi tentang perubahan di setiap versi, lihat EC2riwayat versi Config.

Sebelum Anda mulai

- Verifikasi bahwa Anda memiliki.NET framework 3.5 SP1 atau lebih tinggi.
- Secara default, Setup menggantikan file pengaturan Anda dengan file pengaturan default selama instalasi dan memulai ulang layanan EC2 Config ketika instalasi selesai. Jika Anda mengubah pengaturan layanan EC2 Config, salin `config.xml` file dari direktori. `%Program Files%\Amazon\Ec2ConfigService\Settings` Setelah memperbarui layanan EC2 Config, Anda dapat memulihkan file ini untuk mempertahankan perubahan konfigurasi Anda.

Verifikasi EC2 versi Config

Gunakan prosedur berikut untuk memverifikasi versi EC2 Config yang diinstal pada instans Anda.

Untuk memverifikasi versi EC2 Config yang diinstal

1. Luncurkan sebuah instans dari AMI dan hubungkan diri Anda dengan instans tersebut.
2. Di Panel Kontrol, pilih Program dan Fitur.
3. Dalam daftar program yang diinstal, cari `Ec2ConfigService`. Nomor versinya muncul di kolom Versi.

Perbarui EC2 Config

Gunakan prosedur berikut untuk mengunduh dan menginstal EC2 Config versi terbaru pada instans Anda.

Untuk mengunduh dan menginstal EC2 Config versi terbaru

1. Unduh dan unzip installer EC2Config.
2. Jalankan `EC2Install.exe`. Untuk daftar lengkap opsi, jalankan `EC2Install` dengan opsi `/?`. Secara default, penyiapan menampilkan perintah. Untuk menjalankan perintah tanpa prompt, gunakan opsi `/quiet`.

   > **Important**
   >
   > Untuk menjaga pengaturan kustom dari `config.xml` file yang Anda simpan, jalankan `EC2Install` dengan `/norestart` opsi, pulihkan pengaturan Anda, lalu mulai ulang layanan EC2 Config secara manual.

3. Jika Anda menjalankan EC2 Config versi 4.0 atau yang lebih baru, Anda harus memulai ulang Agen SSM pada instance dari snap-in Microsoft Services.

   > **Note**
   >
   > Informasi versi EC2 Config yang diperbarui tidak akan muncul di Log Sistem instans atau pemeriksaan Trusted Advisor sampai Anda reboot atau berhenti dan memulai instance Anda.

Untuk mengunduh dan menginstal EC2 Config versi terbaru menggunakan PowerShell

Untuk mengunduh, membuka zip, dan menginstal versi terbaru EC2 Config PowerShell menggunakan, jalankan perintah berikut dari PowerShell jendela:

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
```

```
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016 atau sebelumnya, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifikasi instalasi dengan memeriksa `C:\Program Files\Amazon\` untuk direktori `Ec2ConfigService`.

Konfigurasikan setelan proksi .NET untuk EC2 layanan Config

Anda dapat mengonfigurasi layanan EC2 Config untuk berkomunikasi melalui proxy menggunakan salah satu metode berikut: AWS SDK for .NET, elemen`system.net`, atau Kebijakan Grup Microsoft dan Internet Explorer. Menggunakan AWS SDK for .NET adalah metode yang disukai karena Anda dapat menentukan kredensyal login.

Metode

- Konfigurasikan pengaturan proxy menggunakan AWS SDK for .NET (Preferred)
- Konfigurasikan pengaturan proxy menggunakan elemen system.net
- Konfigurasikan pengaturan proxy menggunakan Kebijakan Grup Microsoft dan Internet Explorer Microsoft

Konfigurasikan pengaturan proxy menggunakan AWS SDK for .NET (Preferred)

Anda dapat mengonfigurasi pengaturan proxy untuk layanan EC2 Config dengan menentukan `proxy` elemen dalam file. `Ec2Config.exe.config` Untuk informasi selengkapnya, lihat Referensi File Konfigurasi untuk AWS SDK for .NET.

Untuk menentukan elemen proxy di Ec2Config.exe.config

1. Edit `Ec2Config.exe.config` file pada instance di mana Anda ingin layanan EC2 Config berkomunikasi melalui proxy. Secara default, file terletak di direktori berikut: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Tambahkan elemen `aws` berikut ini ke `configSections`. Jangan tambahkan ini ke `sectionGroups` yang ada.

   Untuk EC2 Config versi 3.17 atau yang lebih lama

   ```
   <configSections>
      <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
   </configSections>
   ```

   Untuk EC2 Config versi 3.18 atau yang lebih baru

   ```
   <configSections>
        <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
   </configSections>
   ```
3. Tambahkan elemen `aws` berikut ini ke file `Ec2Config.exe.config`.

   ```
   <aws>
      <proxy
        host="string value"
        port="string value"
        username="string value"
        password="string value" />
   </aws>
   ```
4. Simpan perubahan Anda.

Konfigurasikan pengaturan proxy menggunakan elemen system.net

Anda dapat menentukan pengaturan proxy di elemen `system.net` di file `Ec2Config.exe.config`. Untuk informasi selengkapnya, lihat elemen DefaultProxy (pengaturan jaringan).

Untuk menentukan elemen system.net di Ec2Config.exe.config

1. Edit `Ec2Config.exe.config` file pada instance di mana Anda ingin layanan EC2 Config berkomunikasi melalui proxy. Secara default, file terletak di direktori berikut: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Tambahkan entri `defaultProxy` ke `system.net`. Untuk informasi selengkapnya, lihat elemen DefaultProxy (pengaturan jaringan).

   Misalnya, konfigurasi berikut merutekan semua lalu lintas untuk menggunakan proxy yang saat ini dikonfigurasi untuk Internet Explorer, dengan pengecualian lalu lintas metadata dan lisensi, yang akan melewati proxy.

   ```
   <defaultProxy>
       <proxy usesystemdefault="true" />
       <bypasslist>
           <add address="169.254.169.250" />
           <add address="169.254.169.251" />
           <add address="169.254.169.254" />
           <add address="[fd00:ec2::250]" />
           <add address="[fd00:ec2::254]" />
       </bypasslist>
   </defaultProxy>
   ```
3. Simpan perubahan Anda.

Konfigurasikan pengaturan proxy menggunakan Kebijakan Grup Microsoft dan Internet Explorer Microsoft

Layanan EC2 Config berjalan di bawah akun pengguna Sistem Lokal. Anda dapat menentukan pengaturan proksi seluruh instans untuk akun ini di Internet Explorer setelah Anda mengubah pengaturan Kebijakan Grup pada instans.

Untuk mengonfigurasi pengaturan proxy menggunakan Kebijakan Grup dan Internet Explorer

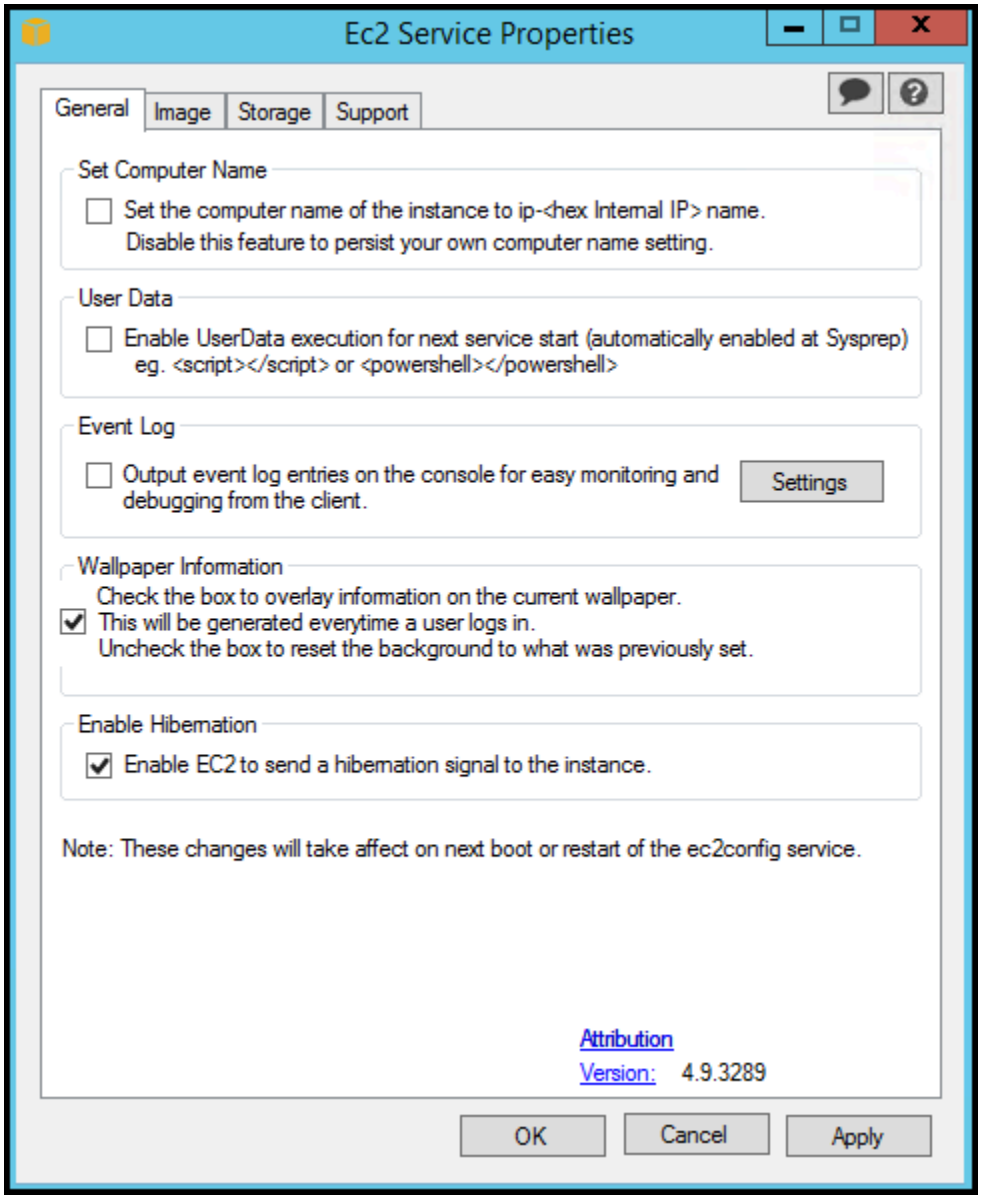
1. Pada instance di mana Anda ingin layanan EC2 Config berkomunikasi melalui proxy, buka Command prompt sebagai Administrator, ketik**`gpedit.msc`**, dan tekan Enter.
2. Di Editor Kebijakan Grup Lokal, di bawah Kebijakan Komputer Lokal, pilih Konfigurasi Komputer, Templat Administratif, Komponen Windows, Internet Explorer.

3. Di panel kanan, pilih Buat pengaturan proxy per mesin (bukan per pengguna) lalu pilih Edit pengaturan kebijakan.
4. Pilih Diaktifkan, lalu pilih Terapkan.
5. Buka Internet Explorer, lalu pilih tombol Alat.
6. Pilih Opsi Internet, lalu pilih tab Koneksi.
7. Pilih Pengaturan LAN.
8. Di bawah Server proxy, pilih opsi Gunakan server proxy untuk LAN Anda.
9. Tentukan alamat dan informasi port lalu pilih OK.

Setel properti layanan EC2config dari dialog sistem pada instans Windows EC2 Anda

Prosedur berikut menjelaskan cara menggunakan dialog sistem Properti Layanan EC2 untuk mengaktifkan atau menonaktifkan pengaturan.

1. Jalankan dan hubungkan ke instans Windows Anda.
2. Dari menu Start , klik All Programs , lalu klik EC2ConfigServicePengaturan .



3. Pada tab Umum dari dialog sistem Properti Layanan EC2, Anda dapat mengaktifkan atau menonaktifkan pengaturan berikut.

   Atur Nama Komputer

   Jika pengaturan ini diaktifkan (dinonaktifkan secara default), nama host dibandingkan dengan alamat IP internal saat ini di setiap boot; jika nama host dan alamat IP internal tidak cocok, nama host disetel ulang untuk memuat alamat IP internal dan kemudian sistem melakukan boot ulang untuk mengambil nama host baru. Untuk mengatur nama host Anda sendiri, atau untuk mencegah perubahan nama host yang ada, jangan aktifkan pengaturan ini.

Data Pengguna

Eksekusi data pengguna memungkinkan Anda menentukan skrip dalam metadata instans. Secara default, skrip ini berjalan selama peluncuran awal. Anda juga dapat mengonfigurasinya untuk dijalankan saat Anda melakukan boot ulang atau memulai instans, atau setiap kali Anda melakukan boot ulang atau memulai instans.

Jika Anda memiliki skrip yang besar, kami menyarankan agar Anda menggunakan data pengguna untuk mengunduh skrip, dan kemudian menjalankannya.

Untuk informasi selengkapnya, lihat Eksekusi data pengguna.

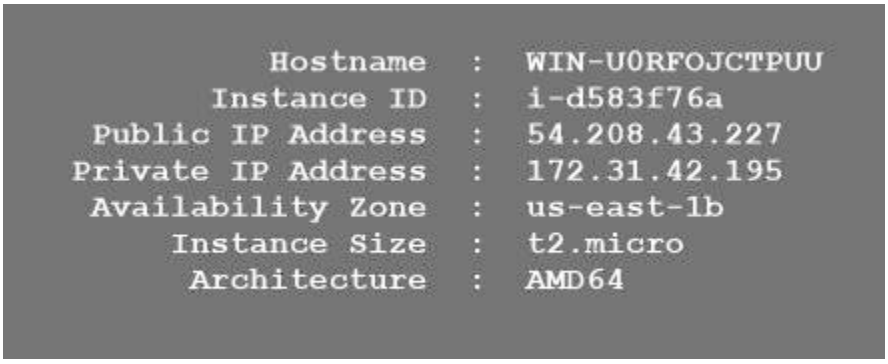
Log Peristiwa

Gunakan pengaturan ini untuk menampilkan entri log peristiwa di konsol selama boot untuk memudahkan pemantauan dan debugging.

Klik Pengaturan untuk menentukan filter untuk entri log yang dikirim ke konsol. Filter default mengirimkan tiga entri kesalahan terbaru dari log peristiwa sistem ke konsol.

Informasi Wallpaper

Gunakan pengaturan ini untuk menampilkan informasi sistem di latar belakang desktop. Berikut ini adalah contoh informasi yang ditampilkan di latar belakang desktop.

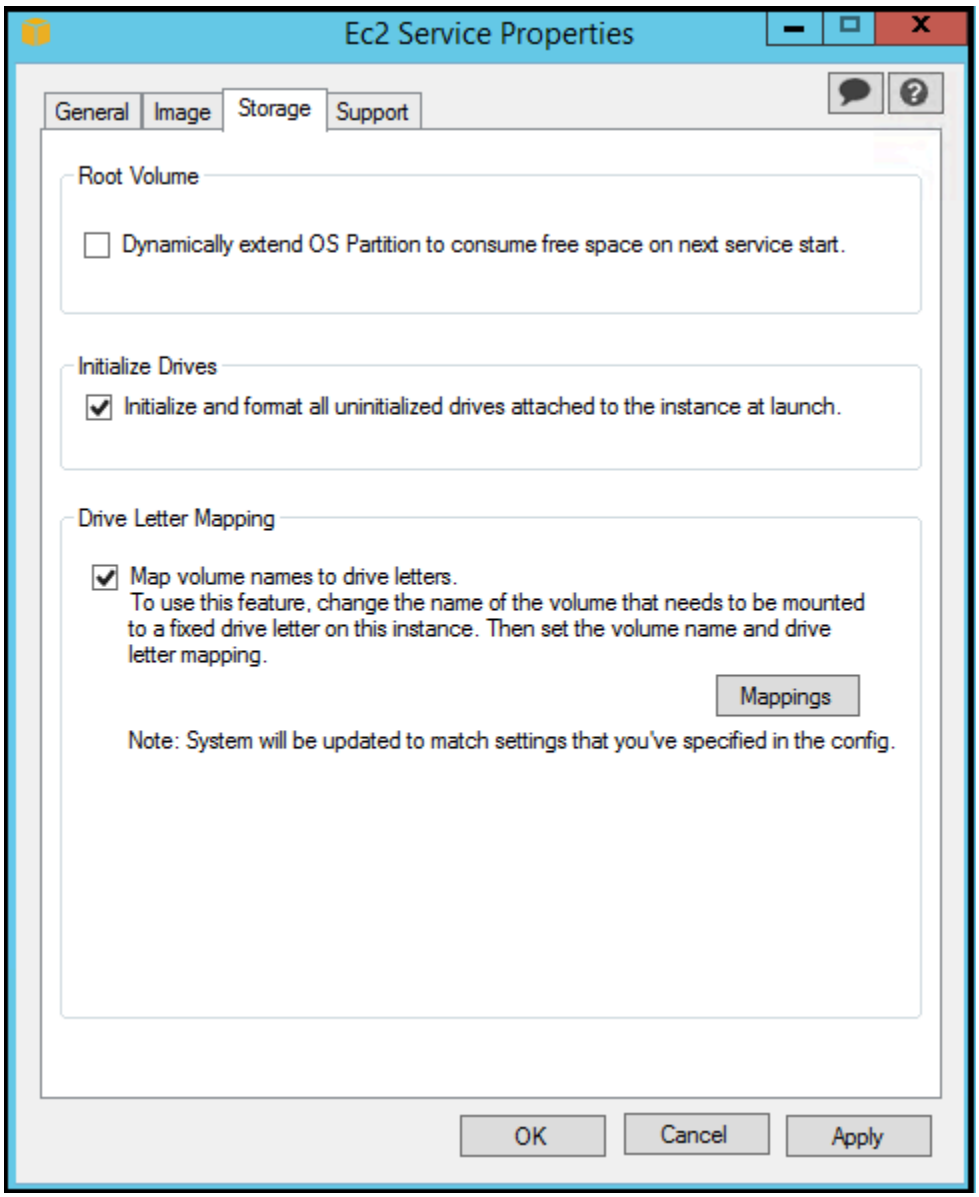


Informasi yang ditampilkan di latar belakang desktop dikontrol oleh file pengaturan `EC2ConfigService\Settings\WallpaperSettings.xml`.

Aktifkan Hibernasi

Gunakan pengaturan ini untuk memungkinkan EC2 memberi sinyal pada sistem operasi untuk melakukan hibernasi.

4. Klik tab Penyimpanan. Anda dapat mengaktifkan atau menonaktifkan pengaturan berikut.



Volume root

Pengaturan ini secara dinamis memperluas Disk 0/Volume 0 untuk menyertakan ruang yang tidak dipartisi. Ini dapat berguna ketika instance di-boot dari volume root yang memiliki ukuran khusus.

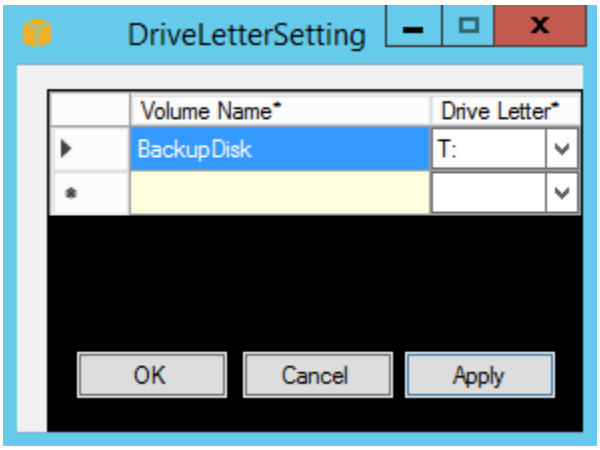
Inisialisasi Drive

Pengaturan ini memformat dan memasang semua volume yang terpasang ke instans selama memulai.

Pemetaan Huruf Drive

Sistem memetakan volume yang dilampirkan ke sebuah instans ke huruf drive. Untuk volume Amazon EBS, default-nya adalah menetapkan huruf drive dari D: ke Z:. Misalnya volume toko, defaultnya tergantung pada driver. AWS Driver PV dan driver Citrix PV menetapkan volume penyimpanan instance huruf drive dari Z: ke A:. Driver Red Hat menetapkan volume penyimpanan instans huruf drive dari D: ke Z:.

Untuk memilih huruf drive untuk volume Anda, klik Pemetaan. DalamDriveLetterSetting kotak dialog, tentukan nilai Volume Name dan Drive Letter untuk setiap volume, klik Apply , lalu klik OK . Kami menganjurkan agar Anda memilih huruf drive yang menghindari konflik dengan huruf drive yang mungkin digunakan, seperti huruf drive di tengah alfabet.



Setelah Anda menentukan pemetaan huruf drive dan melampirkan volume dengan label yang sama dengan salah satu nama volume yang Anda tentukan, EC2 Config secara otomatis menetapkan huruf drive yang Anda tentukan ke volume tersebut. Namun, pemetaan huruf kandar gagal jika huruf kandar sudah digunakan. Perhatikan bahwa EC2 Config tidak mengubah huruf drive volume yang sudah dipasang saat Anda menentukan pemetaan huruf drive.

5. Untuk menyimpan pengaturan Anda dan terus mengerjakannya nanti, klik OK untuk menutup dialog sistem Properti Layanan EC2. Jika Anda telah selesai menyesuaikan instans Anda dan ingin membuat AMI dari instans itu, lihat Buat Amazon EC2 AMI menggunakan Windows Sysprep.

Memecahkan masalah dengan agen peluncuran Config EC2

Informasi berikut dapat membantu Anda memecahkan masalah dengan layanan Config EC2.

Perbarui EC2 Config pada instance yang tidak dapat dijangkau

Gunakan prosedur berikut untuk memperbarui layanan EC2 Config pada instance Windows Server yang tidak dapat diakses menggunakan Remote Desktop.

Untuk memperbarui EC2 Config pada instans Windows yang didukung Amazon EBS yang tidak dapat Anda sambungkan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Cari instans yang terpengaruh. Pilih instans dan pilih status Instans, lalu pilih Hentikan instans.

   > **Warning**
   >
   > Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instans akan hilang. Untuk menyimpan data ini, buat cadangan ke penyimpanan persisten.

4. Pilih Luncurkan instans dan buat instans `t2.micro` sementara di Zona Ketersediaan yang sama dengan instans yang terpengaruh. Gunakan AMI yang berbeda dari AMI yang Anda gunakan untuk meluncurkan instans yang terpengaruh.

   > **Important**
   >
   > Jika Anda tidak membuat instans di Zona Ketersediaan yang sama dengan instans yang terpengaruh, Anda tidak akan dapat melampirkan volume root dari instans yang terpengaruh ke instans baru.

5. Pada konsol EC2 pilih Volume.
6. Cari volume root dari instans yang terdampak. Lepaskan volume dan Lampirkan volume ke instans sementara yang Anda buat sebelumnya. Lampirkan dengan nama perangkat default (xvdf).
7. Gunakan Remote Desktop untuk terhubung ke instans sementara, dan kemudian gunakan utilitas Disk Management agar volume tersedia untuk digunakan.
8. Unduh versi terbaru dari layanan EC2 Config. Ekstrak file dari file `.zip` ke direktori `Temp` pada drive yang Anda lampirkan.
9. Pada instans sementara, buka kotak dialog Run (Jalankan), ketik, **`regedit`**dan tekan Enter.

10. Pilih HKEY_LOCAL_MACHINE. Dari menu File, pilih Muat Hive. Pilih drive dan kemudian arahkan ke dan buka file berikut: Windows\System32\config\SOFTWARE. Saat diminta, tentukan nama kunci.
11. Pilih kunci yang baru saja Anda muat dan arahkan ke Microsoft\Windows \CurrentVersion. Memilih kunci RunOnce. Jika kunci ini tidak ada, pilih CurrentVersion dari menu konteks (klik kanan), pilih Baru lalu pilih Kunci. Beri nama kunci RunOnce.
12. Dari menu konteks (klik kanan), pilih kunci RunOnce, lalu pilih Baru, lalu pilih Nilai String. Masukkan Ec2Install sebagai nama dan C:\Temp\Ec2Install.exe /quiet sebagai data.
13. MemilihHKEY_LOCAL_MACHINE*specified key name*\Microsoft\Windows NT \CurrentVersion\Winlogon kunci. Dari menu konteks (klik kanan) pilih Baru, lalu pilih Nilai String. Masukkan **AutoAdminLogon** sebagai nama dan **1** sebagai data nilai.
14. Memilih kunci HKEY_LOCAL_MACHINE*specified key name*\Microsoft\Windows NT \CurrentVersion\Winlogon>. Dari menu konteks (klik kanan) pilih Baru, lalu pilih Nilai String. Masukkan **DefaultUserName** sebagai nama dan **Administrator** sebagai data nilai.
15. Memilih kunci HKEY_LOCAL_MACHINE*specified key name*\Microsoft\Windows NT \CurrentVersion\Winlogon. Dari menu konteks (klik kanan) pilih Baru, lalu pilih Nilai String. Ketik **DefaultPassword** sebagai nama dan masukkan kata sandi di data nilai.
16. Di panel navigasi Editor Registri, pilih kunci sementara yang Anda buat saat pertama kali membuka Editor Registri.
17. Dari File pilihan, pilih Pembongkaran Hive.
18. Di Pemanfaatan Manajemen DiskIT, pilih drive yang Anda lampirkan sebelumnya, buka menu konteks (klik kanan), dan pilih Offline.
19. Di konsol Amazon EC2, lepaskan volume yang terpengaruh dari instans sementara dan pasang kembali ke instans Anda dengan nama perangkat /dev/sda1. Anda harus menentukan nama perangkat ini untuk menetapkan volume sebagai volume root.
20. Hentikan dan mulai instans Amazon EC2 instans.
21. Setelah instans dimulai, periksa log sistem dan pastikan bahwa Anda melihat pesan Windows siap digunakan.
22. Buka Penyunting Registri dan pilih HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Hapus kunci String Value yang Anda buat sebelumnya: AutoAdminLogonDefaultUserName,, dan DefaultPassword.
23. Hapus atau hentikan instans sementara yang Anda buat dalam prosedur ini.

EC2riwayat versi Config

Tabel berikut menjelaskan versi EC2 Config yang dirilis. Untuk informasi tentang pembaruan untuk SSM Agent, lihat Catatan Rilis Systems Manager SSM Agent.

> **Important**
>
> EC2Config telah mencapai akhir dukungan. Hanya versi terbaru dari agen EC2 Config yang tersedia untuk diunduh. Versi sebelumnya ditandai sebagai pribadi.

Versi	Detail	Tanggal rilis
4.9.5777	• Memperbaiki masalah di mana konfigurasi RSS disetel secara tidak benar untuk beberapa jenis instance. • Versi baru SSM Agent `3.3.484.0` .	17 Juni 2024
4.9.5554	• Membatasi devolusi nama domain berdasarkan entri registri: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Versi baru SSM Agent `3.2.1630.0` .	4 Oktober 2023
4.9.5467	• Menambahkan kemampuan coba lagi untuk menemukan port konsol. • Versi baru SSM Agent `3.1.2282.0` .	1 Agustus 2023
4.9.5288	• AWS Core SDK yang diperbarui ke versi `3.7.103.23` . • Memperbaiki masalah saat dokumen `AWS-UpdateEC2Config` SSM gagal diperbarui hanya `EC2Config` pada instance yang diaktifkan. IMDSv2 •	8 Maret 2023

Versi	Detail	Tanggal rilis
	Versi baru SSM Agent `3.1.2144.0` .	
4.9.5231	• Versi baru SSM Agent 3.1.1927.0.	14 Februari 2023
4.9.5103	• Memperbaiki masalah di mana volume fana diidentifikasi secara tidak benar pada keluarga instans r5d dan i4i. • Versi baru SSM Agent 3.1.1856.0.	5 Desember 2022
4.9.5064	• Diperbarui untuk menggunakan informasi segmen PCI guna memilih port konsol. • PowerShell Skrip yang ditandatangani dan menambahkan header hak cipta. • Logika pemilihan adaptor jaringan utama tetap. • Versi baru SSM Agent 3.1.1732.0.	16 November 2022
4.9.4588	• Logika tunggu IMDS yang diperbarui untuk hanya membuat IMDSv2 permintaan. • Menambahkan pustaka bersama agen peluncuran libec2launch.dll. • Versi baru SSM Agent 3.1.1188.0.	31 Mei 2022
4.9.4556	• Menambahkan logika tunggu untuk memastikan inisialisasi penuh NIC sebelum digunakan. • Versi baru Log4Net 2.0.14.0 mengambil patch keamanan. • Versi baru SSM Agent 3.1.1045.0 mengambil patch keamanan.	1 Maret 2022

Versi	Detail	Tanggal rilis
4.9.4536	• Memperbaiki masalah saat data pengguna mogok saat folder Temp hilang. • Versi baru SSM Agent 3.1.804.0.	31 Januari 2022
4.9.4508	• Memperbaiki masalah untuk menghitung jalur skrip diskpart dengan benar. • Versi baru SSM Agent 3.1.338.0.	6 Oktober 2021
4.9.4500	• `Install-EgpuManagerConfig` yang diperbarui dengan dukungan IMDS v2. • Tautan web yang diperbarui untuk menggunakan https. • Versi baru SSM Agent 3.1.282.0	7 September 2021
4.9.4419	• Memperbaiki logika fallback IMDS versi 1 • Memperbarui semua penggunaan direktori temp Windows ke direktori temp EC2 Config • Versi baru SSM Agent 3.0.1124.0	2 Juni 2021
4.9.4381	• Ditambahkan dukungan untuk skema dokumen SSM versi 2.2 di EC2 ConfigUpdater • Menambahkan versi paket AWS Nitro Enclave ke log konsol • Versi baru SSM Agent 3.0.529.0	4 Mei 2021
4.9.4326	• Menghapus semua tautan di pengaturan UI • Ini adalah versi EC2 Config terakhir yang mendukung Windows Server 2008.	3 Maret 2021

Versi	Detail	Tanggal rilis
4.9.4279	• Memperbaiki masalah keamanan yang terkait dengan tugas terjadwal `Ec2ConfigMonitor` • Memperbaiki masalah pemetaan huruf drive dan jumlah disk ephemeral yang salah • Menambahkan `OsCurrentBuild` dan `OsReleaseId` ke output konsol • Versi baru SSM Agent 2.3.871.0	11 Desember 2020
4.9.4222	• Memperbaiki logika fallback IMDS versi 1 • Versi baru SSM Agent 2.3.842.0	7 April 2020
4.9.4122	• Menambahkan dukungan untuk IMDS V2 • Versi baru SSM Agent 2.3.814.0	4 Maret 2020
4.9.3865	• Memperbaiki masalah pendeteksian port COM untuk Windows Server 2008 R2 pada instans metal • Versi baru SSM Agent 2.3.722.0	31 Oktober 2019
4.9.3519	• Versi baru SSM Agent 2.3.634.0	18 Juni 2019
4.9.3429	• Versi baru SSM Agent 2.3.542.0	25 April 2019
4.9.3289	• Versi baru 2.3.444.0	11 Februari 2019
4.9.3270	• Menambahkan plugin untuk mengatur monitor agar tidak pernah mati untuk memperbaiki masalah ACPI • Edisi dan versi SQL Server yang ditulis ke konsol • Versi baru SSM Agent 2.3.415.0	22 Januari 2019
4.9.3230	• Deskripsi Pemetaan Huruf Drive yang diperbarui agar lebih selaras dengan fungsionalitas • Versi baru SSM Agent 2.3.372.0	10 Januari 2019

Versi	Detail	Tanggal rilis
4.9.3160	• Peningkatan waktu tunggu untuk NIC utama • Menambahkan konfigurasi default untuk pengaturan RSS dan Menerima Antrean untuk perangkat ENA • Hibernasi dinonaktifkan selama Sysprep • Versi baru SSM Agent 2.3.344.0 • AWS SDK yang ditingkatkan ke 3.3.29.13	15 Desember 2018
4.9.3067	• Perbaikan yang dilakukan pada hibernasi instans • Versi baru SSM Agent 2.3.235.0	8 November 2018
4.9.3034	• Menambahkan rute 169.254.169.253/32 untuk server DNS • Versi baru SSM Agent 2.3.193.0	24 Oktober 2018
4.9.2986	• Menambahkan penandatanganan untuk semua EC2 binari terkait Config • Versi baru SSM Agent 2.3.136.0	11 Oktober 2018
4.9.2953	Versi baru SSM Agent (2.3.117.0)	2 Oktober 2018
4.9.2926	Versi baru SSM Agent (2.3.68.0)	18 September 2018
4.9.2905	• Versi baru SSM Agent (2.3.50.0) • Menambahkan rute 169.254.169.123/32 ke layanan waktu AMZN • Menambahkan rute 169.254.169.249/32 ke layanan lisensi GRID • Memperbaiki masalah yang menyebabkan NVMe volume EBS ditandai sebagai fana	17 September 2018
4.9.2854	Versi baru SSM Agent (2.3.13.0)	17 Agustus 2018

Versi	Detail	Tanggal rilis
4.9.2831	Versi baru SSM Agent (2.2.916.0)	7 Agustus 2018
4.9.2818	Versi baru SSM Agent (2.2.902.0)	31 Juli 2018
4.9.2756	Versi baru SSM Agent (2.2.800.0)	27 Juni 2018
4.9.2688	Versi baru SSM Agent (2.2.607.0)	25 Mei 2018
4.9.2660	Versi baru SSM Agent (2.2.546.0)	11 Mei 2018
4.9.2644	Versi baru SSM Agent (2.2.493.0)	26 April 2018
4.9.2586	Versi baru SSM Agent (2.2.392.0)	28 Maret 2018
4.9.2565	• Versi baru SSM Agent (2.2.355.0) • Memperbaiki masalah pada instans M5 dan C5 (tidak dapat menemukan driver PV) • Tambahkan pencatatan konsol untuk jenis instans, driver PV terbaru, dan NVMe driver	13 Maret 2018
4.9.2549	Versi baru SSM Agent (2.2.325.0)	8 Maret 2018
4.9.2461	Versi baru SSM Agent (2.2.257.0)	15 Februari 2018
4.9.2439	Versi baru SSM Agent (2.2.191.0)	6 Februari 2018
4.9.2400	Versi baru SSM Agent (2.2.160.0)	16 Januari 2018

Versi	Detail	Tanggal rilis
4.9.2327	• Versi baru SSM Agent (2.2.120.0) • Penambahan penemuan port COM pada instans bare metal Amazon EC2 • Penambahan logging status Hyper-V pada instans bare metal Amazon EC2	2 Januari 2018
4.9.2294	Versi baru SSM Agent (2.2.103.0)	4 Desember 2017
4.9.2262	Versi baru SSM Agent (2.2.93.0)	15 November 2017
4.9.2246	Versi baru SSM Agent (2.2.82.0)	11 November 2017
4.9.2218	Versi baru SSM Agent (2.2.64.0)	29 Oktober 2017
4.9.2212	Versi baru SSM Agent (2.2.58.0)	23 Oktober 2017
4.9.2203	Versi baru SSM Agent (2.2.45.0)	19 Oktober 2017
4.9.2188	Versi baru SSM Agent (2.2.30.0)	10 Oktober 2017
4.9.2180	• Versi baru SSM Agent (2.2.24.0) • Menambahkan plugin Elastic GPU untuk instans GPU	5 Oktober 2017
4.9.2143	Versi baru SSM Agent (2.2.16.0)	1 Oktober 2017
4.9.2140	Versi baru SSM Agent (2.1.10.0)	
4.9.2130	Versi baru SSM Agent (2.1.4.0)	

Versi	Detail	Tanggal rilis
4.9.2106	Versi baru SSM Agent (2.0.952.0)	
4.9.2061	Versi baru SSM Agent (2.0.922.0)	
4.9.2047	Versi baru SSM Agent (2.0.913.0)	
4.9.2031	Versi baru SSM Agent (2.0.902.0)	
4.9.2016	• Versi baru SSM Agent (2.0.879.0) • Memperbaiki jalur direktori CloudWatch Log untuk Windows Server 2003	
4.9.1981	• Versi baru SSM Agent (2.0.847.0) • Memperbaiki masalah dengan pembuatan `important.txt` sedang di volume EBS.	
4.9.1964	Versi baru SSM Agent (2.0.842.0)	
4.9.1951	• Versi baru SSM Agent (2.0.834.0) • Memperbaiki masalah huruf drive yang tidak dipetakan dari Z: untuk drive singkat.	
4.9.1925	• Versi baru SSM Agent (2.0.822.0) • [Bug] Versi ini bukan target pembaruan yang valid dari SSM Agent v4.9.1775.	
4.9.1900	Versi baru SSM Agent (2.0.805.0)	

Versi	Detail	Tanggal rilis
4.9.1876	• Versi baru SSM Agent (2.0.796.0) • Memperbaiki masalah dengan output/error pengalihan untuk eksekusi data pengguna admin.	
4.9.1863	• Versi baru SSM Agent (2.0.790.0) • Memperbaiki masalah terkait pemasangan beberapa volume EBS ke instans Amazon EC2. • Ditingkatkan CloudWatch untuk mengambil jalur konfigurasi, menjaga kompatibilitas mundur.	
4.9.1791	Versi baru SSM Agent (2.0.767.0)	
4.9.1775	Versi baru SSM Agent (2.0.761.0)	
4.9.1752	Versi baru SSM Agent (2.0.755.0)	
4.9.1711	Versi baru SSM Agent (2.0.730.0)	
4.8.1676	Versi baru SSM Agent (2.0.716.0)	
4.7.1631	Versi baru SSM Agent (2.0.682.0)	
4.6.1579	• Versi baru SSM Agent (2.0.672.0) • Memperbaiki masalah pembaruan agen dengan v4.3, v4.4, dan v4.5	
4.5.1534	Versi baru SSM Agent (2.0.645.1)	
4.4.1503	Versi baru SSM Agent (2.0.633.0)	
4.3.1472	Versi baru SSM Agent (2.0.617.1)	

Versi	Detail	Tanggal rilis
4.2.1442	Versi baru SSM Agent (2.0.599.0)	
4.1.1378	Versi baru SSM Agent (2.0.558.0)	
4.0.1343	• Run Command, State Manager, CloudWatch agen, dan dukungan domain join telah dipindahkan ke agen lain yang disebut SSM Agent. Agen SSM akan diinstal sebagai bagian dari upgrade EC2 Config. Untuk informasi selengkapnya, lihat EC2Config dan AWS Systems Manager. • Jika Anda memiliki proxy yang disiapkan di EC2 Config, Anda perlu memperbarui pengaturan proxy untuk Agen SSM sebelum memutakhirkan. Jika Anda tidak memperbar ui pengaturan proxy, Anda tidak akan dapat menggunak an Jalankan Perintah untuk mengelola instans Anda. Untuk menghindari hal ini, lihat informasi berikut sebelum memperbarui ke versi yang lebih baru: Menginstal dan Mengonfigurasi SSM Agent pada Instans Windows di Panduan Pengguna AWS Systems Manager . • Jika sebelumnya Anda mengaktifkan CloudWatch integrasi pada instance Anda dengan menggunakan file konfigurasi lokal (`AWS.EC2.Windows.CloudWatch.json`), Anda harus mengonfigurasi file agar berfungsi dengan Agen SSM.	
3.19.1153	• Plugin aktivasi yang diaktifkan kembali untuk instance dengan konfigurasi lama AWS KMS . Lewati aktivasi untuk pengguna BYOL. • Ubah perilaku TRIM default untuk dinonaktifkan selama operasi format disk dan tambahkan FormatWith TRIM untuk mengganti InitializeDisks plugin dengan data pengguna.	

Versi	Detail	Tanggal rilis
3.18.1118	• Perbaiki untuk menambahkan rute dengan andal ke adaptor jaringan utama. • Pembaruan untuk meningkatkan dukungan untuk AWS layanan.	
3.17.1032	• Memperbaiki log sistem duplikat yang muncul saat filter disetel ke kategori yang sama. • Perbaikan untuk mencegah hang selama inisialisasi disk.	
3.16.930	Menambahkan dukungan ke log peristiwa "Jendela Siap digunakan" ke Log Peristiwa Windows saat dimulai.	
3.15.880	Perbaikan untuk mengizinkan pengunggahan keluaran System Manager Run Command ke nama bucket S3 dengan '.' karakter.	
3.14.786	Menambahkan dukungan untuk mengganti pengaturan Initializ eDisks plugin. Contoh: Untuk mempercepat inisialisasi disk SSD, Anda dapat menonaktifkan TRIM untuk sementara dengan menentukan ini di userdata: < InitializeDrivesSettings >< > FormatWithout SettingsGroup TRIM SettingsGroup </ ></ InitializeDrivesSettings	
3.13.727	System Manager Run Command - Perbaikan untuk memproses perintah dengan andal setelah windows reboot.	

Versi	Detail	Tanggal rilis
3.12.649	• Perbaikan untuk menangani booting ulang dengan baik saat menjalankan perintah/skrip. • Perbaiki untuk membatalkan perintah yang berjalan dengan andal. • Tambahkan dukungan untuk (secara opsional) mengungga h log MSI ke S3 saat menginstal aplikasi melalui Systems Manager Run Command.	
3.11.521	• Perbaikan untuk mengaktifkan pembuatan sidik jari RDP untuk Windows Server 2003. • Perbaikan untuk menyertakan zona waktu dan offset UTC di baris log Config EC2. • Dukungan Systems Manager untuk menjalankan perintah Run Command secara paralel. • Kembalikan perubahan sebelumnya untuk menghadirkan disk yang dipartisi secara online.	
3.10.442	• Memperbaiki kegagalan konfigurasi Systems Manager saat menginstal aplikasi MSI. • Perbaiki untuk menghadirkan disk penyimpanan online dengan andal. • Pembaruan untuk meningkatkan dukungan untuk AWS layanan.	

Versi	Detail	Tanggal rilis
3.9.359	• Perbaiki dalam skrip pasca Sysprep untuk membiarkan konfigurasi pembaruan windows dalam status default. • Perbaiki plugin pembuat kata sandi untuk meningkatkan keandalan dalam mendapatkan pengaturan kebijakan kata sandi GPO. • Batasi izin folder log EC2 konfigurasi/SSM ke grup Administrator lokal. • Pembaruan untuk meningkatkan dukungan untuk AWS layanan.	
3.8.294	• Memperbaiki masalah CloudWatch yang mencegah log diunggah saat tidak di drive utama. • Meningkatkan proses inisialisasi disk dengan menambahkan logika coba lagi. • Menambahkan penanganan kesalahan yang ditingkatkan saat SetPassword plugin terkadang gagal selama pembuatan AMI. • Pembaruan untuk meningkatkan dukungan untuk AWS layanan.	

Versi	Detail	Tanggal rilis
3.7.308	• Perbaikan pada utilitas ec2config-cli untuk pengujian konfigurasi dan pemecahan masalah dalam instans. • Hindari menambahkan rute statis untuk AWS KMS dan layanan meta-data pada adaptor OpenVPN. • Memperbaiki masalah ketika eksekusi data pengguna tidak mematuhi tag "persisten". • Penanganan kesalahan yang lebih baik saat masuk ke konsol EC2 tidak tersedia. • Pembaruan untuk meningkatkan dukungan untuk AWS layanan.	
3.6.269	• Perbaikan keandalan aktivasi Windows untuk pertama kali menggunakan alamat lokal tautan 169.254.0.250/251 untuk mengaktifkan windows melalui AWS KMS • Penanganan proxy yang lebih baik untuk skenario Systems Manager, Aktivasi Windows, dan Penggabungan Domain • Memperbaiki masalah di mana baris duplikat akun pengguna ditambahkan ke file jawaban Sysprep	
3.5.228	• Mengatasi skenario di mana CloudWatch plugin dapat mengkonsumsi CPU yang berlebihan dan membaca memori Windows Event Logs • Menambahkan link ke dokumentasi CloudWatch konfigurasi di EC2 Config Settings UI	

Versi	Detail	Tanggal rilis
3.4.212	• Perbaikan ke EC2 Config saat digunakan dalam kombinasi dengan VM-Import. • Memperbaiki masalah penamaan layanan di pemasang WiX.	
3.3.174	• Penanganan pengecualian yang lebih baik untuk Systems Manager dan kegagalan penggabungan domain. • Ubah untuk mendukung versioning skema SSM Systems Manager. • Memperbaiki format disk sementara pada Win2K3. • Ubah untuk mendukung konfigurasi ukuran disk yang lebih besar dari 2TB. • Mengurangi penggunaan memori virtual dengan menyetel mode GC ke default. • Dukungan untuk mengunduh artefak dari jalur UNC di plugin `aws:psModule` dan `aws:application` . • Peningkatan logging untuk plugin aktivasi Windows.	

Versi	Detail	Tanggal rilis
3.2.97	• Peningkatan performa dengan penundaan pemuatan rakitan Systems Manager SSM. • Penanganan pengecualian yang lebih baik untuk format sysprep2008.xml yang salah. • Dukungan baris perintah untuk konfigurasi "Terapkan" Systems Manager. • Ubah untuk mendukung penggabungan domain ketika ada penggantian nama komputer yang tertunda. • Dukungan untuk parameter opsional di plugin `aws:applications` . • Dukungan untuk array perintah di plugin `aws:psModule` .	
3.0.54	• Aktifkan dukungan untuk Systems Manager. • Domain secara otomatis bergabung dengan instans EC2 Windows ke direktori AWS melalui Systems Manager. • Konfigurasikan dan unggah CloudWatch log/metrik melalui Systems Manager. • Instal PowerShell modul melalui Systems Manager. • Instal aplikasi MSI melalui Systems Manager.	

Versi	Detail	Tanggal rilis
2.4.233	• Menambahkan tugas terjadwal untuk memulihkan EC2 Config dari kegagalan startup layanan. • Perbaikan pesan kesalahan log Konsol. • Pembaruan untuk meningkatkan dukungan untuk AWS layanan.	
2.3.313	• Memperbaiki masalah dengan konsumsi memori yang besar dalam beberapa kasus ketika fitur CloudWatch Log diaktifkan. • Memperbaiki bug pemutakhiran sehingga ec2config versi yang lebih rendah dari 2.1.19 sekarang dapat dimutakhirkan ke versi terbaru. • Pengecualian pembukaan port COM yang diperbarui agar lebih ramah pengguna dan berguna dalam log. • configServiceSettings UI Ec2 menonaktifkan pengubahan ukuran dan memperbaiki atribusi dan penempatan tampilan versi di UI.	
2.2.12	• Ditangani NullPointerException saat menanyakan kunci registri untuk menentukan status Windows Sysprep yang mengembalikan null sesekali. • Membebaskan sumber daya yang tidak terkelola pada akhirnya diblokir.	
2.2.11	Memperbaiki masalah di CloudWatch plugin untuk menangani baris log kosong.	

Versi	Detail	Tanggal rilis
2.2.10	• Menghapus konfigurasi pengaturan CloudWatch Log melalui UI. • Memungkinkan pengguna untuk menentukan pengatura n CloudWatch Log dalam `%ProgramFiles%\Amazon \Ec2ConfigService\Settings\AWS.EC2.Windows .CloudWatch.json` file untuk memungkinkan perangkat tambahan di masa mendatang.	
2.2.9	Memperbaiki pengecualian yang tidak tertangani dan menambahkan logging.	
2.2.8	• Memperbaiki pemeriksaan versi OS Windows di EC2 Config Installer untuk mendukung Windows Server SP1 2003 dan yang lebih baru. • Memperbaiki penanganan nilai null saat membaca kunci registri yang terkait dengan memperbarui file konfigurasi Sysprep.	
2.2.7	• Ditambahkan dukungan untuk EC2 Config untuk berjalan selama eksekusi Sysprep untuk Windows 2008 dan lebih besar. • Penanganan pengecualian dan logging yang lebih baik untuk diagnostik yang lebih baik	
2.2.6	• Mengurangi beban pada instance dan pada CloudWatch Log saat mengunggah peristiwa log. • Mengatasi masalah pemutakhiran di mana plug-in CloudWatc h Log tidak selalu diaktifkan	

Versi	Detail	Tanggal rilis
2.2.5	• Menambahkan dukungan untuk mengunggah CloudWatch log ke Layanan Log. • Memperbaiki masalah kondisi balapan di plug-in Ec2Output RDPCert • Mengubah opsi pemulihan Layanan EC2 Config untuk Restart dari TakeNoAction • Menambahkan lebih banyak informasi pengecualian saat EC2 Config Crashes	
2.2.4	• Memperbaiki kesalahan ketik di.cmd PostSysprep • Memperbaiki bug yang EC2 Config tidak menyematkan dirinya sendiri ke menu mulai untuk + OS2012	
2.2.3	• Ditambahkan pilihan untuk menginstal EC2 Config tanpa layanan mulai segera setelah menginstal. Untuk menggunak an, jalankan 'Ec2Install.exe start=false' dari prompt perintah • Menambahkan parameter di plugin wallpaper untuk mengontrol penambahan/penghapusan wallpaper. Untuk menggunakan, jalankan 'Ec2 WallpaperInfo .exe set' atau 'Ec2 .exe revert' dari command prompt WallpaperInfo • Ditambahkan memeriksa RealTimeIsUniversal kunci, output pengaturan yang salah dari kunci RealTimeIsUniveral registri ke Konsol • Menghapus ketergantungan EC2 Config pada folder temp Windows • Dihapus ketergantungan UserData eksekusi pada .Net 3.5	

Versi	Detail	Tanggal rilis
2.2.2	• Menambahkan pemeriksaan ke perilaku penghentian layanan untuk memastikan bahwa sumber daya sedang dirilis • Memperbaiki masalah waktu eksekusi yang lama saat bergabung dengan domain	
2.2.1	• Penginstal yang diperbarui untuk memungkinkan pemutakhiran dari versi sebelumnya • Memperbaiki WallpaperInfo bug Ec2 di lingkungan.Net4.5 saja • Memperbaiki bug deteksi driver yang terputus-putus • Menambahkan opsi instal diam. Menjalankan Ec2Install.exe dengan opsi '-q'. Misalnya: 'Ec2Install.exe -q'	
2.2.0	• Menambahkan dukungan untuk lingkungan khusus .Net4 dan .Net4.5 • Penginstal yang Diperbarui	
2.1.19	• Menambahkan dukungan pelabelan disk sementara saat menggunakan driver jaringan Intel (mis. Tipe instans C3). Untuk informasi selengkapnya, lihat Jaringan yang disempurnakan di EC2 instans Amazon. • Menambahkan Versi Asli AMI dan dukungan Nama Asli AMI ke output konsol • Membuat perubahan pada Output Konsol untuk pemformatan/penguraian yang konsisten • File Bantuan yang Diperbarui	

Versi	Detail	Tanggal rilis
2.1.18	• Menambahkan EC2 Config WMI Object untuk pemberitahuan Penyelesaian (-Namespace root\ Amazon -Class _) EC2 ConfigService • Kueri Peningkatan Performa WMI Startup dengan Log Peristiwa besar; dapat menyebabkan CPU tinggi yang berkepanjangan selama eksekusi awal	
2.1.17	• Memperbaiki masalah UserData eksekusi dengan Output Standar dan pengisian buffer Kesalahan Standar • Sidik jari RDP yang salah yang terkadang muncul di Output Konsol untuk> = w2k8 OS telah diperbaiki • Output Konsol sekarang berisi 'RDPCERTIFICATE-Su bjectName: 'untuk Windows 2008+, yang berisi nilai nama mesin • Menambahkan D:\ ke menu tarik-turun Pemetaan Huruf Drive • Tombol Bantuan dipindahkan ke kanan atas dan mengubah tampilan/nuansa • Menambahkan tautan survei Umpan Balik di kanan atas	

Versi	Detail	Tanggal rilis
2.1.16	• Tab Umum menyertakan tautan ke halaman unduhan EC2 Config untuk Versi baru • Hamparan Wallpaper Desktop sekarang disimpan di folder Appdata Lokal Pengguna alih-alih Dokumen Saya untuk mendukung MyDoc pengalihan • MSSQLServer sinkronisasi nama dengan sistem dalam skrip Post-Sysprep (2008+) • Folder Aplikasi yang Diurutkan Ulang (memindahkan file ke direktori Plugin dan menghapus file duplikat) • Output Log Sistem Diubah (Konsol): • * Telah memindahkan ke format tanggal, nama, nilai untuk penguraian yang lebih mudah (Harap mulai memigrasikan dependensi ke format baru) • * Ditambahkan status plugin 'Ec2 SetPassword ' • * Telah menambahkan waktu Mulai dan Akhir Sysprep • Memperbaiki masalah Ephemeral Disks yang tidak diberi label sebagai 'Penyimpanan Sementara' untuk Sistem Operasi non-Inggris • Memperbaiki kegagalan EC2 Config Uninstall setelah menjalankan Sysprep	

Versi	Detail	Tanggal rilis
2.1.15	• Permintaan yang dioptimalkan ke layanan Metadata • Metadata sekarang melewati Pengaturan Proxy • Ephemeral Disks diberi label sebagai 'Penyimpanan Sementara' dan Important.txt ditempatkan pada volume saat ditemukan (hanya driver Citrix PV). Untuk informasi selengkap nya, lihat Tingkatkan driver PV pada instans EC2 Windows. • Ephemeral Disk menetapkan huruf drive dari Z ke A (hanya driver Citrix PV) - penetapan dapat ditimpa menggunakan plugin Pemetaan Huruf Drive dengan label Volume 'Penyimpa nan Sementara X' di mana x adalah angka 0-25) • UserData sekarang berjalan segera setelah 'Windows Siap'	
2.1.14	Perbaikan wallpaper desktop	
2.1.13	• Wallpaper desktop akan menampilkan nama host secara default • Ketergantungan yang dihapus pada layanan Windows Time • Rute ditambahkan dalam kasus di IPs mana beberapa ditugaskan ke satu antarmuka	
2.1.11	• Perubahan dilakukan pada Plugin Ec2Activation • -Memverifikasi status Aktivasi setiap 30 hari • -Jika Masa Tenggang memiliki sisa 90 hari (dari 180 hari), coba kembali aktivasi	

Versi	Detail	Tanggal rilis
2.1.10	• Hamparan wallpaper desktop tidak lagi dipertahankan dengan Sysprep atau Mati tanpa Sysprep • Opsi data pengguna untuk dijalankan pada setiap layanan dimulai dengan <persist>true</persist> • Mengubah lokasi dan nama /.cmd menjadi /Script/ DisableWi nUpdate .cmd PostSysprep • Kata sandi administrator diatur agar tidak kedaluwarsa secara default di PostSysprep /Script/ .cmd • Uninstall akan menghapus skrip EC2 PostSysprep Config dari c:\windows\setup\script\ .cmd CommandComplete • Tambah Rute mendukung metrik antarmuka kustom	
2.1.9	UserData Eksekusi tidak lagi terbatas pada 3851 Karakter	

Versi	Detail	Tanggal rilis
2.1.7	• Versi OS dan pengenal bahasa yang ditulis pada konsol • EC2Versi Config ditulis ke konsol • Versi driver PV yang ditulis pada konsol • Deteksi Pemeriksaan Bug dan output ke konsol pada boot berikutnya ketika ditemukan • Opsi ditambahkan ke config.xml untuk mempertahankan kredensial Sysprep • Tambahkan logika Coba Ulang Rute jika ENI tidak tersedia di awal • PID eksekusi Data Pengguna ditulis ke konsol • Panjang kata sandi minimum yang dihasilkan diambil dari GPO • Setel layanan mulai mencoba lagi 3 kali • Menambahkan contoh file DownloadFile S3_.ps1 dan S3_Upload file.ps1 ke folder/Scripts	

Versi	Detail	Tanggal rilis
2.1.6	• Informasi versi ditambahkan ke tab Umum • Mengganti nama tab Bundel menjadi Gambar • Menyederhanakan proses menentukan kata sandi dan memindahkan UI terkait kata sandi dari tab Umum ke tab Gambar • Mengganti nama tab Pengaturan Disk menjadi Penyimpanan • Menambahkan tab Dukungan dengan alat umum untuk pemecahan masalah • `sysprep.ini` Windows Server 2003 diatur untuk memperluas partisi OS secara default • Menambahkan alamat IP privat ke wallpaper • Alamat IP pribadi ditampilkan di wallpaper • Menambahkan logika coba lagi untuk output Konsol • Memperbaiki pengecualian port Com untuk aksesibilitas metadata - menyebabkan EC2 Config dihentikan sebelum output konsol ditampilkan • Memeriksa status aktivasi pada setiap boot -- aktifkan seperlunya • Memperbaiki masalah jalur relatif -- yang disebabkan saat eksekusi pintasan wallpaper secara manual dari folder startup; menunjuk ke Administrator/log • Memperbaiki warna latar belakang default untuk pengguna Windows Server 2003 (selain Administrator)	

Versi	Detail	Tanggal rilis
2.1.2	• Stempel waktu konsol dalam UTC (Zulu) • Tampilan hyperlink pada tab Sysprep dihapus • Penambahan fitur untuk memperluas Volume Root secara dinamis saat boot pertama untuk Windows 2008+ • Ketika Set-Password diaktifkan, sekarang secara otomatis mengaktifkan EC2 Config untuk mengatur kata sandi • EC2Config memeriksa status aktivasi sebelum menjalankan Sysprep (menyajikan peringatan jika tidak diaktifkan) • `Sysprep.xml` Windows Server 2003 sekarang default ke zona waktu UTC, bukan Pasifik • Server Aktivasi Acak • Mengganti nama tab Pemetaan Drive menjadi Pengaturan Disk • Pindah Inisialisasi item UI Drive dari Umum ke tab Pengaturan Disk • Tombol bantuan sekarang mengarah ke file bantuan HTML • File bantuan HTML yang diperbarui dengan perubahan • ‘Catatan’ yang diperbarui untuk Pemetaan Huruf Drive • Ditambahkan InstallUpdates .ps1 ke/Scripts folder untuk mengotomatisasi Patch dan pembersihan sebelum Sysprep	

Versi	Detail	Tanggal rilis
2.1.0	• Wallpaper desktop menampilkan informasi instans secara default saat logon pertama kali (tidak memutuskan/menghubungkan kembali) • PowerShell dapat dijalankan dari data pengguna dengan mengelilingi kode dengan<powershell></powershell>	

Gunakan EC2 Fast Launch untuk instans Windows Anda

Saat Anda mengonfigurasi AMI Windows Server untuk Peluncuran Cepat EC2, Amazon EC2 membuat serangkaian snapshot yang telah disediakan sebelumnya untuk digunakan untuk peluncuran lebih cepat, sebagai berikut.

1. Amazon EC2 meluncurkan satu set instans t3 temporer, berdasarkan pengaturan Anda.
2. Saat setiap instans temporer menyelesaikan langkah peluncuran standar, Amazon EC2 membuat snapshot instans yang telah disediakan sebelumnya. Poses ini menyimpan snapshot di bucket Amazon S3.
3. Saat snapshot sudah siap, Amazon EC2 mengakhiri instans t3 terkait untuk menekan biaya sumber daya.
4. Lain kali Amazon EC2 meluncurkan instance dari EC2 Fast Launch mengaktifkan AMI, ia menggunakan salah satu snapshot untuk secara signifikan mengurangi waktu yang diperlukan untuk meluncurkan.

Amazon EC2 secara otomatis mengisi ulang snapshot yang Anda miliki saat menggunakannya untuk meluncurkan instans dari AMI yang mengaktifkan Peluncuran Cepat EC2.

Akun apa pun yang memiliki akses ke AMI dengan Peluncuran Cepat EC2 diaktifkan dapat memperoleh manfaat dari pengurangan waktu peluncuran. Ketika pemilik AMI memberikan akses bagi Anda untuk meluncurkan instans, snapshot yang telah disediakan sebelumnya diambil dari akun pemilik AMI.

Jika AMI yang mendukung Peluncuran Cepat EC2 dibagikan dengan Anda, Anda dapat mengaktifkan atau menonaktifkan peluncuran lebih cepat di AMI bersama sendiri. Jika Anda mengaktifkan AMI bersama untuk Peluncuran Cepat EC2, Amazon EC2 akan membuat snapshot yang telah disediakan

sebelumnya secara langsung di akun Anda. Jika Anda menghabiskan snapshot di akun Anda, Anda masih dapat menggunakan snapshot dari akun pemilik AMI.

> **Note**
>
> Peluncuran Cepat EC2 menghapus snapshot yang telah disediakan sebelumnya segera setelah dikonsumsi oleh peluncuran untuk meminimalkan biaya penyimpanan dan mencegah penggunaan kembali. Namun, jika snapshot yang dihapus cocok dengan aturan retensi, Keranjang Sampah secara otomatis mempertahankannya. Kami menyarankan Anda meninjau cakupan aturan retensi Keranjang Sampah Anda sehingga hal ini tidak terjadi. Untuk informasi selengkapnya, lihat Recycle Bin di Panduan Pengguna Amazon EBS.
> Fitur ini tidak sama dengan Pemulihan snapshot cepat EBS. Anda harus secara eksplisit mengaktifkan pemulihan snapshot cepat EBS dengan basis per snapshot, dan memiliki biaya tersendiri.

Video berikut menunjukkan cara mengonfigurasi AMI Windows Anda untuk peluncuran lebih cepat dengan ikhtisar singkat tentang istilah kunci terkait dan definisinya: Meluncurkan instans Windows EC2 hingga 65% lebih cepat aktif. AWS

Biaya sumber daya

Tidak ada biaya layanan untuk mengkonfigurasi AMI Windows untuk Peluncuran Cepat EC2. Namun, harga standar berlaku untuk AWS sumber daya dasar apa pun yang digunakan Amazon EC2. Untuk mempelajari lebih lanjut tentang biaya sumber daya terkait dan cara mengelolanya, lihat Kelola biaya untuk sumber daya dasar Peluncuran EC2 Cepat.

Daftar Isi

- Istilah kunci
- EC2 Prasyarat Peluncuran Cepat untuk Windows
- Konfigurasikan pengaturan Peluncuran Cepat EC2 untuk AMI Amazon EC2 Windows Server Anda
- Lihat AMIs dengan Peluncuran EC2 Cepat diaktifkan
- Kelola biaya untuk sumber daya dasar Peluncuran EC2 Cepat
- Pantau Peluncuran EC2 Cepat
- Peran terkait layanan untuk Peluncuran Cepat EC2
- Memecahkan Masalah Peluncuran Cepat Windows EC2

Istilah kunci

Fitur Peluncuran Cepat EC2 menggunakan istilah kunci berikut:

Snapshot yang telah tersedia

Cuplikan instance yang diluncurkan dari Windows AMI dengan EC2 Fast Launch diaktifkan, dan yang telah menyelesaikan langkah-langkah peluncuran Windows berikut, me-reboot sesuai kebutuhan.

- Sysprep specialize
- Windows Out of Box Experience (OOBE)

Ketika langkah-langkah ini selesai, Peluncuran Cepat EC2 menghentikan instans, dan membuat snapshot yang nantinya digunakan untuk peluncuran lebih cepat dari AMI, berdasarkan konfigurasi Anda.

Frekuensi peluncuran

Mengontrol jumlah snapshot yang telah tersedia yang dapat diluncurkan Amazon EC2 dalam jangka waktu yang ditentukan. Saat Anda mengaktifkan Peluncuran Cepat EC2 untuk AMI, Amazon EC2 akan membuat kumpulan awal snapshot yang telah disediakan sebelumnya di latar belakang. Misalnya, jika frekuensi peluncuran diatur ke lima peluncuran per jam, yang merupakan default, maka Peluncuran Cepat EC2 membuat set awal lima snapshot yang telah disediakan sebelumnya.

Saat Amazon EC2 meluncurkan instans dari AMI dengan Peluncuran Cepat EC2 diaktifkan, Amazon EC2 menggunakan salah satu snapshot yang telah disediakan sebelumnya untuk mengurangi waktu peluncuran. Saat snapshot digunakan, mereka secara otomatis akan diisi ulang, hingga jumlah yang ditentukan oleh frekuensi peluncuran.

Jika Anda memperkirakan ada lonjakan jumlah instans yang diluncurkan dari AMI Anda – misalnya selama acara khusus, – Anda dapat meningkatkan frekuensi peluncuran terlebih dahulu untuk memperhitungkan instans tambahan yang akan Anda perlukan. Ketika tingkat peluncuran Anda kembali normal, Anda dapat menurunkan frekuensi kembali.

Ketika Anda mengalami jumlah peluncuran yang lebih tinggi daripada yang diperkirakan, Anda mungkin menggunakan semua snapshot yang telah tersedia yang ada. Hal ini tidak menyebabkan peluncuran menjadi gagal. Namun, dapat mengakibatkan beberapa instans mengalami proses peluncuran standar, sampai snapshot diisi ulang.

Jumlah sumber daya target

Jumlah snapshot yang telah disediakan sebelumnya untuk tetap tersedia untuk Amazon EC2 Windows Server AMI dengan Peluncuran Cepat EC2 diaktifkan.

Maksimal peluncuran paralel

Mengontrol berapa banyak instans Amazon EC2 yang dapat diluncurkan secara bersamaan untuk membuat snapshot yang telah disediakan sebelumnya untuk Peluncuran Cepat EC2. Jika jumlah sumber daya target Anda lebih tinggi dari peluncuran paralel maksimum yang telah Anda tetapkan, Amazon EC2 meluncurkan jumlah instans yang ditentukan oleh Maksimal peluncuran paralel untuk mulai membuat snapshot. Saat instans tersebut menyelesaikan proses, Amazon EC2 mengambil snapshot dan menghentikan instans. Lalu meluncurkan lebih banyak instans hingga jumlah total snapshot yang tersedia telah mencapai jumlah target sumber daya. Nilai untuk Maksimal peluncuran paralel harus 6 atau lebih besar.

EC2 Prasyarat Peluncuran Cepat untuk Windows

Sebelum Anda mengatur Peluncuran EC2 Cepat, verifikasi bahwa Anda telah memenuhi prasyarat berikut yang diperlukan untuk membuat snapshot untuk di: AMIs Akun AWS

- Jika Anda menyediakan templat peluncuran kustom saat mengonfigurasi Peluncuran EC2 Cepat, layanan akan menggunakan VPC dan pengaturan konfigurasi lain yang telah Anda tetapkan dalam templat peluncuran. Untuk informasi selengkapnya, lihat Gunakan template peluncuran saat Anda mengatur Peluncuran Cepat EC2.
- Jika tidak menggunakan templat peluncuran khusus untuk mengonfigurasi setelan, Anda harus melampirkan EC2FastLaunchFullAccess kebijakan tersebut ke peran IAM saat ini sebelum mengaktifkan Peluncuran EC2 Cepat. Kemudian layanan secara otomatis membuat CloudFormation tumpukan dengan sumber daya berikut di Anda Akun AWS.
  - Awan pribadi virtual (VPC)
  - Subnet pribadi di beberapa Availability Zone
  - Template peluncuran yang dikonfigurasi dengan Layanan Metadata Instance Versi 2 () IMDSv2
  - Grup keamanan tanpa aturan masuk atau keluar
- Peluncuran EC2 Cepat Pribadi AMIs harus mendukung eksekusi skrip data pengguna.
- Untuk mengonfigurasi Peluncuran EC2 Cepat untuk AMI, Anda harus membuat AMI menggunakan Sysprep opsi shutdown. Fitur EC2 Fast Launch saat ini tidak mendukung AMIs yang dibuat dari instance yang sedang berjalan.

Untuk membuat AMI menggunakan Sysprep, lihat Buat Amazon EC2 AMI menggunakan Windows Sysprep.

- Untuk mengaktifkan Peluncuran EC2 Cepat untuk AMI terenkripsi yang menggunakan kunci terkelola pelanggan untuk enkripsi, Anda harus memberikan peran terkait layanan untuk izin Peluncuran EC2 Cepat untuk menggunakan CMK. Untuk informasi selengkapnya, lihat the section called “Akses ke kunci yang dikelola pelanggan”.
- Kuota default untuk peluncuran paralel Max di semua AMIs dalam an Akun AWS adalah 40 per Wilayah. Anda dapat meminta peningkatan Kuota Layanan untuk akun Anda, sebagai berikut.

  1. Buka konsol Service Quotas di https://console.aws.amazon.com/servicequotas/.
  2. Di panel navigasi, pilih Layanan AWS.
  3. Di bilah pencarian, masukkan **`EC2 Fast Launch`**, dan pilih hasilnya.
  4. Pilih link untuk peluncuran instance Parallel untuk membuka halaman detail kuota layanan.
  5. Pilih Permintaan peningkatan di tingkat akun.

  Untuk informasi selengkapnya, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Konfigurasikan pengaturan Peluncuran Cepat EC2 untuk AMI Amazon EC2 Windows Server Anda

Anda dapat mengonfigurasi EC2 Fast Launch untuk Windows AMIs yang Anda miliki, atau AMIs yang dibagikan dengan Anda dari API Konsol Manajemen AWS,, SDKs CloudFormation, atau AWS Command Line Interface (AWS CLI). Sebelum Anda mengonfigurasi Peluncuran Cepat EC2, verifikasi bahwa AMI Anda memenuhi semua prasyarat yang diperlukan untuk membuat snapshot yang telah disediakan sebelumnya. Untuk informasi selengkapnya, lihat EC2 Prasyarat Peluncuran Cepat untuk Windows.

Saat Anda mengaktifkan peluncuran instans Windows yang lebih cepat, Amazon EC2 memeriksa untuk memastikan bahwa Anda memiliki izin yang diperlukan untuk meluncurkan instance dari AMI dan Template Peluncuran yang ditentukan (jika disediakan), termasuk izin untuk AMI terenkripsi. Untuk mencegah kesalahan selama proses peluncuran instans, layanan memvalidasi izin Anda sebelum Peluncuran Cepat EC2 diaktifkan. Jika Anda tidak memiliki izin yang diperlukan, layanan akan mengembalikan kesalahan, dan tidak mengaktifkan Peluncuran Cepat EC2.

EC2 Fast Launch terintegrasi dengan EC2 Image Builder untuk membantu Anda membuat gambar kustom dengan EC2 Fast Launch diaktifkan. Untuk informasi selengkapnya, lihat Membuat pengaturan distribusi untuk AMI Windows dengan Peluncuran Cepat EC2 yang diaktifkan (AWS CLI) di Panduan Pengguna EC2 Image Builder.

Aktifkan Peluncuran Cepat EC2

Sebelum mengubah pengaturan ini, pastikan AMI Anda, dan Wilayah yang Anda jalankan memenuhi semua EC2 Prasyarat Peluncuran Cepat untuk Windows.

Console

Untuk mengaktifkan Peluncuran Cepat EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, di bagian Image, pilih AMIs.
3. Pilih AMI yang akan diperbarui dengan memilih kotak centang di samping Nama.
4. Dari menu Tindakan di atas daftar AMIs, pilih Konfigurasi peluncuran cepat. Ini membuka halaman Konfigurasi peluncuran cepat, tempat Anda mengonfigurasi pengaturan untuk Peluncuran Cepat EC2.
5. Untuk mulai menggunakan snapshot yang telah disediakan sebelumnya untuk meluncurkan instance dari AMI Windows Anda lebih cepat, pilih kotak centang Aktifkan peluncuran cepat untuk Windows.
6. Dari daftar drop-down Tetapkan frekuensi peluncuran yang diantisipasi, pilih nilai untuk menentukan jumlah snapshot yang dibuat dan dipertahankan untuk mencukupi volume peluncuran instans yang Anda harapkan.
7. Setelah selesai membuat perubahan, pilih Simpan perubahan.

> **Note**
>
> Jika Anda perlu menggunakan template peluncuran untuk menentukan VPC, atau untuk mengonfigurasi pengaturan metadata, lihat. IMDSv2 Gunakan template peluncuran saat Anda mengatur Peluncuran Cepat EC2

AWS CLI

Untuk mengaktifkan Peluncuran Cepat EC2

Gunakan enable-fast-launchperintah berikut untuk mengaktifkan Peluncuran Cepat EC2 untuk AMI yang ditentukan, meluncurkan enam instance paralel untuk pra-penyediaan.

```
aws ec2 enable-fast-launch \
    --image-id ami-0abcdef1234567890  \
    --max-parallel-launches 6 \
    --resource-type snapshot
```

Berikut ini adalah output contoh.

```
{
 "ImageId": "ami-0abcdef1234567890",
 "ResourceType": "snapshot",
 "SnapshotConfiguration": {
     "TargetResourceCount": 10
 },
 "LaunchTemplate": {},
 "MaxParallelLaunches": 6,
 "OwnerId": "0123456789123",
 "State": "enabling",
 "StateTransitionReason": "Client.UserInitiated",
 "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
}
```

PowerShell

Untuk mengaktifkan Peluncuran Cepat EC2

Gunakan Enable-EC2FastLaunchcmdlet untuk mengaktifkan Peluncuran Cepat EC2 untuk AMI yang ditentukan, meluncurkan enam instance paralel untuk pra-penyediaan.

```
Enable-EC2FastLaunch `
 -ImageId ami-0abcdef1234567890 `
 -MaxParallelLaunch 6 `
 -Region us-west-2 `
 -ResourceType snapshot
```

Berikut ini adalah output contoh.

```
ImageId               : ami-0abcdef1234567890
 LaunchTemplate        :
 MaxParallelLaunches   : 6
 OwnerId               : 0123456789123
 ResourceType          : snapshot
 SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
 State                 : enabling
 StateTransitionReason : Client.UserInitiated
 StateTransitionTime   : 2/25/2022 12:24:11 PM
```

Nonaktifkan Peluncuran Cepat EC2

Sebelum mengubah pengaturan ini, pastikan AMI Anda, dan Wilayah yang Anda jalankan memenuhi semua EC2 Prasyarat Peluncuran Cepat untuk Windows.

Console

Untuk menonaktifkan Peluncuran Cepat EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, di bagian Image, pilih AMIs.
3. Pilih AMI yang akan diperbarui dengan memilih kotak centang di samping Nama.
4. Dari menu Tindakan di atas daftar AMIs, pilih Konfigurasi peluncuran cepat. Ini membuka halaman Konfigurasi peluncuran cepat, tempat Anda mengonfigurasi pengaturan untuk Peluncuran Cepat EC2.
5. Kosongkan kotak centang Aktifkan peluncuran cepat untuk Windows untuk menonaktifkan Peluncuran Cepat EC2 dan untuk menghapus snapshot yang telah disediakan sebelumnya. Ini membuat AMI menggunakan proses peluncuran standar untuk setiap instans untuk seterusnya.

   > **Note**
   >
   > Saat Anda menonaktifkan optimisasi gambar Windows, snapshot yang telah tersedia akan dihapus secara otomatis. Langkah ini harus diselesaikan sebelum Anda dapat mulai menggunakan fitur ini lagi.

6. Setelah selesai membuat perubahan, pilih Simpan perubahan.

AWS CLI

Untuk menonaktifkan Peluncuran Cepat EC2

Gunakan disable-fast-launchperintah berikut untuk menonaktifkan Peluncuran Cepat EC2 pada AMI yang ditentukan, dan bersihkan snapshot yang sudah ada sebelumnya.

```
aws ec2 disable-fast-launch --image-id ami-01234567890abcedf
```

Berikut ini adalah output contoh.

```
{
    "ImageId": "ami-01234567890abcedf",
    "ResourceType": "snapshot",
    "SnapshotConfiguration": {},
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-01234567890abcedf",
        "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
        "Version": "1"
    },
    "MaxParallelLaunches": 6,
    "OwnerId": "0123456789123",
    "State": "disabling",
    "StateTransitionReason": "Client.UserInitiated",
    "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
}
```

PowerShell

Untuk menonaktifkan Peluncuran Cepat EC2

Gunakan Disable-EC2FastLaunchcmdlet untuk menonaktifkan Peluncuran Cepat EC2 pada AMI yang ditentukan, dan bersihkan snapshot yang sudah ada sebelumnya.

```
Disable-EC2FastLaunch -ImageId ami-0abcdef1234567890
```

Berikut ini adalah output contoh.

```
ImageId               : ami-0abcdef1234567890
```

```
LaunchTemplate        :
Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : disabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Gunakan template peluncuran saat Anda mengatur Peluncuran Cepat EC2

Dengan templat peluncuran, Anda dapat mengonfigurasi serangkaian parameter peluncuran yang digunakan Amazon EC2 setiap kali meluncurkan instans dari templat tersebut. Anda dapat menentukan hal-hal seperti AMI yang akan digunakan untuk gambar dasar, tipe instans, penyimpanan, pengaturan jaringan, dan lainnya.

Templat peluncuran bersifat opsional, kecuali untuk kasus spesifik berikut, di mana Anda harus menggunakan templat peluncuran untuk AMI Windows Anda saat Anda mengonfigurasi peluncuran yang lebih cepat:

- Anda harus menggunakan template peluncuran untuk menentukan VPC yang ada untuk AMI Windows Anda. Ini tidak berlaku jika Anda menggunakan VPC default untuk Anda. Akun AWS
- Jika akun Anda menyertakan kebijakan yang memberlakukan instans IMDSv2 untuk Amazon EC2, Anda harus membuat templat peluncuran yang menentukan konfigurasi metadata yang akan diterapkan. IMDSv2

  Gunakan template peluncuran yang menyertakan konfigurasi metadata Anda dari konsol EC2, atau saat Anda menjalankan enable-fast-launchperintah di AWS CLI, atau panggil tindakan API. EnableFastLaunch

Amazon EC2 EC2 Fast Launch tidak mendukung konfigurasi berikut saat Anda menggunakan template peluncuran. Jika Anda menggunakan template peluncuran untuk Peluncuran Cepat EC2, Anda tidak boleh menentukan salah satu dari berikut ini:

- Skrip data pengguna
- Perlindungan pengakhiran
- Metadata dinonaktifkan

- Opsi spot
- Perilaku shutdown yang mengakhiri instance
- Tag sumber daya untuk antarmuka jaringan, grafik elastis, atau permintaan instance spot

Tentukan VPC

Langkah 1: Buat templat peluncuran

Buat templat peluncuran yang menetapkan detail berikut untuk instans Windows Anda:

- Subnet VPC.
- Tipe instans `t3.xlarge`.

Untuk informasi selengkapnya, lihat Buat template peluncuran Amazon EC2.

Langkah 2: Tentukan template peluncuran untuk AMI Peluncuran Cepat EC2 Anda

Console

Untuk menentukan template peluncuran untuk EC2 Fast Launch

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, di bagian Image, pilih AMIs.
3. Pilih AMI yang akan diperbarui dengan memilih kotak centang di samping Nama.
4. Dari menu Tindakan di atas daftar AMIs, pilih Konfigurasi peluncuran cepat. Ini membuka halaman Konfigurasi peluncuran cepat, tempat Anda mengonfigurasi pengaturan untuk Peluncuran Cepat EC2.
5. Kotak Templat peluncuran melakukan penelusuran tersaring yang mencari templat peluncuran di akun Anda di Wilayah saat ini yang cocok dengan teks yang Anda masukkan. Tentukan semua atau sebagian nama atau ID templat peluncuran di kotak untuk menampilkan daftar templat peluncuran yang cocok. Misalnya, jika Anda memasukkan `fast` dalam kotak, Amazon EC2 mencari semua templat peluncuran di akun Anda di Wilayah saat ini yang memiliki nama “cepat”.

   Untuk membuat templat peluncuran baru, Anda dapat memilih Buat templat peluncuran.
6. Saat Anda memilih sebuah templat peluncuran, Amazon EC2 menampilkan versi default untuk templat tersebut di kotak Versi templat asal. Untuk menentukan versi yang berbeda,

sorot versi default untuk menggantinya, dan masukkan nomor versi yang Anda inginkan di kotak.

7. Setelah selesai membuat perubahan, pilih Simpan perubahan.

AWS CLI

Untuk menentukan template peluncuran untuk EC2 Fast Launch

Gunakan enable-fast-launchperintah dengan `--launch-template` opsi, tentukan nama atau ID dari template peluncuran.

```
--launch-template LaunchTemplateName=my-launch-template
```

PowerShell

Untuk menentukan template peluncuran untuk EC2 Fast Launch

Gunakan Enable-EC2FastLaunchcmdlet dengan parameter -`LaunchTemplate_LaunchTemplateId` or-`LaunchTemplate_LaunchTemplateName`.

```
-LaunchTemplate_LaunchTemplateName my-launch-template
```

Untuk informasi selengkapnya tentang templat peluncuran EC2, lihat Simpan parameter peluncuran instans di templat peluncuran Amazon EC2.

Lihat AMIs dengan Peluncuran EC2 Cepat diaktifkan

Anda dapat menggunakan describe-fast-launch-imagesperintah di AWS CLI, atau Get-EC2FastLaunchImageTools for PowerShell Cmdlet untuk mendapatkan detail AMIs yang mengaktifkan EC2 Fast Launch.

Amazon EC2 memberikan rincian berikut untuk setiap AMI Windows yang dikembalikan dalam hasil:

- ID gambar untuk AMI dengan Peluncuran EC2 Cepat diaktifkan.
- Tipe sumber daya yang digunakan untuk pra-penyediaan AMI Windows terkait. Nilai yang didukung: `snapshot`.
- Konfigurasi snapshot, yang merupakan sekelompok parameter yang mengonfigurasi pra-penyediaan untuk AMI Windows terkait menggunakan snapshot.

- Meluncurkan informasi templat, termasuk ID, nama, dan versi templat peluncuran yang digunakan AMI terkait saat meluncurkan instans Window dari snapshot yang telah tersedia.
- Jumlah maksimum instans yang dapat diluncurkan pada saat yang sama untuk membuat sumber daya.
- ID pemilik untuk AMI terkait. Ini tidak diisi untuk AMIs yang dibagikan dengan Anda.
- Status Peluncuran EC2 Cepat saat ini untuk AMI terkait. Nilai yang didukung meliputi: `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

> **Note**
>
> Anda juga dapat melihat status saat ini yang ditampilkan di halaman Kelola pengoptimalan gambar di EC2 konsol, sebagai status Pengoptimalan gambar.

- Alasan Peluncuran EC2 Cepat untuk AMI terkait berubah ke status saat ini.
- Waktu Peluncuran EC2 Cepat untuk AMI terkait berubah ke status saat ini.

AWS CLI

Untuk menemukan AMIs konfigurasi untuk Peluncuran EC2 Cepat

Gunakan describe-fast-launch-imagesperintah berikut untuk menjelaskan detail untuk masing-masing akun yang AMIs dikonfigurasi untuk Peluncuran EC2 Cepat. Dalam contoh ini, hanya satu AMI di akun yang dikonfigurasi untuk Peluncuran EC2 Cepat.

```
aws ec2 describe-fast-launch-images
```

Berikut ini adalah output contoh.

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
```

```
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

PowerShell

Untuk menemukan AMIs konfigurasi untuk Peluncuran EC2 Cepat

Gunakan Get-EC2FastLaunchImagecmdlet berikut untuk menjelaskan detail untuk masing-masing akun yang AMIs dikonfigurasi untuk Peluncuran EC2 Cepat. Dalam contoh ini, hanya satu AMI di akun yang dikonfigurasi untuk Peluncuran EC2 Cepat.

```
Get-EC2FastLaunchImage -ImageId ami-0abcdef1234567890
```

Berikut ini adalah output contoh.

```
ImageId               : ami-0abcdef1234567890
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 012345678912
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Kelola biaya untuk sumber daya dasar Peluncuran EC2 Cepat

Tidak ada biaya layanan untuk mengkonfigurasi Windows AMIs untuk Peluncuran EC2 Cepat. Namun, saat Anda mengaktifkan Peluncuran EC2 Cepat untuk Amazon EC2 Windows AMI, harga standar berlaku untuk AWS sumber daya dasar yang EC2 digunakan Amazon untuk menyiapkan dan menyimpan snapshot yang telah disediakan sebelumnya. Anda dapat mengonfigurasi tag alokasi biaya untuk membantu Anda melacak dan mengelola biaya yang terkait dengan sumber

daya Peluncuran EC2 Cepat. Untuk informasi selengkapnya tentang cara mengonfigurasi tag alokasi biaya, lihat Lacak biaya Peluncuran EC2 Cepat pada tagihan Anda.

Contoh berikut menunjukkan bagaimana biaya yang terkait dengan biaya snapshot Peluncuran EC2 Cepat mungkin dialokasikan.

Contoh skenario: Perusahaan AtoZ memiliki AMI Windows dengan volume root 50 GiB EBS. Mereka mengaktifkan Peluncuran EC2 Cepat untuk AMI mereka, dan menetapkan jumlah sumber daya target menjadi lima. Selama sebulan, menggunakan Peluncuran EC2 Cepat untuk AMI mereka harganya sekitar $5,00, dan rincian biaya adalah sebagai berikut:

1. Saat AtoZ Example mengaktifkan Peluncuran EC2 Cepat, Amazon EC2 meluncurkan lima instans kecil. Setiap instans berjalan melalui langkah-langkah peluncuran Windows Sysprep dan OOBE, dan boot ulang sesuai kebutuhan. Proses ini memakan waktu beberapa menit untuk setiap instans (waktu dapat bervariasi, berdasarkan seberapa sibuk Wilayah atau Zona Ketersediaan (AZ), dan pada ukuran AMI).

   Biaya

   - Biaya runtime instans (atau runtime minimum, jika ada): lima instans
   - Biaya volume: lima volume root EBS
2. Saat proses pra-penyediaan selesai, EC2 Amazon mengambil snapshot instance, yang disimpan di Amazon S3. Snapshot biasanya disimpan selama 4–8 jam sebelum dikonsumsi oleh peluncuran. Dalam hal ini, biayanya kira-kira 0,02 USD hingga 0,05 USD per snapshot.

   Biaya

   - Penyimpanan snapshot (Amazon S3): lima snapshot
3. Setelah Amazon EC2 mengambil snapshot, itu menghentikan instance. Pada saat itu, instans tidak lagi dikenai biaya. Namun biaya volume EBS terus bertambah.

   Biaya

   - Volume EBS: biaya berlanjut untuk volume root EBS terkait.

> **Note**
>
> Biaya yang ditampilkan di sini hanya contoh. Biaya yang Anda bayar akan bervariasi, tergantung pada konfigurasi AMI dan paket harga Anda.

Lacak biaya Peluncuran EC2 Cepat pada tagihan Anda

Tag alokasi biaya dapat membantu Anda mengatur AWS tagihan untuk mencerminkan biaya yang terkait dengan Peluncuran EC2 Cepat. Anda dapat menggunakan tag berikut yang EC2 ditambahkan Amazon ke sumber daya yang dibuatnya saat menyiapkan dan menyimpan snapshot yang telah disediakan sebelumnya untuk Peluncuran Cepat: EC2

Kunci tag: `CreatedBy`, Nilai: `EC2 Fast Launch`

Setelah Anda mengaktivasi tag tersebut di konsol Manajemen Penagihan dan Biaya, lalu mengatur laporan penagihan terperinci, kolom `user:CreatedBy` tersebut muncul di laporan. Kolom mencakup nilai dari semua layanan. Namun, jika Anda mengunduh file CSV, Anda dapat mengimpor data ke dalam spreadsheet, dan memfilter `EC2 Fast Launch` pada nilainya. Informasi ini juga muncul di AWS Cost and Usage Report saat tag diaktifkan.

Langkah 1: Aktivasi tag alokasi biaya yang ditentukan pengguna

Untuk menyertakan tag sumber daya di laporan biaya Anda, Anda harus mengaktivasi tag tersebut terlebih dahulu di konsol Manajemen Penagihan dan Biaya. Untuk informasi selengkapnya, lihat Mengaktifkan Tag Alokasi Biaya Buatan Pengguna dalam Panduan Pengguna AWS Manajemen Penagihan dan Biaya .

> **Note**
>
> Aktivasi dapat memakan waktu hingga 24 jam.

Langkah 2: Mengatur laporan biaya

Jika Anda sudah mengatur laporan biaya, kolom untuk tag Anda akan muncul saat laporan berikutnya setelah aktivasi selesai. Untuk mengatur laporan biaya untuk pertama kalinya, pilih salah satu dari hal berikut ini.

- Lihat Mengatur laporan alokasi biaya bulanan di Panduan Pengguna AWS Manajemen Penagihan dan Biaya .
- Lihat Membuat Laporan Biaya dan Penggunaan di Panduan Pengguna AWS Cost and Usage Report .

> **Note**
>
> Diperlukan waktu hingga 24 jam untuk AWS mulai mengirimkan laporan ke bucket S3 Anda.

Anda dapat mengonfigurasi Peluncuran EC2 Cepat untuk Windows AMIs AMIs yang Anda miliki, atau yang dibagikan dengan Anda dari EC2 konsol Amazon, API SDKs, CloudFormation,, atau ec2 perintah di AWS CLI. Bagian berikut mencakup langkah-langkah konfigurasi untuk EC2 konsol Amazon dan AWS CLI.

Anda juga dapat membuat Windows kustom AMIs yang dikonfigurasi untuk EC2 Fast Launch dengan EC2 Image Builder. Untuk informasi selengkapnya, lihat Membuat setelan distribusi untuk AMI Windows dengan Peluncuran EC2 Cepat diaktifkan (AWS CLI).

Pantau Peluncuran EC2 Cepat

Bagian ini mencakup cara memantau Amazon EC2 Windows Server AMIs di akun Anda yang mengaktifkan Peluncuran EC2 Cepat.

Pantau perubahan status Peluncuran EC2 Cepat dengan EventBridge

Saat status berubah untuk AMI Windows dengan Peluncuran EC2 Cepat diaktifkan, Amazon EC2 menghasilkan `EC2 Fast Launch State-change Notification` acara. Kemudian Amazon EC2 mengirimkan peristiwa perubahan status ke Amazon EventBridge (sebelumnya dikenal sebagai Amazon CloudWatch Events).

Anda dapat membuat EventBridge aturan yang memicu satu atau beberapa tindakan sebagai respons terhadap peristiwa perubahan status. Misalnya, Anda dapat membuat EventBridge aturan yang mendeteksi kapan Peluncuran EC2 Cepat diaktifkan dan melakukan tindakan berikut:

- Mengirim pesan ke topik Amazon SNS yang memberi tahu para pelanggan.
- Menginvokasi fungsi Lambda yang melakukan beberapa tindakan.
- Mengirim data perubahan status ke Amazon Data Firehose untuk analitik.

Untuk informasi selengkapnya, lihat Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa di Panduan EventBridge Pengguna Amazon.

Peristiwa perubahan status

Fitur Peluncuran EC2 Cepat memancarkan peristiwa perubahan status berformat JSON dengan upaya terbaik. Amazon EC2 mengirimkan acara ke EventBridge dalam waktu dekat. Bagian ini menjelaskan bidang peristiwa dan menunjukkan contoh format peristiwa.

EC2 Fast Launch State-change Notification

imageId

Mengidentifikasi AMI dengan perubahan status Peluncuran EC2 Cepat.

resourceType

Tipe sumber daya yang digunakan untuk pra-penyediaan. Nilai yang didukung: `snapshot`. Nilai default-nya adalah `snapshot`.

status

Status fitur EC2 Fast Launch saat ini untuk AMI yang ditentukan. Nilai-nilai yang valid meliputi:

- mengaktifkan - Anda telah mengaktifkan fitur Peluncuran EC2 Cepat untuk AMI, dan Amazon EC2 telah mulai membuat snapshot untuk proses pra-penyediaan.
- enabling-failed - Ada yang tidak beres yang menyebabkan proses pra-penyediaan gagal saat pertama kali Anda mengaktifkan Peluncuran Cepat EC2 untuk AMI. Hal ini dapat terjadi kapan saja selama proses pra-penyediaan.
- diaktifkan - Fitur Peluncuran EC2 Cepat diaktifkan. Status berubah menjadi `enabled` segera setelah Amazon EC2 membuat snapshot pra-penyediaan pertama untuk AMI Peluncuran Cepat EC2 yang baru diaktifkan. Jika AMI sudah diaktifkan dan melalui pra-penyediaan lagi, perubahan status akan segera terjadi.
- enabled-failed - Status ini hanya berlaku jika ini bukan pertama kalinya AMI EC2 Peluncuran Cepat Anda melewati proses pra-penyediaan. Hal ini dapat terjadi jika fitur EC2 Fast Launch dinonaktifkan dan kemudian diaktifkan lagi, atau jika ada perubahan konfigurasi atau kesalahan lain setelah pra-penyediaan selesai untuk pertama kalinya.
- menonaktifkan - Pemilik AMI telah mematikan fitur Peluncuran EC2 Cepat untuk AMI, dan Amazon EC2 telah memulai proses pembersihan.
- dinonaktifkan - Fitur Peluncuran EC2 Cepat dinonaktifkan. Status berubah menjadi `disabled` segera setelah Amazon EC2 menyelesaikan proses pembersihan.
- gagal-menonaktifkan – Terjadi kesalahan yang menyebabkan proses pembersihan gagal. Ini berarti bahwa beberapa snapshot pra-penyediaan mungkin masih ada di akun.

stateTransitionReason

Alasan bahwa negara berubah untuk EC2 Fast Launch AMI.

> **Note**
>
> Semua bidang dalam pesan peristiwa ini diperlukan.

Contoh berikut menunjukkan AMI Peluncuran EC2 Cepat yang baru diaktifkan yang telah meluncurkan instance pertama untuk memulai proses pra-penyediaan. Pada saat ini, statusnya adalah `enabling`. Setelah Amazon EC2 membuat snapshot pra-penyediaan pertama, status berubah menjadi. `enabled`

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
 "source": "aws.ec2",
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Pantau metrik Peluncuran EC2 Cepat dengan CloudWatch

Amazon EC2 AMIs dengan Peluncuran EC2 Cepat mengaktifkan kirim metrik ke Amazon CloudWatch. Anda dapat menggunakan, API Konsol Manajemen AWS AWS CLI, atau API untuk mencantumkan metrik yang dikirimkan EC2 Fast Launch. CloudWatch `AWS/EC2`Namespace mencakup metrik Peluncuran EC2 Cepat berikut:

Metrik	Deskripsi
NumberOfAvailableFastLaunchSnapshots	Jumlah snapshot pra-penyediaan yang tersedia per EC2 Peluncuran Cepat mengaktifkan AMI.
NumberOfInstancesFastLaunched	Jumlah instans per Peluncuran EC2 Cepat memungkinkan AMI yang diluncurkan dari snapshot yang telah disediakan sebelumnya.
NumberOfInstancesNotFastLaunched	Jumlah instans per Peluncuran EC2 Cepat memungkinkan AMI yang menghasilkan boot dingin karena kurangnya snapshot pra-penye diaan yang tersedia pada waktu peluncuran.
FastLaunchSnapshotUsedToRefillStartTime	Stempel waktu saat Amazon EC2 meluncurk an gambar baru dari Peluncuran EC2 Cepat memungkinkan AMI membuat snapshot lain setelah snapshot yang ada digunakan.
FastLaunchSnapshotCreationTime	Mengukur waktu yang dibutuhkan Amazon EC2 untuk meluncurkan instance dan membuat snapshot untuk AMI yang mengaktifkan Peluncuran EC2 Cepat.

Peran terkait layanan untuk Peluncuran Cepat EC2

Amazon EC2 menggunakan peran tertaut layanan untuk izin yang diperlukan untuk memanggil Layanan AWS lain mewakili Anda. Peran terkait layanan adalah jenis unik dari peran IAM yang ditautkan langsung ke sebuah. Layanan AWS Peran terkait layanan menyediakan cara aman untuk mendelegasikan izin Layanan AWS karena hanya layanan tertaut yang dapat mengambil peran terkait layanan. Untuk informasi selengkapnya tentang cara Amazon EC2 menggunakan peran IAM, termasuk peran tertaut layanan, lihat IAM role untuk Amazon EC2.

Amazon EC2 menggunakan peran tertaut layanan bernama AWSServiceRoleForEC2FastLaunch untuk membuat dan mengelola sepaket snapshot pra-penyediaan yang mengurangi waktu yang diperlukan untuk meluncurkan instans dari AMI Windows Anda.

Izin diberikan oleh AWSServiceRoleForEC2FastLaunch

Peran terkait layanan AWSServiceRoleForEC2FastLaunch memercayai layanan berikut untuk mengambil peran tersebut:

- `ec2fastlaunch.amazonaws.com`

Amazon EC2 menggunakan kebijakan yang dikelola EC2FastLaunchServiceRolePolicy untuk menyelesaikan tindakan berikut:

- AWS CloudFormation— Izinkan Peluncuran Cepat EC2 untuk mendapatkan deskripsi CloudFormation tumpukan terkait.
- Amazon CloudWatch — Posting data metrik yang terkait dengan Peluncuran Cepat EC2 ke namespace Amazon EC2.
- Amazon EC2 - Akses diberikan untuk Peluncuran Cepat EC2 untuk melakukan tindakan berikut:
  - Luncurkan instans dari Amazon EC2 Windows Server AMI dengan Peluncuran Cepat EC2 diaktifkan, untuk melakukan langkah-langkah penyediaan. Selain itu tentukan pola sumber daya `ec2:RunInstances` yang memungkinkan AMI yang terkait dengan License Manager.
  - Hentikan dan hentikan instance yang diluncurkan oleh EC2 Fast Launch setelah membuat snapshot yang telah disediakan sebelumnya.
  - Jelaskan sumber daya jenis gambar dan instans yang digunakan untuk meluncurkan instans dari Amazon EC2 Windows Server AMI dengan Peluncuran Cepat EC2 diaktifkan dan buat snapshot darinya.
  - Jelaskan sumber daya template peluncuran dan luncurkan instance dari template peluncuran.
  - Jelaskan instance, atribut instance dan status instance, volume, dan atribut volume.
  - Jelaskan antarmuka jaringan.
  - Hapus sumber daya yang dibuat oleh Peluncuran Cepat EC2, termasuk snapshot, template peluncuran, volume, dan antarmuka jaringan.
  - Beri tag sumber daya yang dibuat oleh Peluncuran Cepat EC2 untuk diluncurkan dan pra-penyediaan, instans Windows, dan buat snapshot untuk proses peluncuran akhir untuk dikonsumsi.
- Amazon EventBridge - Termasuk akses untuk membuat aturan EventBridge acara dan mengambil detail tentang atau menghapus aturan yang dibuatnya. Peluncuran Cepat EC2 juga dapat memperoleh daftar layanan target yang menerima acara Peluncuran Cepat EC2 yang diteruskan

berdasarkan aturan acara, dan menambahkan layanan target ke atau menghapusnya dari aturan acara yang dibuatnya.

- IAM - Memungkinkan Peluncuran Cepat EC2 untuk membuat peran `EC2FastLaunchServiceRolePolicy` terkait layanan, untuk mendapatkan dan menggunakan profil instans yang namanya berisi`ec2fastlaunch`, dan untuk meluncurkan instance atas nama Anda menggunakan profil instans dari template peluncuran Anda.
- AWS KMS— Termasuk akses untuk membuat hibah dan daftar hibah yang dibuat oleh EC2 Fast Launch yang dapat dihentikan. Juga untuk mendeskripsikan atau menggunakan kunci untuk tujuan mengenkripsi atau mendekripsi volume yang dilampirkan ke instance yang dibuat oleh Peluncuran Cepat EC2, dan untuk menghasilkan kunci data yang bukan teks biasa.

Untuk melihat izin kebijakan ini, lihat EC2FastLaunchServiceRolePolicydi Referensi Kebijakan AWS Terkelola.

Untuk informasi selengkapnya tentang penggunaan kebijakan terkelola untuk Amazon EC2, lihat AWS kebijakan terkelola untuk Amazon EC2.

Buat peran tertaut layanan

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda mulai menggunakan Peluncuran Cepat EC2 untuk AMI, Amazon EC2 akan membuat peran terkait layanan untuk Anda, jika belum ada.

Jika peran terkait layanan dihapus dari akun Anda, Anda dapat mengaktifkan Peluncuran Cepat EC2 untuk AMI Windows lain untuk membuat ulang peran di akun Anda. Atau, Anda dapat menonaktifkan Peluncuran Cepat EC2 untuk AMI Anda saat ini, dan kemudian mengaktifkannya lagi. Namun, menonaktifkan fitur ini akan membuat AMI Anda menggunakan proses peluncuran standar untuk semua instans baru sementara Amazon EC2 menghapus semua snapshot pra-penyediaan Anda. Setelah semua snapshot yang telah disediakan sebelumnya hilang, Anda dapat mengaktifkan kembali penggunaan EC2 Fast Launch untuk AMI Anda.

Akses ke kunci yang dikelola pelanggan

Untuk mengaktifkan Peluncuran Cepat EC2 untuk AMI terenkripsi yang menggunakan kunci terkelola pelanggan untuk enkripsi, Anda harus memberikan AWSServiceRoleForEC2FastLaunch izin peran untuk menggunakan CMK. Untuk melakukan ini, panggil perintah create-grant. Untuk`--grantee-principal`, tentukan ARN untuk AWSServiceRoleForEC2FastLaunch peran di akun Anda. Untuk `--operations`, tentukan `CreateGrant`.

```
aws kms create-grant \
    --key-id arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2FastLaunch \
    --operations CreateGrant
```

Edit peran tertaut layanan

Amazon EC2 tidak mengizinkan Anda untuk mengubah peran tertaut layanan AWSServiceRoleForEC2FastLaunch. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran, karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengubah deskripsi peran dengan menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Hapus peran tertaut layanan

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus semua sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Amazon EC2 yang terkait dengan Amazon EC2 Windows Server AMI Anda dengan Peluncuran Cepat EC2 diaktifkan, karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForEC2FastLaunchterkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna IAM.

Wilayah yang Didukung

Amazon EC2 mendukung peran terkait layanan Peluncuran Cepat EC2 di semua Wilayah tempat layanan Amazon EC2 tersedia.

Memecahkan Masalah Peluncuran Cepat Windows EC2

Skenario pemecahan masalah

Skenario berikut dapat membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat mencoba mengaktifkan Peluncuran EC2 Cepat.

Tidak dapat menghentikan instance untuk pembuatan snapshot

Deskripsi

Saat Anda mengaktifkan Peluncuran EC2 Cepat, layanan akan meluncurkan serangkaian instance yang digunakan untuk membuat snapshot yang telah disediakan sebelumnya. Setiap contoh diberikan 30 menit untuk menyelesaikan proses. Jika salah satu instans berhasil diselesaikan, maka layanan akan menetapkan status Peluncuran Cepat untuk AMI. `Enabled` Namun, jika instans gagal menyelesaikan proses dalam waktu yang ditentukan, dan tidak ada instans lain yang menyelesaikan proses, layanan akan menghentikan semua instance dan menetapkan status Peluncuran Cepat untuk AMI dan alasan status Peluncuran Cepat sebagai berikut: `enabling_failed`

```
Unable to stop instance ID=i-1234567890abcdef0 for snapshot creation.
```

Penyebab

Paling sering, ini disebabkan oleh mencoba mengaktifkan Peluncuran EC2 Cepat untuk AMI Windows yang dibuat dari instance yang sedang berjalan, atau AMI yang tidak memenuhi semuaEC2 Prasyarat Peluncuran Cepat.

Solusi

Pastikan AMI yang Anda gunakan memenuhi semuaEC2 Prasyarat Peluncuran Cepat.

Untuk mengonfigurasi Peluncuran EC2 Cepat untuk AMI, Anda harus membuat AMI menggunakan Sysprep opsi shutdown. Untuk informasi selengkapnya, lihat Buat Amazon EC2 AMI menggunakan Windows Sysprep.

Anda telah mencapai batas VPC Anda

Deskripsi

Jika Anda tidak menggunakan template peluncuran untuk menentukan VPC yang ada, dan tidak memiliki VPC default yang ditentukan untuk akun Anda, layanan akan secara otomatis membuat CloudFormation tumpukan yang menyertakan VPC dan sumber daya lainnya, seperti yang dijelaskan dalam. EC2 Prasyarat Peluncuran Cepat

Penyebab

Anda telah mencapai jumlah maksimum VPCs yang diizinkan di Wilayah Anda, dan Anda belum menentukan VPC yang ada Akun AWS untuk Peluncuran EC2 Cepat untuk digunakan. Hal ini menyebabkan proses gagal.

Solusi

Anda dapat mengatasi masalah ini dengan salah satu opsi berikut:

- Anda dapat meminta kenaikan kuota
- Anda dapat memberikan template peluncuran yang menentukan VPC yang ada

Untuk meminta peningkatan jumlah VPCs yang dapat ditentukan akun Anda per Wilayah, ikuti langkah-langkah berikut:

1. Buka konsol Service Quotas di https://console.aws.amazon.com/servicequotas/.
2. Di Dasbor Konsol Layanan, pilih Amazon Virtual Private Cloud (Amazon VPC). Ini membuka kuota layanan VPC.
3. Filter `VPCs per Region` untuk langsung menuju kuota.
4. Pilih VPCs per Wilayah, dan pilih Permintaan peningkatan di tingkat akun.

Jika Anda memiliki permintaan kuota yang mendesak, atau jika permintaan kenaikan kuota Anda ditolak, hubungi Support untuk bantuan. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Izin tidak cukup untuk mengaktifkan Peluncuran EC2 Cepat

Deskripsi

Saat Anda mengaktifkan Peluncuran EC2 Cepat untuk pertama kalinya tanpa menentukan Template Peluncuran, Peluncuran EC2 Cepat membuat CloudFormation tumpukan milik layanan dengan sumber daya default layanan. Namun, CloudFormation template akan gagal diterapkan jika kepala sekolah IAM Anda (peran atau pengguna) tidak memiliki izin yang diperlukan.

Pesan log mungkin terlihat seperti berikut:

```
Can't enable EC2 Fast Launch. The IAM credentials that you are using do not have
 sufficient permissions. Attach EC2FastLaunchFullAccess in the IAM console.
```

Penyebab

Pengguna atau peran IAM Anda tidak memiliki izin yang diperlukan untuk mengaktifkan EC2 Peluncuran Cepat.

Solusi

Verifikasi bahwa prinsipal IAM Anda (pengguna atau peran) yang mengaktifkan Peluncuran EC2 Cepat memiliki `EC2FastLaunchFullAccess` kebijakan yang dilampirkan. Kebijakan AWS terkelola ini memberikan akses penuh ke semua sumber daya Peluncuran EC2 Cepat. Untuk melihat izin kebijakan ini, lihat kebijakan di Referensi EC2FastLaunchFullAccessKebijakan AWS Terkelola.

Ubah kata sandi Administrator Windows untuk instans Amazon EC2 Anda

Jika Anda meluncurkan instans Anda dari AMI AWS Windows, agen peluncuran yang sudah diinstal sebelumnya menetapkan kata sandi default sebagai berikut:

- Untuk Windows Server 2022 dan yang lebih baruEC2Luncurkan v2, buat kata sandi default.
- Untuk Windows Server 2016 dan 2019, EC2Peluncuran agen menghasilkan kata sandi default.
- Untuk Windows Server 2012 R2 dan sebelumnya, EC2Layanan Config menghasilkan kata sandi default.

> **Note**
>
> Untuk Windows Server 2016 dan yang lebih baru AMIs, `Password never expires` dinonaktifkan untuk administrator lokal. Untuk versi AMI sebelum Windows Server 2016, `Password never expires` diaktifkan untuk administrator lokal.

Mengubah kata sandi Administrator setelah terhubung

Saat Anda terhubung ke sebuah instans untuk pertama kalinya, kami menyarankan Anda untuk mengubah kata sandi Administrator dari nilai default-nya. Gunakan prosedur berikut untuk mengubah kata sandi Administrator untuk instans Windows.

> **Important**
>
> Simpan kata sandi baru di tempat yang aman. Anda tidak akan bisa mendapatkan kembali kata sandi baru menggunakan konsol Amazon EC2. Konsol hanya dapat mengambil kata sandi default. Jika Anda mencoba untuk menyambung ke instans menggunakan kata sandi default setelah mengubahnya, Anda akan mendapatkan pesan kesalahan "Kredensial Anda tidak berfungsi".

Untuk mengubah kata sandi Administrator lokal

1. Hubungkan ke instans dan buka prompt perintah.
2. Jalankan perintah berikut. Jika kata sandi baru Anda menyertakan karakter khusus, apit kata sandi dengan tanda kutip ganda.

```
net user Administrator "new_password"
```

3. Simpan kata sandi baru di tempat yang aman.

Mengubah kata sandi yang hilang atau kedaluwarsa

Jika Anda kehilangan kata sandi atau kedaluwarsa, Anda dapat membuat kata sandi baru. Untuk prosedur pengaturan ulang kata sandi, lihat Setel ulang kata sandi administrator Windows untuk instans Windows Amazon EC2.

Tambahkan komponen Windows Server opsional ke instans Amazon EC2 Windows

Untuk mengakses dan menginstal komponen opsional, Anda harus menemukan snapshot EBS yang benar untuk versi Windows Server Anda, membuat volume dari snapshot, dan melampirkan volume ke instans Anda.

Sebelum Anda mulai

Gunakan Konsol Manajemen AWS atau alat baris perintah untuk mendapatkan ID instance dan Availability Zone dari instance Anda. Anda harus membuat volume EBS di Zona Ketersediaan yang sama dengan instans.

Gunakan salah satu prosedur berikut untuk menambahkan komponen Windows Server ke instans Anda.

Console

Untuk menambahkan komponen Windows ke instans Anda

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Snapshot.
3. Dari bilah Filter, pilih Snapshot publik.

4. Tambahkan filter Alias Pemilik dan pilih amazon.
5. Tambahkan filter Deskripsi dan masukkan **`Windows`**.
6. Tekan Enter
7. Pilih snapshot yang sesuai dengan arsitektur sistem dan preferensi bahasa Anda. Misalnya, pilih Media Instalasi Bahasa Inggris Windows 2019 jika instans Anda menjalankan Windows Server 2019.
8. Pilih Tindakan, Buat volume dari snapshot.
9. Untuk Zona Ketersediaan, pilih Zona Ketersediaan yang cocok dengan instans Windows Anda. Pilih Tambahkan tanda dan masukkan **`Name`** untuk kunci tanda serta nama deskriptif untuk nilai tanda. Pilih Buat volume.
10. Di pesan volume Berhasil dibuat (spanduk hijau), pilih volume yang baru saja Anda buat.
11. Pilih Tindakan, Lampirkan Volume.
12. Dari instans, pilih ID instans.
13. Untuk Nama perangkat, masukkan nama perangkat untuk lampiran. Jika Anda memerlukan bantuan terkait nama perangkat, lihat Nama perangkat untuk volume di EC2 instans Amazon.
14. Pilih Lampirkan volume.
15. Hubungkan ke instans Anda dan sediakan volume. Untuk informasi selengkapnya, lihat Menyediakan volume Amazon EBS untuk digunakan dalam Panduan Pengguna Amazon EBS.

    > **Important**
    >
    > Jangan menginisialisasi volume.

16. Buka Panel Kontrol, Program dan Fitur. Pilih Aktifkan atau nonaktifkan fitur Windows. Jika Anda diminta untuk media instalasi, tentukan volume EBS dengan media instalasi.
17. (Opsional) Saat Anda selesai menggunakan media instalasi, Anda dapat melepaskan volume. Setelah Anda melepaskan volume, Anda dapat menghapusnya.

AWS CLI

Untuk menambahkan komponen Windows ke instans Anda

1. Gunakan perintah describe-snapshots dengan parameter `owner-ids` dan filter `description` untuk mendapatkan daftar snapshot media instalasi yang tersedia.

```
aws ec2 describe-snapshots \
    --owner-ids amazon \
    --filters Name=description,Values=Windows*
```

2. Dalam keluaran, catat ID snapshot yang cocok dengan arsitektur sistem dan preferensi bahasa Anda. Misalnya:

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
   ]
}
```

3. Gunakan perintah create-volume untuk membuat volume dari snapshot. Tentukan Zona Ketersediaan yang sama dengan instans Anda.

```
aws ec2 create-volume \
    --snapshot-id snap-0abcdef1234567890 \
    --volume-type gp2 \
    --availability-zone us-east-1a
```

4. Pada keluaran, catat ID volume.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-01234567890abcdef",
    "State": "creating",
```

```
    "Iops": 100,
    "SnapshotId": "snap-0abcdef1234567890",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Gunakan perintah attach-volume untuk melampirkan volume ke instans Anda.

```
aws ec2 attach-volume \
    --volume-id vol-0c98b37f30bcbc290 \
    --instance-id i-01474ef662b89480 \
    --device xvdg
```

6. Hubungkan ke instans Anda dan sediakan volume. Untuk informasi selengkapnya, lihat Menyediakan volume Amazon EBS untuk digunakan dalam Panduan Pengguna Amazon EBS.

> **Important**
>
> Jangan menginisialisasi volume.

7. Buka Panel Kontrol, Program dan Fitur. Pilih Aktifkan atau nonaktifkan fitur Windows. Jika Anda diminta untuk media instalasi, tentukan volume EBS dengan media instalasi.
8. (Opsional) Saat Anda selesai menggunakan media instalasi, gunakan perintah detach-volume untuk melepaskan volume dari instans Anda. Setelah Anda melepaskan volume, Anda dapat menggunakan perintah delete-volume untuk menghapus volume.

PowerShell

Untuk menambahkan komponen Windows ke instans Anda

1. Gunakan Get-EC2Snapshotcmdlet dengan `description` filter `Owner` dan untuk mendapatkan daftar snapshot media instalasi yang tersedia.

```
Get-EC2Snapshot `
    -Owner amazon `
    -Filter @{ Name="description"; Values="Windows*" }
```

2. Dalam keluaran, catat ID snapshot yang cocok dengan arsitektur sistem dan preferensi bahasa Anda. Contoh:

```
...
DataEncryptionKeyId :
Description         : Windows 2019 English Installation Media
Encrypted           : False
KmsKeyId            :
OwnerAlias          : amazon
OwnerId             : 123456789012
Progress            : 100%
SnapshotId          : snap-0abcdef1234567890
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-01234567890abcdef
VolumeSize          : 6
...
```

3. Gunakan New-EC2Volumecmdlet untuk membuat volume dari snapshot. Tentukan Zona Ketersediaan yang sama dengan instans Anda.

```
New-EC2Volume `
    -AvailabilityZone us-east-1a `
    -VolumeType gp2 `
    -SnapshotId snap-0abcdef1234567890
```

4. Pada keluaran, catat ID volume.

```
Attachments      : {}
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
Size             : 6
SnapshotId       : snap-0abcdef1234567890
State            : creating
Tags             : {}
VolumeId         : vol-01234567890abcdef
VolumeType       : gp2
```

5. Gunakan Add-EC2Volumecmdlet untuk melampirkan volume ke instance Anda.

```
Add-EC2Volume `
    -InstanceId i-1234567890abcdef0 `
    -VolumeId vol-01234567890abcdef `
    -Device xvdh
```

6. Hubungkan ke instans Anda dan sediakan volume. Untuk informasi selengkapnya, lihat Menyediakan volume Amazon EBS untuk digunakan dalam Panduan Pengguna Amazon EBS.

> **Important**
>
> Jangan menginisialisasi volume.

7. Buka Panel Kontrol, Program dan Fitur. Pilih Aktifkan atau nonaktifkan fitur Windows. Jika Anda diminta untuk media instalasi, tentukan volume EBS dengan media instalasi.
8. (Opsional) Ketika Anda selesai dengan media instalasi, gunakan Dismount-EC2Volumecmdlet untuk melepaskan volume dari instans Anda. Setelah Anda melepaskan volume, Anda dapat menggunakan Remove-EC2Volumecmdlet untuk menghapus volume.

Instal Windows Subsystem untuk Linux pada instans EC2 Windows Anda

Windows Subsystem for Linux (WSL) adalah fitur dari Microsoft Windows. Dengan menginstal WSL pada instans Windows EC2 Anda, Anda dapat menjalankan alat Linux asli langsung pada instance Windows Anda.

Ada dua versi Windows Subsystem for Linux (WSL): WSL 1 dan WSL 2. Untuk informasi selengkapnya, lihat Dokumentasi Subsistem Windows untuk Linux di situs web Microsoft.

Persyaratan

- Sistem operasi harus Windows Server 2019 atau yang lebih baru.
- Anda hanya dapat menginstal WSL 1 pada instance Windows virtual (ukuran instans tidak `.metal` atau tidak mendukung virtualisasi bersarang).
- Anda dapat menginstal WSL 1 atau WSL 2 pada instance yang mendukung virtualisasi bersarang dan mengaktifkan Opsi CPU. `NestedVirtualization`

- Anda dapat menginstal WSL 1 atau WSL 2 pada instance bare metal (ukuran instans adalah). `.metal` Instans bare metal menyediakan dukungan yang diperlukan untuk virtualisasi bersarang secara default.

Untuk informasi selengkapnya tentang virtualisasi bersarang untuk EC2, lihat. Gunakan virtualisasi bersarang untuk menjalankan hypervisor di instans Amazon EC2

Menginstal WSL pada instans Windows Anda

Untuk menginstal WSL 1

1. Instal WSL. Proses yang akan Anda gunakan tergantung pada versi Windows Server yang berjalan pada instance.
   - Windows Server 2022 dan yang lebih baru - Jalankan perintah instalasi standar berikut pada instans EC2 Anda.

     ```
     wsl --install --enable-wsl1 --no-launch
     ```

   - Windows Server 2019 - Aktifkan WSL dan kemudian instal WSL seperti yang dijelaskan dalam Instal WSL pada versi Windows Server sebelumnya di situs web Microsoft.
2. Mulai ulang instans EC2 Anda.

   ```
   shutdown -r -t 20
   ```

3. Untuk mengonfigurasi WSL untuk menggunakan WSL 1, jalankan perintah berikut pada instans Anda. Langkah ini diperlukan untuk instance tervirtualisasi (ukuran instans tidak `.metal` atau tidak dikonfigurasi untuk virtualisasi bersarang).

   ```
   wsl --set-default-version 1
   ```

4. Instal distribusi default.

   ```
   wsl --install
   ```

Untuk menginstal WSL 2 (.metal atau instance dengan virtualisasi bersarang diaktifkan)

Jalankan perintah instalasi standar berikut pada instans EC2 Anda. Secara default, WSL 2 diinstal.

```
wsl --install
```

Utilitas pemecahan masalah Windows EC2

`EC2WinUtil`Driver menyediakan jenis dukungan pemecahan masalah berikut untuk instance Windows Anda.

Tumpukan panggilan crash

`EC2WinUtil`mengumpulkan informasi kerusakan dasar dari instans Anda dan menuliskannya ke konsol serial. Daftar berikut mencakup beberapa detail utama yang ditulis utilitas ke konsol.

- Identifikasi modul yang menghasilkan kesalahan.
- Kode kesalahan Windows yang terkait dengan acara tersebut.
- Jejak tumpukan panggilan terbaru.

Dengan rincian ini, Anda dapat melakukan analisis akar penyebab awal dan menentukan apakah analisis lebih lanjut diperlukan. Output ke konsol serial juga memungkinkan AWS untuk melacak tren crash untuk driver Amazon EC2, dan mendiagnosis kejadian crash skala besar.

> **Note**
>
> `EC2WinUtil`tidak mengumpulkan data pelanggan apa pun di tumpukan panggilan kerusakannya.

Untuk catatan rilis driver, lihat Riwayat versi Driver Utilitas Windows EC2

Riwayat versi Driver Utilitas Windows EC2

Tabel berikut menunjukkan `EC2WinUtil` driver mana yang berjalan pada setiap versi Windows Server di Amazon EC2. Versi sebelumnya dari sistem operasi menggunakan driver yang sudah diinstal pada AWS Windows Server AMIs yang diluncurkan instans. AMIs yang dibagikan dengan Anda atau yang Anda berlangganan AWS Marketplace tidak memiliki driver yang sudah diinstal sebelumnya.

Versi Windows Server	EC2WinUtil versi driver
Windows Server 2025	versi terbaru

Versi Windows Server	EC2WinUtil versi driver
Windows Server 2022	versi terbaru
Windows Server 2019	versi terbaru
Windows Server 2016	versi terbaru

> **Note**
>
> Sebelum driver versi 3.0.0, `EC2WinUtil` driver tidak tersedia untuk diunduh untuk instalasi manual. Versi sebelumnya hanya tersedia sebagai driver prainstal untuk AWS Windows AMIs.

Tabel berikut menjelaskan versi `EC2WinUtil` driver yang dirilis.

Versi Package	Versi Driver	Detail	Tanggal rilis
3.1.1	3.1.1	Peningkatan panjang tumpukan panggilan saat masuk ke output konsol.	Maret 3, 2026
3.1.0	3.1.0	Peningkatan penanganan acara manajemen daya.	Februari 4, 2026
3.0.0	3.0.0	Memodernisasi driver untuk Windows 10 dan menambahkan dukungan untuk instalasi sebagai driver primitif.	Juni 13, 2024
2.0.0	2.0.0	Menambahkan dukungan untuk output pada port serial MMIO untuk jenis instance logam. Juga meningkat kan penguraian kerusakan dan memperbarui format output.	23 Agustus 2018

Versi Package	Versi Driver	Detail	Tanggal rilis
1.0.1	1.0.1	Mengubah nama driver `EC2WinUtil` karena konflik namespace dengan Amazon Inspector. Beberapa perbaikan bug disertakan.	1 Maret 2018
1.0.0	1.0.0	Pelepasan awal. Sopir awalnya dipanggil`AwsAgent`.	28 November 2017

Tingkatkan instans EC2 Windows ke versi Windows Server yang lebih baru

Jika sudah waktunya untuk memutakhirkan sistem operasi Windows Server pada instans EC2 Windows Anda dari versi sebelumnya, Anda dapat menggunakan salah satu metode berikut.

Peningkatan di tempat

Upgrade di tempat beroperasi pada instance yang ada. Hanya file sistem operasi yang terpengaruh selama proses ini, sementara pengaturan, peran server, dan data Anda dibiarkan utuh.

Migrasi (juga dikenal sebagai side-by-side upgrade)

Migrasi melibatkan pengambilan pengaturan, konfigurasi, dan data, dan porting ini ke sistem operasi yang lebih baru pada instans Windows EC2 baru. Anda dapat meluncurkan instans Anda dari AMI Windows publik atau pribadi yang Anda berlangganan dari AWS Marketplace, atau AMI yang dibagikan dengan Anda. Anda juga dapat membuat AMI kustom dengan EC2 Image Builder. Lihat Panduan Pengguna Image Builder untuk informasi selengkapnya.

> **Note**
>
> AWS menyediakan satu set Amazon Machine Images (AMI) yang tersedia untuk umum untuk versi Windows Server yang berjalan pada instans EC2. Ini AMIs diperbarui setiap bulan. Untuk informasi tentang Windows terbaru AMIs, lihat Referensi AMI AWS Windows.

Microsoft secara tradisional merekomendasikan migrasi ke versi Windows Server yang lebih baru daripada memutakhirkan di tempat. Migrasi dapat mengakibatkan lebih sedikit kesalahan atau masalah pemutakhiran, tetapi dapat memakan waktu lebih lama daripada peningkatan di tempat karena kebutuhan untuk menyediakan instance baru, merencanakan dan port aplikasi, dan menyesuaikan pengaturan konfigurasi pada instance baru. Pemutakhiran langsung bisa lebih cepat, tetapi ketidaksesuaian perangkat lunak dapat menghasilkan kesalahan.

Daftar Isi

- Lakukan pemutakhiran di tempat pada instans Windows EC2 Anda
- Gunakan runbook Otomasi untuk memutakhirkan instans Windows EC2
- Migrasikan instans Windows EC2 ke tipe instans berbasis Nitro
- Memecahkan masalah upgrade sistem operasi pada instans EC2 Windows

Lakukan pemutakhiran di tempat pada instans Windows EC2 Anda

Sebelum Anda melakukan pemutakhiran langsung, Anda harus menentukan driver jaringan mana yang dijalankan instans. Driver jaringan PV memungkinkan Anda mengakses instans Anda menggunakan Desktop Jarak Jauh. Instans menggunakan AWS PV, Intel Network Adapter, atau driver Enhanced Networking. Untuk informasi selengkapnya, lihat Driver paravirtual untuk instans Windows.

Sebelum Anda memulai pemutakhiran langsung

Selesaikan tugas berikut dan catat detail penting berikut sebelum Anda memulai pemutakhiran langsung.

- Baca dokumentasi Microsoft untuk memahami persyaratan pemutakhiran, masalah umum, dan batasan. Tinjau juga instruksi resmi untuk pemutakhiran.
  - Opsi Pemutakhiran untuk Windows Server 2012
  - Opsi Pemutakhiran untuk Windows Server 2012 R2
  - Opsi peningkatan dan konversi untuk Windows Server 2016 dan di atasnya
  - Peningkatan Server Windows
- Kami merekomendasikan untuk melakukan upgrade sistem operasi pada instans dengan setidaknya 2 v CPUs dan 4GB RAM. Jika perlu, Anda dapat mengubah instans ke ukuran yang lebih besar dengan tipe yang sama (misalnya t2.small ke t2.large), melakukan pemutakhiran,

lalu mengubah ukurannya kembali ke ukuran aslinya. Jika Anda diminta untuk mempertahankan ukuran instans, Anda dapat memantau kemajuannya menggunakan tangkapan layar konsol instans. Untuk informasi selengkapnya, lihat Perubahan jenis instans Amazon EC2.

- Verifikasi bahwa volume root pada instans Windows Anda memiliki ruang disk yang cukup. Proses Penataan Windows mungkin tidak memperingatkan Anda tentang ruang disk yang tidak mencukupi. Untuk informasi tentang berapa banyak ruang disk yang diperlukan untuk memutakhirkan sistem operasi tertentu, lihat dokumentasi Microsoft. Jika volume tidak memiliki cukup ruang, volume dapat diperbesar. Untuk informasi selengkapnya, lihat Volume Elastis Amazon EBS di Panduan Pengguna Amazon EBS.
- Tentukan jalur pemutakhiran Anda. Anda harus memutakhirkan sistem operasi ke arsitektur yang sama. Misalnya, Anda harus memutakhirkan sistem 32-bit ke sistem 32-bit. Windows Server 2008 R2 dan setelahnya hanya 64-bit.
- Nonaktifkan perangkat lunak antivirus dan anti-spyware serta firewall. Tipe perangkat lunak ini dapat bertentangan dengan proses pemutakhiran. Aktifkan kembali perangkat lunak antivirus dan anti-spyware serta firewall setelah pemutakhiran versi selesai.
- Perbarui ke driver terbaru seperti yang dijelaskan di Migrasikan instans Windows EC2 ke tipe instans berbasis Nitro.
- Layanan Pembantu Pemutakhiran hanya mendukung instans yang menjalankan driver Citrix PV. Jika instans menjalankan driver Red Hat, Anda harus memutakhirkan driver tersebut secara manual terlebih dahulu.

Tingkatkan instans di tempat dengan AWS PV, Intel Network Adapter, atau driver Enhanced Networking

Gunakan prosedur berikut untuk memutakhirkan instans Windows Server menggunakan AWS PV, Adaptor Jaringan Intel, atau driver jaringan untuk Peningkatan Jaringan.

Untuk melakukan pemutakhiran langsung

1. Buat AMI dari sistem yang Anda rencanakan untuk dimutakhirkan, baik untuk tujuan pencadangan atau pengujian. Anda kemudian dapat melakukan pemutakhiran pada salinan untuk menyimulasikan lingkungan pengujian. Jika pemutakhiran selesai, Anda dapat mengalihkan lalu lintas ke instans ini dengan sedikit waktu henti. Jika pemutakhiran gagal, Anda dapat kembali ke cadangan. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.
2. Pastikan instans Windows Server Anda menggunakan driver jaringan terbaru.

a. Untuk memperbarui driver AWS PV Anda, lihatTingkatkan driver PV pada instans EC2 Windows.

b. Untuk memperbarui driver ENA Anda, lihatInstal driver ENA pada instans EC2 Windows.

c. Untuk memperbarui driver Intel, lihat Jaringan yang disempurnakan dengan antarmuka Intel 82599 VF

3. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

4. Di panel navigasi, pilih Instans. Temukan instans tersebut. Catat ID instans dan Zona Ketersediaan untuk instans tersebut. Anda membutuhkan informasi ini nanti dalam prosedur ini.

5. Jika Anda memutakhirkan dari Windows Server 2012 atau 2012 R2 ke Windows Server 2016 atau yang lebih baru, lakukan hal berikut pada instans Anda sebelum melanjutkan.

   a. Copot pemasangan layanan EC2 Config. Untuk informasi selengkapnya, lihat Administrasi Layanan Windows untuk agen EC2 Launch v2 dan EC2 Config.

   b. Instal EC2 Launch v1 atau agen EC2 Launch v2. Untuk informasi selengkapnya, lihat Gunakan agen EC2launch v1 untuk melakukan tugas selama peluncuran instans Windows EC2 dan Gunakan agen EC2launch v2 untuk melakukan tugas selama peluncuran instans Windows EC2.

   c. Instal Agen AWS Systems Manager SSM. Untuk informasi selengkapnya, lihat Menginstal Agen SSM secara manual di Amazon EC2 untuk Windows Server di Panduan Pengguna AWS Systems Manager .

6. Buat volume baru dari snapshot media instalasi Windows Server.

   a. Di panel navigasi, di bagian Elastic Block Store, pilih Snapshot.

   b. Dari bilah filter, pilih Snapshot publik.

   c. Di bilah pencarian, tentukan filter berikut ini:

      - Pilih Alias Pemilik, lalu =, kemudian amazon.
      - Pilih Deskripsi, lalu mulai mengetik **`Windows`**. Pilih filter Windows yang cocok dengan arsitektur sistem dan preferensi bahasa yang Anda tingkatkan. Misalnya, pilih Media Instalasi Bahasa Inggris Windows 2019 untuk memutakhirkan ke Windows Server 2019.

   d. Pilih kotak centang di samping snapshot yang cocok dengan arsitektur sistem dan preferensi bahasa yang Anda upgrade, lalu pilih Tindakan, Buat volume dari snapshot.

   e. Di halaman Buat volume, pilih Zona Ketersediaan yang cocok dengan instans Windows Anda, dan pilih Buat volume.

7. Di *1234567890example* spanduk volume vol- yang berhasil dibuat di bagian atas halaman, pilih ID volume yang baru saja Anda buat.
8. Pilih Tindakan, Lampirkan Volume.
9. Pada halaman Lampirkan volume, untuk Instans, pilih ID instans dari instans Windows Anda, lalu pilih Lampirkan volume.
10. Buat volume baru tersedia untuk digunakan dengan mengikuti langkah-langkah di Buat volume Amazon EBS tersedia untuk digunakan.

> **Important**
>
> Jangan menginisialisasi disk karena melakukannya akan menghapus data yang ada.

11. Di Windows PowerShell, beralih ke drive volume baru. Mulailah pemutakhiran dengan membuka volume media instalasi yang Anda lampirkan pada instans.

    a. Jika Anda meningkatkan ke Windows Server 2016 atau lebih baru, jalankan perintah berikut:

    ```
    .\setup.exe /auto upgrade /dynamicupdate disable
    ```

    > **Note**
    >
    > Menjalankan setup.exe dengan opsi `/dynamicupdate` yang diatur ke nonaktif akan mencegah Windows menginstal pembaruan selama proses pemutakhiran Windows Server, karena menginstal pembaruan selama pemutakhiran dapat menyebabkan kegagalan. Anda dapat menginstal pembaruan dengan Windows Update setelah pemutakhiran selesai.

    Jika Anda meningkatkan ke Windows Server versi sebelumnya, jalankan perintah berikut:

    ```
    Sources\setup.exe
    ```

    b. Untuk Pilih sistem operasi yang ingin Anda instal, pilih opsi instalasi lengkap untuk instance Windows Server Anda, dan pilih Berikutnya.

    c. Untuk Jenis penginstalan apa yang Anda inginkan?, pilih Pemutakhiran.

    d. Selesaikan wizard.

Windows Server Setup menyalin dan memproses file. Setelah beberapa menit, sesi Remote Desktop Anda ditutup. Waktu yang diperlukan untuk memutakhirkan tergantung pada jumlah aplikasi dan peran server yang berjalan pada instans Windows Server Anda. Proses pemutakhiran dapat memakan waktu sedikitnya 40 menit atau beberapa jam. Instance mungkin gagal satu atau lebih pemeriksaan status selama proses upgrade. Ketika upgrade selesai, semua pemeriksaan status lulus. Anda dapat memeriksa log sistem untuk keluaran konsol atau menggunakan Amazon CloudWatch metrik untuk aktivitas disk dan CPU untuk menentukan apakah peningkatan sedang berlangsung.

> **Note**
>
> Jika memutakhirkan ke Windows Server 2019, setelah pemutakhiran selesai Anda dapat mengubah latar belakang desktop secara manual untuk menghapus nama sistem operasi sebelumnya jika diinginkan.

Jika instance belum lulus semua pemeriksaan status setelah beberapa jam, lihatMemecahkan masalah upgrade sistem operasi pada instans EC2 Windows.

Tugas pasca pemutakhiran

1. Masuk ke instans untuk menginisiasi pemutakhiran untuk .NET Framework dan boot ulang sistem saat diminta.
2. Jika Anda belum melakukannya pada langkah sebelumnya, instal agen EC2 Launch v1 atau EC2 Launch v2. Untuk informasi selengkapnya, lihat Gunakan agen EC2launch v1 untuk melakukan tugas selama peluncuran instans Windows EC2 dan Gunakan agen EC2launch v2 untuk melakukan tugas selama peluncuran instans Windows EC2.
3. Jika Anda memutakhirkan ke Windows Server 2012 R2, kami sarankan Anda meningkatkan driver PV ke driver AWS PV. Jika Anda memutakhirkan pada instans berbasis Nitro, kami menyarankan Anda untuk menginstal atau memutakhirkan driver NVME dan ENA. Untuk informasi selengkapnya, lihat AWS NVMe driver atau Mengaktifkan jaringan yang ditingkatkan di Windows.
4. Aktifkan kembali perangkat lunak antivirus dan anti-spyware serta firewall.

Gunakan runbook Otomasi untuk memutakhirkan instans Windows EC2

Anda dapat melakukan pemutakhiran otomatis instance Windows dan SQL Server Anda AWS dengan runbook AWS Systems Manager Automation.

Daftar Isi

- Layanan terkait
- Opsi eksekusi
- Mutakhirkan Windows Server
- Mutakhirkan SQL Server

Layanan terkait

AWS Layanan berikut digunakan dalam proses peningkatan otomatis:

- AWS Systems Manager. AWS Systems Manager adalah antarmuka yang kuat dan terpadu untuk mengelola sumber daya Anda AWS secara terpusat. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Systems Manager.
- AWS Systems Manager Agen (Agen SSM) adalah perangkat lunak Amazon yang dapat diinstal dan dikonfigurasi pada instans Amazon EC2, server lokal, atau mesin virtual (VM). SSM Agent memungkinkan Systems Manager untuk memperbarui, mengelola, dan mengonfigurasi sumber daya ini. Agen memproses permintaan dari layanan Systems Manager di AWS Cloud, dan kemudian menjalankannya seperti yang ditentukan dalam permintaan. Untuk informasi selengkapnya, lihat Bekerja dengan SSM Agent dalam Panduan Pengguna AWS Systems Manager .
- AWS Systems Manager Runbook SSM. Runbook SSM menentukan tindakan yang dilakukan Systems Manager pada instans yang Anda kelola. Runbook SSM menggunakan JavaScript Object Notation (JSON) atau YAMB, dan menyertakan langkah-langkah dan parameter yang Anda tentukan. Topik ini menggunakan dua runbook SSM Systems Manager untuk otomatisasi. Untuk informasi selengkapnya, lihat Referensi runbook AWS Systems Manager Automation di Panduan Pengguna AWS Systems Manager .

Opsi eksekusi

Saat Anda memilih Otomatisasi di konsol Systems Manager, pilih Jalankan. Setelah Anda memilih dokumen Otomatisasi, Anda akan diminta untuk memilih opsi eksekusi otomatisasi. Anda memilih

dari opsi berikut. Dalam langkah-langkah untuk jalur yang disediakan dalam topik ini nanti, kami menggunakan opsi Eksekusi simpel.

Eksekusi sederhana

Pilih opsi ini jika Anda ingin memperbarui satu instans tetapi tidak ingin melalui setiap langkah otomasi untuk mengaudit hasil. Opsi ini dijelaskan lebih detail dalam langkah-langkah pemutakhiran yang mengikuti.

Kontrol tarif

Pilih opsi ini jika Anda ingin menerapkan pemutakhiran ke lebih dari satu instans. Anda menentukan pengaturan berikut.

- Parameter

  Pengaturan ini, yang juga diatur dalam pengaturan Multiakun dan Wilayah, menentukan bagaimana otomatisasi Anda bercabang.
- Target

  Pilih target yang ingin Anda terapkan otomatisasi. Pengaturan ini juga diatur dalam pengaturan Multiakun dan Wilayah.
- Nilai Parameter

  Gunakan nilai yang ditentukan dalam parameter dokumen otomatisasi.
- Grup Sumber Daya

  Di AWS, sumber daya adalah entitas yang dapat Anda gunakan. Contohnya termasuk instans Amazon EC2, AWS CloudFormation tumpukan, atau bucket Amazon S3. Jika Anda bekerja dengan banyak sumber daya, mungkin berguna untuk mengelolanya sebagai grup daripada berpindah dari satu AWS layanan ke layanan lain untuk setiap tugas. Dalam beberapa kasus, Anda mungkin ingin mengelola sejumlah besar sumber daya terkait, seperti instans EC2 yang membentuk lapisan aplikasi. Dalam kasus ini, Anda mungkin perlu melakukan tindakan massal pada sumber daya ini sekaligus.
- Tanda

  Tag membantu Anda mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Kategorisasi ini berguna jika Anda memiliki banyak sumber daya dengan tipe yang sama. Anda dapat dengan cepat mengidentifikasi sumber daya tertentu menggunakan tanda yang ditetapkan.

- Kontrol Tingkat

  Kontrol Tarif juga diatur dalam pengaturan Multiakun dan Wilayah. Saat Anda menetapkan parameter kontrol tarif, Anda menentukan berapa banyak armada Anda yang akan menerapkan otomatisasi, baik berdasarkan jumlah target maupun persentase armada.

Multiakun dan Wilayah

Selain parameter yang ditentukan dalam Kontrol Tarif yang juga digunakan dalam pengaturan Multiakun dan Wilayah, ada dua pengaturan tambahan:

- Akun dan unit organisasi (OUs)

  Tentukan beberapa akun tempat Anda ingin menjalankan otomatisasi.
- Wilayah AWS

  Tentukan beberapa Wilayah AWS tempat Anda ingin menjalankan otomatisasi.

Eksekusi manual

Opsi ini mirip dengan Eksekusi simpel, tetapi memungkinkan Anda untuk melangkah melalui setiap langkah otomatisasi dan mengaudit hasilnya.

Mutakhirkan Windows Server

Runbook `AWSEC2-CloneInstanceAndUpgradeWindows` membuat Amazon Machine Image (AMI) dari instans Windows Server di akun Anda dan memutakhirkan AMI ini ke versi pilihan Anda yang didukung. Penyelesaian proses multilangkah ini dapat memakan waktu hingga dua jam.

Ada dua yang AMIs termasuk dalam proses upgrade otomatis:

- Instans yang sedang berjalan. AMI pertama adalah instans yang sedang berjalan, yang tidak dimutakhirkan. AMI ini digunakan untuk meluncurkan instans lain untuk menjalankan pemutakhiran langsung. Ketika prosesnya selesai, AMI ini dihapus dari akun, kecuali Anda secara khusus meminta untuk menyimpan instans aslinya. Pengaturan ini ditangani oleh parameter `KeepPreUpgradeImageBackUp` (nilai defaultnya adalah `false`, yang berarti AMI dihapus secara default).
- AMI yang dimutakhirkan. AMI ini adalah hasil dari proses otomasi.

Hasil akhirnya adalah satu AMI, yang merupakan instans AMI yang dimutakhirkan.

Saat pemutakhiran selesai, Anda dapat menguji fungsionalitas aplikasi Anda dengan meluncurkan AMI baru di Amazon VPC Anda. Setelah pengujian, dan sebelum Anda melakukan pemutakhiran lainnya, jadwalkan waktu henti aplikasi sebelum sepenuhnya beralih ke instans yang dimutakhirkan.

Prasyarat

Untuk mengotomatiskan upgrade Windows Server Anda dengan dokumen AWS Systems Manager Otomasi, Anda harus melakukan tugas-tugas berikut:

- Buat peran IAM dengan kebijakan IAM yang ditentukan untuk memungkinkan Systems Manager melakukan tugas otomatisasi pada instans Amazon EC2 Anda dan memastikan Anda memenuhi prasyarat untuk menggunakan Systems Manager. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan di AWS Identity and Access Management Panduan Pengguna.
- Pilih opsi bagaimana Anda ingin otomatisasi dijalankan. Opsi untuk eksekusi adalah Eksekusi simpel, Kontrol nilai, Multiakun dan Wilayah, serta Eksekusi manual. Untuk informasi selengkapnya tentang opsi ini, lihat Opsi eksekusi.
- Pastikan bahwa SSM Agent diinstal pada instans Anda. Untuk informasi selengkapnya, lihat Menginstal dan mengonfigurasi SSM Agent di instans Amazon EC2 untuk Windows Server.
- Windows PowerShell 3.0 atau yang lebih baru harus diinstal pada instans Anda.
- Untuk instans yang bergabung dengan domain Microsoft Active Directory, sebaiknya tentukan `SubnetId` yang tidak memiliki konektivitas ke kontroler domain Anda untuk membantu menghindari konflik nama host.
- Subnet instance harus memiliki konektivitas keluar ke internet, yang menyediakan akses ke Layanan AWS seperti Amazon S3 dan akses untuk mengunduh tambalan dari Microsoft. Persyaratan ini terpenuhi jika subnet adalah subnet publik dan instans memiliki alamat IP publik, atau jika subnet adalah subnet pribadi dengan rute yang mengirimkan lalu lintas internet ke perangkat NAT publik.
- Otomatisasi ini bekerja dengan instans yang menjalankan Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, dan Windows Server 2019.
- Verifikasi bahwa instans memiliki 20 GB ruang disk kosong di disk boot.
- Jika instans tidak menggunakan lisensi Windows yang disediakan oleh AWS, maka tentukan ID snapshot Amazon EBS yang menyertakan media instalasi Windows Server 2012 R2. Untuk melakukannya:

1. Pastikan bahwa instans Amazon EC2 menjalankan Windows Server 2012 atau setelahnya.
2. Buat volume Amazon EBS 6 GB di Zona Ketersediaan yang sama tempat instans berjalan. Lampirkan volume ke instans. Pasang, misalnya, sebagai drive D.
3. Klik kanan ISO dan pasang ke instans sebagai, misalnya, drive E.
4. Salin konten ISO dari drive E:\ ke drive D:\
5. Buat snapshot Amazon EBS dengan volume 6 GB yang dibuat pada langkah 2 di atas.

Batasan pemutakhiran Windows Server

Otomatisasi ini tidak mendukung peningkatan kontroler domain Windows, klaster, atau sistem operasi desktop Windows. Selain itu, otomatisasi ini tidak mendukung instans Amazon EC2 untuk Windows Server dengan peran berikut diinstal:

- Host Sesi Desktop Jarak Jauh (RDSH)
- Broker Koneksi Desktop Jarak Jauh (RDCB)
- Host Virtualisasi Desktop Jarak Jauh (RDVH)
- Akses Web Desktop Jarak Jauh (RDWA)

Langkah-langkah untuk melakukan pemutakhiran otomatis Windows Server

Ikuti langkah-langkah ini untuk memutakhirkan instance Windows Server Anda menggunakan runbook AWSEC2- CloneInstanceAndUpgradeWindows otomatisasi.

1. Buka Systems Manager dari Konsol Manajemen.AWS
2. Dari panel navigasi kiri, pada Pengaturan, pilih Pengaturan.
3. Pilih Eksekusi otomatisasi.
4. Cari dokumen otomatisasi bernama `AWSEC2-CloneInstanceAndUpgradeWindows`.
5. Saat nama dokumen muncul, pilih nama itu. Saat Anda memilihnya, detail dokumen muncul.
6. Pilih Eksekusi otomatisasi untuk memasukkan parameter untuk dokumen ini. Biarkan Eksekusi sederhana dipilih di bagian atas halaman.
7. Masukkan parameter yang diminta berdasarkan panduan berikut.

   - `InstanceID`

     Tipe: String

(Wajib) Instans yang menjalankan Windows Server 2008 R2, 2012 R2, 2016, atau 2019 dengan agen SSM terinstal.

- `InstanceProfile`.

  Tipe: String

  (Wajib) Profil instans IAM. Ini adalah peran IAM yang digunakan untuk melakukan otomatisasi Systems Manager terhadap instans Amazon EC2 dan. AWS AMIs Untuk informasi selengkapnya, lihat Mengonfigurasi izin instans EC2 di AWS Systems Manager Panduan Pengguna.

- `TargetWindowsVersion`

  Tipe: String

  (Wajib) Pilih versi Windows target.

- `SubnetId`

  Tipe: String

  (Wajib) Ini adalah subnet untuk proses pemutakhiran dan tempat instans EC2 sumber Anda berada. Verifikasi bahwa subnet memiliki konektivitas keluar ke AWS layanan, termasuk Amazon S3, dan juga ke Microsoft (untuk mengunduh tambalan).

- `KeepPreUpgradedBackUp`

  Tipe: String

  (Opsional) Jika parameter ini diatur ke `true`, otomatisasi mempertahankan gambar yang dibuat dari instans. Pengaturan default-nya adalah `false`.

- `RebootInstanceBeforeTakingImage`

  Tipe: String

  (Opsional) Default-nya adalah `false` (tanpa reboot). Jika parameter ini disetel ke`true`, Systems Manager melakukan boot ulang pada instans sebelum membuat AMI untuk peningkatan.

8. Setelah Anda memasukkan parameter, pilih Eksekusi. Saat otomatisasi dimulai, Anda dapat memantau kemajuan eksekusi.

9. Saat otomatisasi selesai, Anda akan melihat ID AMI. Anda dapat meluncurkan AMI untuk memverifikasi bahwa OS Windows telah dimutakhirkan.

> **Note**
>
> Tidak perlu otomatisasi untuk menjalankan semua langkah. Langkah-langkahnya bersyarat berdasarkan perilaku otomatisasi dan instans. Systems Manager mungkin melewatkan beberapa langkah yang tidak diperlukan.
> Selain itu, beberapa langkah mungkin kehabisan waktu. Systems Manager mencoba memutakhirkan dan menginstal semua patch terbaru. Namun, terkadang, tambalan waktu habis berdasarkan pengaturan batas waktu yang dapat ditentukan untuk langkah tertentu. Ketika ini terjadi, otomatisasi Systems Manager melanjutkan ke langkah berikutnya untuk memastikan bahwa OS internal dimutakhirkan ke versi Windows Server target.

10. Setelah otomatisasi selesai, Anda dapat meluncurkan instans Amazon EC2 menggunakan ID AMI untuk meninjau pemutakhiran Anda. Untuk informasi selengkapnya tentang cara membuat instans Amazon EC2 dari AWS AMI, lihat Bagaimana cara meluncurkan instans EC2 dari AMI kustom?

Mutakhirkan SQL Server

CloneInstanceAndUpgradeSQLServerSkrip AWSEC2- membuat AMI dari instans Amazon EC2 yang menjalankan SQL Server di akun Anda, dan kemudian memutakhirkan AMI ke versi SQL Server yang lebih baru. Penyelesaian proses multilangkah ini dapat memakan waktu hingga dua jam.

Dalam alur kerja ini, otomatisasi membuat AMI dari instans, lalu meluncurkan AMI baru di subnet yang Anda sediakan. Otomatisasi kemudian melakukan pemutakhiran langsung SQL Server. Setelah pemutakhiran selesai, otomatisasi membuat AMI baru sebelum menghentikan instans yang ditingkatkan.

Ada dua yang AMIs termasuk dalam proses upgrade otomatis:

- Instans yang sedang berjalan. AMI pertama adalah instans yang sedang berjalan, yang tidak dimutakhirkan. AMI ini digunakan untuk meluncurkan instans lain untuk menjalankan pemutakhiran langsung. Ketika prosesnya selesai, AMI ini dihapus dari akun, kecuali Anda secara khusus meminta untuk menyimpan instans aslinya. Pengaturan ini ditangani oleh parameter

`KeepPreUpgradeImageBackUp` (nilai defaultnya adalah `false`, yang berarti AMI dihapus secara default).

- AMI yang dimutakhirkan. AMI ini adalah hasil dari proses otomasi.

Hasil akhirnya adalah satu AMI, yang merupakan instans AMI yang dimutakhirkan.

Saat pemutakhiran selesai, Anda dapat menguji fungsionalitas aplikasi Anda dengan meluncurkan AMI baru di Amazon VPC Anda. Setelah pengujian, dan sebelum Anda melakukan pemutakhiran lainnya, jadwalkan waktu henti aplikasi sebelum sepenuhnya beralih ke instans yang dimutakhirkan.

Prasyarat

Untuk mengotomatiskan peningkatan SQL Server Anda dengan dokumen AWS Systems Manager Otomasi, Anda harus melakukan tugas-tugas berikut:

- Buat peran IAM dengan kebijakan IAM yang ditentukan untuk memungkinkan Systems Manager melakukan tugas otomatisasi pada instans Amazon EC2 Anda dan memastikan Anda memenuhi prasyarat untuk menggunakan Systems Manager. Untuk informasi selengkapnya, silakan lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam AWS Identity and Access Management Panduan pengguna .
- Pilih opsi bagaimana Anda ingin otomatisasi dijalankan. Opsi untuk eksekusi adalah Eksekusi simpel, Kontrol nilai, Multiakun dan Wilayah, serta Eksekusi manual. Untuk informasi selengkapnya tentang opsi ini, lihat Opsi eksekusi.
- Instans Amazon EC2 harus menggunakan Windows Server 2008 R2 atau setelahnya dan SQL Server 2008 atau setelahnya.
- Pastikan bahwa SSM Agent diinstal pada instans Anda. Untuk informasi selengkapnya, lihat Bekerja dengan SSM Agent di instans Amazon EC2 untuk Windows Server.
- Verifikasi bahwa instans memiliki cukup ruang disk:
  - Jika Anda memutakhirkan dari Windows Server 2008 R2 ke 2012 R2, atau dari Windows Server 2012 R2 ke sistem operasi yang lebih baru, verifikasi bahwa Anda memiliki 20 GB ruang disk kosong di disk boot instans.
  - Jika Anda memutakhirkan dari Windows Server 2008 R2 ke 2016 atau versi lebih baru, verifikasi bahwa instans memiliki 40 GB ruang disk kosong di disk boot instans.
- Untuk instans yang menggunakan versi SQL Server Bawa Lisensi Sendiri (BYOL), prasyarat tambahan berikut ini berlaku:

- Berikan ID snapshot Amazon EBS yang menyertakan media instalasi SQL Server target. Untuk melakukannya:
  1. Verifikasi bahwa instans Amazon EC2 menjalankan Windows Server 2008 R2 atau setelahnya.
  2. Buat volume Amazon EBS 6 GB di Zona Ketersediaan yang sama tempat instans berjalan. Lampirkan volume ke instans. Pasang, misalnya, sebagai drive D.
  3. Klik kanan ISO dan pasang ke instans sebagai, misalnya, drive E.
  4. Salin konten ISO dari drive E:\ ke drive D:\
  5. Buat snapshot Amazon EBS dengan volume 6 GB yang dibuat pada langkah 2.

Batasan pemutakhiran otomatis SQL Server

Batasan berikut berlaku saat menggunakan AWSEC2- CloneInstanceAndUpgrade SQLServer runbook untuk melakukan peningkatan otomatis:

- Pemutakhiran dapat dilakukan hanya pada SQL Server menggunakan autentikasi Windows.
- Verifikasi bahwa tidak ada pembaruan patch keamanan yang tertunda pada instans. Buka Panel Kontrol, lalu pilih Periksa pembaruan.
- Penerapan SQL Server dalam mode HA dan mirroring tidak didukung.

Langkah-langkah untuk melakukan pemutakhiran otomatis SQL Server

Ikuti langkah-langkah ini untuk meningkatkan SQL Server Anda menggunakan runbook AWSEC2-CloneInstanceAndUpgrade SQLServer otomatisasi.

1. Jika Anda belum melakukannya, unduh file.iso SQL Server 2016 dan pasang ke server sumber.
2. Setelah file .iso dipasang, salin semua file komponen dan letakkan di volume apa pun pilihan Anda.
3. Ambil snapshot volume Amazon EBS dan salin ID snapshot ke clipboard untuk digunakan nanti. Untuk informasi selengkapnya, lihat Membuat snapshot Amazon EBS di Panduan Pengguna Amazon EBS.
4. Lampirkan profil instans ke instans sumber Amazon EC2. Hal ini memungkinkan Systems Manager untuk berkomunikasi dengan instans EC2 dan menjalankan perintah di atasnya setelah ditambahkan ke AWS Systems Manager layanan. Untuk contoh ini, kami menamai peran

tersebut `SSM-EC2-Profile-Role` dengan kebijakan `AmazonSSMManagedInstanceCore` yang dilampirkan pada peran tersebut.

5. Di AWS Systems Manager konsol, di panel navigasi kiri, pilih Instans Terkelola. Verifikasi bahwa instans EC2 Anda ada dalam daftar instans terkelola. Jika Anda tidak melihat instans Anda setelah beberapa menit, lihat Di Mana Instans Saya? di Panduan Pengguna AWS Systems Manager .
6. Dari panel navigasi kiri, pada Manajemen Perubahan, pilih Otomatisasi.
7. Pilih Eksekusi otomatisasi.
8. Cari dokumen otomatisasi bernama `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Pilih tombol dokumen `AWSEC2-CloneInstanceAndUpgradeSQLServer` SSM, lalu pilih Berikutnya.
10. Pastikan opsi Eksekusi simpel dipilih.
11. Masukkan parameter yang diminta berdasarkan panduan berikut.

    - `InstanceId`

      Tipe: String

      (Wajib) Instans yang menjalankan SQL Server 2008 R2 (atau setelahnya).

    - `IamInstanceProfile`

      Tipe: String

      (Wajib) Profil instans IAM.

    - `SQLServerSnapshotId`

      Tipe: String

      (Wajib) ID Snapshot untuk media penginstalan SQL Server target. Parameter ini tidak diperlukan untuk instans yang disertakan lisensi SQL Server.

    - `SubnetId`

      Tipe: String

      (Wajib) Ini adalah subnet untuk proses pemutakhiran dan tempat instans EC2 sumber Anda berada. Verifikasi bahwa subnet memiliki konektivitas keluar ke AWS layanan, termasuk Amazon S3, dan juga ke Microsoft (untuk mengunduh tambalan).

- `KeepPreUpgradedBackUp`

  Tipe: String

  (Opsional) Jika parameter ini diatur ke `true`, otomatisasi mempertahankan gambar yang dibuat dari instans. Pengaturan default-nya adalah `false`.

- `RebootInstanceBeforeTakingImage`

  Tipe: String

  (Opsional) Default-nya adalah `false` (tanpa reboot). Jika parameter ini atur ke `true`, Systems Manager melakukan boot ulang pada instans sebelum membuat AMI untuk peningkatan.

- `TargetSQLVersion`

  Tipe: String

  (Opsional) Versi SQL Server target. Nilai default-nya `2016`.

12. Setelah Anda memasukkan parameter, pilih Eksekusi. Saat otomatisasi dimulai, Anda dapat memantau kemajuan eksekusi.
13. Ketika Status eksekusi menunjukkan Berhasil, luaskan Output untuk melihat informasi AMI. Anda dapat menggunakan AMI ID untuk meluncurkan instans SQL Server untuk VPC pilihan Anda.
14. Buka konsol Amazon EC2. Di panel navigasi kiri, pilih AMIs. Anda akan melihat AMI baru.
15. Untuk memverifikasi bahwa versi SQL Server yang baru telah berhasil diinstal, pilih AMI baru dan pilih Luncurkan.
16. Pilih tipe instans yang Anda inginkan untuk AMI, VPC dan subnet yang ingin Anda deploy, dan penyimpanan yang ingin Anda gunakan. Karena Anda meluncurkan instans baru dari AMI, volume disajikan kepada Anda sebagai opsi untuk disertakan dalam instans EC2 baru yang Anda luncurkan. Anda dapat menghapus salah satu volume ini, atau Anda dapat menambahkan volume.
17. Tambahkan tanda untuk membantu Anda mengidentifikasi instans Anda.
18. Tambahkan grup keamanan atau grup ke instans.
19. Pilih Luncurkan Instans.
20. Pilih nama tanda untuk instans tersebut dan pilih Hubungkan di bawah menu tarik-turun Tindakan.
21. Verifikasi bahwa versi SQL Server baru adalah mesin basis data pada instans baru.

Migrasikan instans Windows EC2 ke tipe instans berbasis Nitro

AWS Windows AMIs dikonfigurasi dengan pengaturan default yang digunakan oleh media instalasi Microsoft, dengan beberapa penyesuaian. Kustomisasi mencakup driver dan konfigurasi yang mendukung instans berbasis Nitro, seperti M5 dan C5.

Saat bermigrasi dari instance berbasis Xen ke instans berbasis Nitro, termasuk instans bare metal, sebaiknya ikuti langkah-langkah dalam topik ini dalam kasus berikut:

- Jika Anda meluncurkan instance dari Windows khusus AMIs
- Jika Anda meluncurkan instance dari Windows yang AMIs disediakan oleh Amazon yang dibuat sebelum Agustus 2018

Atau, Anda dapat menggunakan dokumen otomatisasi `AWSSupport-UpgradeWindowsAWSDrivers` untuk mengotomatisasi prosedur yang dijelaskan di Bagian 1, Bagian 2, dan Bagian 3. Jika Anda memilih untuk menggunakan prosedur otomatis, lihat (Alternatif) Tingkatkan AWS PV, ENA, dan NVMe driver menggunakan AWS Systems Manager, lalu lanjutkan dengan Bagian 4 dan Bagian 5.

Untuk informasi selengkapnya, lihat Pembaruan Amazon EC2 - Tipe Instans Tambahan, Nitro System, dan Opsi CPU.

> **Note**
>
> Prosedur migrasi berikut dapat dilakukan pada Windows Server versi 2016 dan yang lebih baru. Versi sistem operasi sebelumnya yang telah mencapai akhir masa pakai tidak diuji, dan mungkin tidak kompatibel dengan jenis instance terbaru.
> Untuk memigrasikan instance Linux, lihat. the section called “Perubahan jenis instans”

Daftar Isi

- Bagian 1: Instal dan tingkatkan driver AWS PV
- Bagian 2: Instal dan mutakhirkan ENA
- Bagian 3: Tingkatkan AWS NVMe driver
- Bagian 4: Perbarui EC2 Config dan Luncurkan EC2
- Bagian 5: Instal driver port serial untuk instans bare metal

- Bagian 6: Perbarui pengaturan manajemen daya
- Bagian 7: Perbarui driver chipset Intel untuk tipe instans baru
- (Alternatif) Tingkatkan AWS PV, ENA, dan NVMe driver menggunakan AWS Systems Manager

Sebelum Anda memulai

Prosedur ini mengasumsikan bahwa Anda memiliki instance berbasis Xen, seperti M4 atau C4, dan Anda bermigrasi ke instans berbasis Nitro.

Anda harus menggunakan PowerShell versi 3.0 atau yang lebih baru untuk berhasil melakukan upgrade.

> **Note**
>
> Saat bermigrasi, IP statis atau pengaturan jaringan DNS khusus pada kartu antarmuka jaringan yang ada mungkin hilang karena instance akan default ke perangkat Adaptor Jaringan yang Ditingkatkan yang baru.

Sebelum mengikuti langkah-langkah dalam prosedur ini, kami menyarankan Anda untuk membuat cadangan instans. Dari konsol EC2, pilih instans yang memerlukan migrasi, buka menu konteks (klik kanan), dan pilih Status Instans, Berhenti.

> **Warning**
>
> Ketika Anda menghentikan instans, data pada setiap volume penyimpanan instans akan dihapus. Untuk menyimpan data dalam volume penyimpanan instan, pastikan Anda mencadangkan data ke penyimpanan persisten.

Buka menu konteks (klik kanan) untuk instans di konsol EC2, pilih Gambar, lalu pilih Buat Gambar.

> **Note**
>
> Bagian 4 dan 5 dari instruksi ini dapat diselesaikan setelah Anda memigrasi atau mengubah jenis instans. Namun, sebaiknya Anda menyelesaikannya sebelum bermigrasi, terutama jika Anda bermigrasi ke tipe instans bare metal.

Bagian 1: Instal dan tingkatkan driver AWS PV

Meskipun driver AWS PV tidak digunakan dalam sistem Nitro, Anda masih harus memutakhirkannya jika Anda menggunakan versi sebelumnya dari Citrix PV atau PV. AWS Driver AWS PV terbaru menyelesaikan masalah bug di versi driver sebelumnya yang mungkin muncul saat Anda menggunakan sistem Nitro, atau jika Anda perlu bermigrasi kembali ke instans berbasis Xen. Sebagai praktik terbaik, kami sarankan untuk selalu memperbarui ke driver terbaru untuk instance Windows. AWS

Gunakan prosedur berikut untuk melakukan peningkatan driver AWS PV di tempat, atau untuk meningkatkan dari driver Citrix PV ke driver AWS PV pada Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, atau Windows Server 2019. Untuk informasi selengkapnya, lihat Tingkatkan driver PV pada instans EC2 Windows.

Untuk memutakhirkan Kontroler Domain, lihat Tingkatkan pengontrol domain (peningkatan AWS PV).

Untuk melakukan upgrade atau ke driver AWS PV

1. Hubungkan ke instans menggunakan Desktop Jarak Jauh dan persiapkan instans untuk pemutakhiran. Buat semua disk non-sistem offline sebelum Anda melakukan pemutakhiran. Jika Anda melakukan pembaruan driver AWS PV di tempat, langkah ini tidak diperlukan. Setel layanan yang tidak penting ke Pengaktifan manual di konsol Layanan.
2. Unduh paket driver terbaru ke instans.
3. Ekstrak isi folder dan jalankan `AWSPVDriverSetup.msi`.

Setelah menjalankan MSI, instans secara otomatis melakukan boot ulang dan memutakhirkan driver. Instans mungkin tidak tersedia hingga 15 menit.

Setelah peningkatan selesai dan instans lulus pada pemeriksaan kondisi di konsol Amazon EC2, hubungkan ke instans menggunakan Desktop Jarak Jauh dan pastikan driver baru terinstal. Di Pengelola Perangkat, di bawah Kontroler Penyimpanan, temukan Adaptor Host Penyimpanan AWS PV. Pastikan versi driver sama dengan versi terbaru yang terdaftar pada tabel Riwayat Versi Driver. Untuk informasi selengkapnya, lihat AWS Riwayat paket driver PV.

Bagian 2: Instal dan mutakhirkan ENA

Mutakhirkan ke driver Adaptor Jaringan Elastis terbaru untuk memastikan bahwa semua fitur jaringan didukung. Jika Anda meluncurkan instans dan jaringan yang ditingkatkan belum diaktifkan, Anda harus mengunduh dan menginstal driver adaptor jaringan yang diperlukan pada instans Anda.

Kemudian, setel atribut instans enaSupport untuk mengaktifkan jaringan yang ditingkatkan. Anda hanya dapat mengaktifkan atribut ini pada tipe instans yang didukung dan hanya jika driver ENA diinstal. Untuk informasi selengkapnya, lihat Aktifkan jaringan yang disempurnakan dengan ENA pada instans EC2 Anda.

1. Unduh driver terbaru ke instans. Jika Anda memerlukan versi driver sebelumnya, lihatRiwayat versi driver ENA Windows.
2. Ekstrak arsip zip.
3. Instal driver dengan menjalankan `install.ps1` PowerShell skrip dari folder yang diekstraksi.

> **Note**
>
> Untuk menghindari kesalahan penginstalan, jalankan`install.ps1` skrip sebagai administrator.

4. Periksa apakah AMI Anda telah mengaktifkan enaSupport. Jika tidak, lanjutkan dengan mengikuti dokumentasi di Aktifkan jaringan yang disempurnakan dengan ENA pada instans EC2 Anda.

Bagian 3: Tingkatkan AWS NVMe driver

AWS NVMe driver digunakan untuk berinteraksi dengan Amazon EBS dan volume penyimpanan instans SSD yang diekspos sebagai perangkat NVMe blok dalam sistem Nitro untuk kinerja yang lebih baik.

> **Important**
>
> Instruksi berikut dimodifikasi secara khusus ketika Anda menginstal atau AWS NVMe memutakhirkan instans berbasis Xen dengan maksud untuk memigrasikan instance ke instance berbasis Nitro.

1. Unduh paket driver terbaru ke instans.

   Jika Anda memerlukan versi driver sebelumnya, lihat NVMe Rilis driver Windows untuk versi yang didukung.
2. Ekstrak arsip zip.

3. Instal driver seperti yang dijelaskan dalam`Readme.txt`.
4. Buka PowerShell dan jalankan perintah berikut:

```
PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

> **Note**
>
> Untuk menerapkan perintah, Anda harus menjalankan PowerShell sesi sebagai administrator. PowerShell (x86) versi akan menghasilkan kesalahan.
> Perintah ini hanya menjalankan sysprep pada driver perangkat. Itu tidak menjalankan persiapan sysprep lengkap.

5. Untuk Windows Server 2008 R2 dan Windows Server 2012, matikan instance, ubah jenis instance dan mulai instance, lalu lanjutkan ke Bagian 4. Jika Anda memulai instance lagi pada tipe instance berbasis Xen sebelum bermigrasi ke tipe instance berbasis Nitro, instance tidak akan bisa boot. Untuk Windows lain yang didukung AMIs, Anda dapat mengubah jenis instans kapan saja setelah sysprep perangkat.

Bagian 4: Perbarui EC2 Config dan Luncurkan EC2

Untuk instans Windows, utilitas EC2Config dan EC2Launch terbaru menyediakan fungsionalitas dan informasi tambahan saat dijalankan pada sistem Nitro, termasuk pada EC2 Bare Metal. Secara default, layanan EC2 Config disertakan AMIs sebelum Windows Server 2016. EC2Peluncuran menggantikan EC2 Config pada Windows Server 2016 dan yang lebih baru. AMIs

Ketika layanan EC2 Config dan EC2 Launch diperbarui, Windows baru AMIs dari AWS menyertakan versi terbaru dari layanan. Namun, Anda harus memperbarui Windows AMIs dan instance Anda sendiri dengan EC2 Config EC2 dan Launch versi terbaru.

Untuk menginstal atau memperbarui EC2 Config

1. Unduh dan unzip EC2Config Installer.
2. Jalankan `EC2Install.exe`. Untuk daftar lengkap opsi, jalankan `EC2Install` dengan opsi `/?`. Secara default, penyiapan menampilkan perintah. Untuk menjalankan perintah tanpa prompt, gunakan opsi `/quiet`.

Untuk informasi selengkapnya, lihat Instal EC2 Config versi terbaru.

Untuk menginstal atau memperbarui EC2 Peluncuran

1. Jika Anda telah menginstal dan mengkonfigurasi EC2 Launch pada sebuah instance, buat cadangan file konfigurasi EC2 Launch. Proses penginstalan tidak menyimpan perubahan dalam file ini. Secara default, file terletak di direktori `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Unduh EC2-Windows-Launch.zip ke direktori pada instans.
3. Unduh install.ps1 ke direktori yang sama tempat Anda mengunduh `EC2-Windows-Launch.zip`.
4. Jalankan `install.ps1`.

> **Note**
>
> Untuk menghindari kesalahan penginstalan, jalankan skrip `install.ps1` sebagai administrator.

5. Jika Anda membuat cadangan file konfigurasi EC2 Launch, salin ke `C:\ProgramData\Amazon\EC2-Windows\Launch\Config` direktori.

Untuk informasi selengkapnya, lihat Gunakan agen EC2launch v1 untuk melakukan tugas selama peluncuran instans Windows EC2.

Bagian 5: Instal driver port serial untuk instans bare metal

Jenis `i3.metal` instans menggunakan perangkat serial berbasis PCI daripada perangkat serial I/O berbasis port. AMI Windows terbaru secara otomatis menggunakan perangkat serial berbasis PCI dan menginstal driver port serial. Jika Anda tidak menggunakan instans yang diluncurkan dari AMI Windows yang disediakan Amazon tertanggal 2018.04.11 atau lebih baru, Anda harus menginstal Driver Port Serial untuk mengaktifkan perangkat serial untuk fitur EC2 seperti Pembuatan Kata Sandi dan Output Konsol. Utilitas EC2 Config dan EC2 Launch terbaru juga mendukung i3.metal dan menyediakan fungsionalitas tambahan. Ikuti langkah-langkah di Bagian 4, jika Anda belum melakukannya.

Untuk menginstal driver port serial

1. Unduh paket driver serial ke instans.
2. Ekstrak konten folder, buka menu konteks (klik kanan) untuk, `aws_ser.INF`dan pilih instal.

3. Pilih Oke.

Bagian 6: Perbarui pengaturan manajemen daya

Pembaruan berikut untuk pengaturan manajemen daya mengatur tampilan ke tidak pernah mati, yang memungkinkan pematian terkontrol OS pada sistem Nitro. Semua Windows AMIs disediakan oleh Amazon pada 2018.11.28 sudah memiliki konfigurasi default ini.

1. Buka prompt perintah atau PowerShell sesi.
2. Jalankan perintah berikut:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Bagian 7: Perbarui driver chipset Intel untuk tipe instans baru

Jenisu-6tb1.metal,u-9tb1.metal, dan u-12tb1.metal instance menggunakan perangkat keras yang membutuhkan driver chipset yang sebelumnya tidak diinstal pada Windows AMIs. Jika Anda tidak menggunakan instans yang diluncurkan dari AMI Windows yang disediakan Amazon tertanggal 2018.11.19 atau setelahnya, maka Anda harus menginstal driver menggunakan Intel Chipset INF Utility.

Untuk menginstal driver chipset

1. Chipset INF Utility untuk instance.
2. Ekstrak file.
3. Jalankan SetupChipset.exe.
4. Terima perjanjian lisensi perangkat lunak Intel dan instal driver chipset.
5. Boot ulang instans.

(Alternatif) Tingkatkan AWS PV, ENA, dan NVMe driver menggunakan AWS Systems Manager

Dokumen otomatisasi `AWSSupport-UpgradeWindowsAWSDrivers` mengotomatisasi langkah-langkah yang dijelaskan di Bagian 1, Bagian 2, dan Bagian 3. Metode ini juga dapat memperbaiki instans di mana pemutakhiran driver gagal.

Dokumen `AWSSupport-UpgradeWindowsAWSDrivers` otomatisasi meningkatkan atau memperbaiki penyimpanan dan AWS driver jaringan pada instans EC2 yang ditentukan. Dokumen ini mencoba menginstal versi terbaru AWS driver online dengan menghubungi AWS Systems Manager Agen (Agen SSM). Jika Agen SSM tidak dapat dihubungi, dokumen dapat melakukan instalasi offline AWS driver jika diminta secara eksplisit.

> **Note**
>
> Prosedur ini akan gagal pada kontroler domain. Untuk memperbarui driver pada kontroler domain, lihat Tingkatkan pengontrol domain (peningkatan AWS PV).

Untuk secara otomatis meng-upgrade AWS PV, ENA, dan NVMe driver menggunakan AWS Systems Manager

1. Buka konsol Systems Manager di https://console.aws.amazon.com/systems-manager.
2. Pilih Otomasi, Eksekusi Otomasi.
3. Cari dan kemudian pilih dokumen AWSSupport-UpgradeWindowsAWSDriversotomatisasi, lalu pilih Jalankan otomatisasi.
4. Di bagian Parameter Input, konfigurasikan opsi berikut:

   ID Instans

   Masukkan ID unik dari instance yang akan ditingkatkan.

   AllowOffline

   (Opsional) Pilih salah satu opsi berikut:

   - `True` — Pilih opsi ini untuk melakukan penginstalan offline. Instans dihentikan dan dimulai ulang selama proses pemutakhiran.

> **Warning**
>
> Ketika Anda menghentikan instans, data pada setiap volume penyimpanan instans akan dihapus. Untuk menyimpan data dalam volume penyimpanan instan, pastikan Anda mencadangkan data ke penyimpanan persisten.

- `False` — (Default) Untuk melakukan penginstalan online, biarkan opsi ini dipilih. Instans dimulai ulang selama proses pemutakhiran.

> **Important**
>
> Pemutakhiran online dan offline membuat AMI sebelum mencoba operasi pemutakhiran. AMI tetap ada setelah otomatisasi selesai. Amankan akses Anda ke AMI, atau hapus jika tidak lagi diperlukan.

SubnetId

(Opsional) Masukkan salah satu nilai berikut:

- `SelectedInstanceSubnet` — (Default) Proses pemutakhiran meluncurkan instans helper ke subnet yang sama dengan instans yang akan dimutakhirkan. Subnet harus mengizinkan komunikasi ke titik akhir Systems Manager (`ssm.*`).
- `CreateNewVPC` — Proses pemutakhiran meluncurkan instans pembantu menjadi VPC baru. Gunakan opsi ini jika Anda tidak yakin apakah subnet instans target mengizinkan komunikasi ke titik akhir `ssm.*`. Pengguna Anda harus memiliki izin untuk membuat VPC.
- ID subnet tertentu — Tentukan ID subnet tertentu yang akan digunakan untuk meluncurkan instans helper. Subnet harus berada di Zona Ketersediaan yang sama dengan instans yang akan dimutakhirkan, dan harus mengizinkan komunikasi dengan titik akhir `ssm.*`.

5. Pilih Eksekusi.
6. Izinkan pemutakhiran selesai. Diperlukan waktu hingga 10 menit untuk menyelesaikan pemutakhiran secara online, dan hingga 25 menit untuk menyelesaikan pemutakhiran secara offline.

Memecahkan masalah upgrade sistem operasi pada instans EC2 Windows

AWS menyediakan dukungan upgrade untuk masalah atau masalah dengan Upgrade Helper Service, sebuah AWS utilitas yang membantu Anda melakukan upgrade di tempat yang melibatkan driver Citrix PV.

Setelah pemutakhiran, instans mungkin untuk sementara mengalami penggunaan CPU yang lebih tinggi dari rata-rata sementara layanan .NET Runtime Optimization mengoptimalkan kerangka kerja .NET. Ini adalah perilaku yang diharapkan.

Jika instance belum lulus semua pemeriksaan status setelah beberapa jam, periksa yang berikut ini.

- Jika Anda memutakhirkan ke Windows Server 2008 dan semua pemeriksaan status gagal setelah beberapa jam, pemutakhiran mungkin gagal dan menampilkan prompt untuk Klik OK untuk mengonfirmasi pemutaran kembali. Karena konsol tidak dapat diakses pada status ini, tombol tersebut tidak dapat diklik Untuk menyiasatinya, lakukan boot ulang melalui konsol atau API Amazon EC2. Boot ulang membutuhkan waktu sepuluh menit atau lebih untuk memulai. Instans mungkin tersedia setelah 25 menit.
- Hapus aplikasi atau peran server dari server dan coba lagi.

Jika instance tidak lulus semua pemeriksaan status setelah menghapus aplikasi atau peran server dari server, lakukan hal berikut.

- Hentikan instans dan lampirkan volume root ke instans lain. Untuk informasi selengkapnya, lihat penjelasan cara menghentikan dan melampirkan volume root ke instans lain di “Menunggu layanan metadata”.
- Menganalisis file log Windows Setup dan log peristiwa untuk kegagalan.

Untuk isu atau masalah lain tekait pemutakhiran atau migrasi sistem operasi, sebaiknya tinjau artikel yang tercantum di Sebelum Anda memulai pemutakhiran langsung.

Tutorial: Hubungkan instans Amazon EC2 ke basis data Amazon RDS

Tujuan Tutorial

Tujuan dari tutorial ini adalah untuk mempelajari cara mengonfigurasi koneksi aman antara instans Amazon EC2 dan basis data Amazon RDS dengan menggunakan Konsol Manajemen AWS.

Ada berbagai opsi untuk mengonfigurasi koneksi. Dalam tutorial ini, kami mengeksplorasi tiga opsi berikut ini:

- Opsi 1: Secara otomatis menghubungkan instance ke database RDS menggunakan konsol EC2

  Gunakan fitur koneksi otomatis di konsol EC2 untuk secara otomatis mengonfigurasi koneksi antara instans EC2 dan basis data RDS Anda untuk memungkinkan lalu lintas antara instans EC2 dan basis data RDS.
- Opsi 2: Secara otomatis menghubungkan instance ke database RDS menggunakan konsol RDS

  Gunakan fitur koneksi otomatis di konsol RDS untuk secara otomatis mengonfigurasi koneksi antara instans EC2 dan basis data RDS Anda untuk memungkinkan lalu lintas antara instans EC2 dan basis data RDS.
- Opsi 3: Hubungkan instance secara manual ke database RDS dengan membuat grup keamanan

  Konfigurasikan koneksi antara instans EC2 Anda ke basis data RDS Anda dengan mengonfigurasi dan menetapkan grup keamanan secara manual untuk mereproduksi konfigurasi yang secara otomatis dibuat oleh fitur koneksi otomatis di Opsi 1 dan Opsi 2.

Konteks

Sebagai konteks mengapa Anda harus mengonfigurasi koneksi antara instans EC2 Anda dan basis data RDS, mari pertimbangkan skenario berikut: Situs web Anda menyajikan formulir kepada pengguna Anda untuk diisi. Anda perlu menangkap data formulir dalam basis data. Anda dapat meng-hosting situs web Anda pada instans EC2 yang telah dikonfigurasi sebagai server web, dan Anda dapat menangkap data formulir dalam basis data RDS. Instans EC2 dan basis data RDS harus terhubung satu sama lain sehingga data formulir dapat keluar dari instans EC2 menuju basis data RDS. Tutorial ini menjelaskan cara mengonfigurasi koneksi itu. Perhatikan bahwa ini hanyalah salah satu contoh kasus penggunaan untuk menghubungkan instans EC2 dan basis data RDS.

Arsitektur

Diagram berikut menunjukkan sumber daya yang dibuat dan konfigurasi arsitektur yang dihasilkan dari menyelesaikan semua langkah dalam tutorial ini.

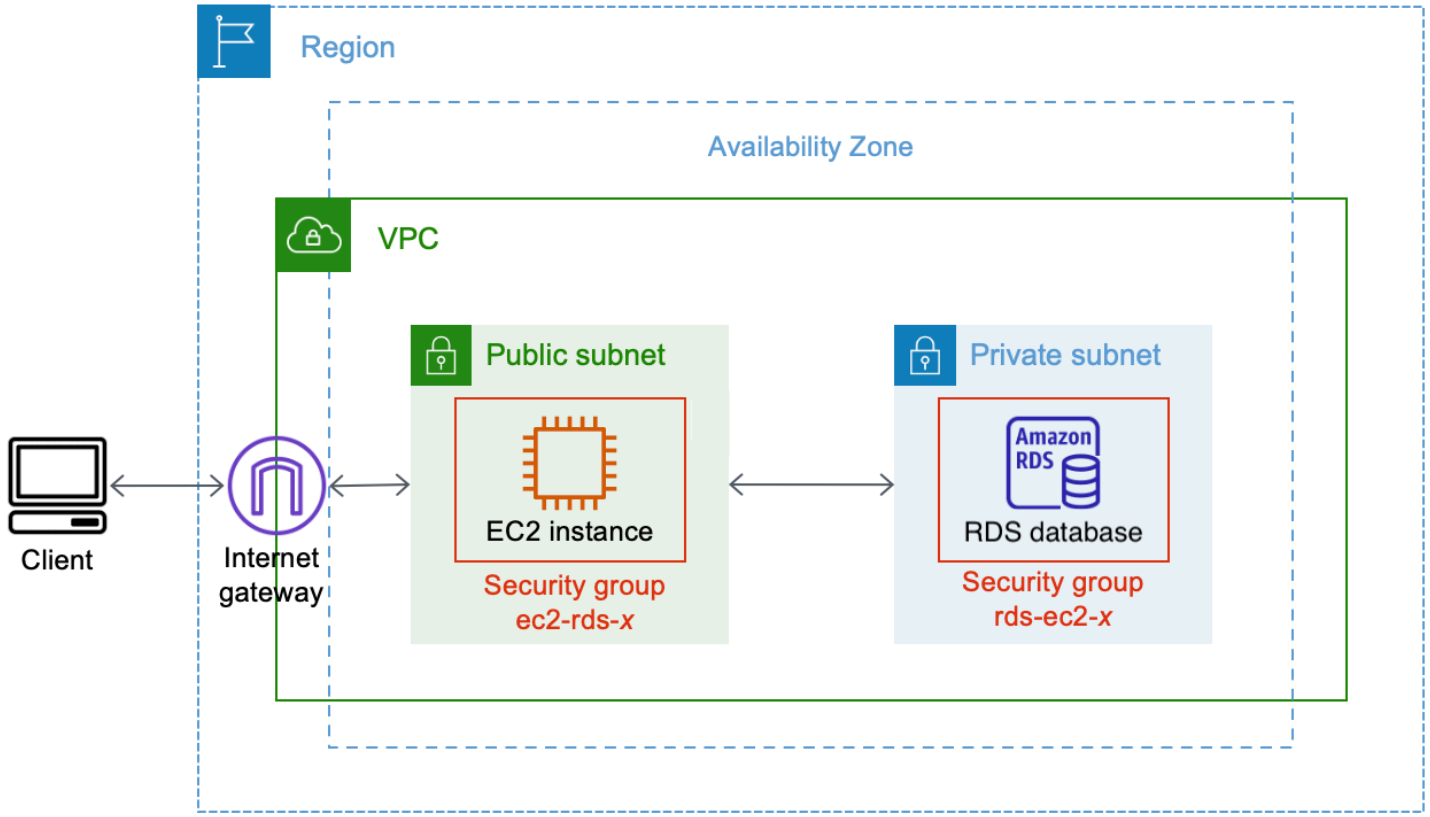


Diagram ini menggambarkan sumber daya berikut yang akan Anda buat:

- Anda akan membuat instans EC2 dan database RDS di AWS Region VPC, dan Availability Zone yang sama.
- Anda akan membuat instans EC2 di subnet publik.
- Anda akan membuat basis data RDS di subnet privat.

  Saat Anda menggunakan konsol RDS untuk membuat basis data RDS dan secara otomatis menghubungkan instans EC2, VPC, grup subnet DB, dan pengaturan akses publik untuk basis data dipilih secara otomatis. Basis data RDS secara otomatis dibuat dalam subnet privat dalam VPC yang sama dengan instans EC2.
- Pengguna internet dapat terhubung ke instans EC2 dengan menggunakan SSH atau HTTP/HTTPS melalui gateway Internet.

- Pengguna internet tidak dapat terhubung langsung ke basis data RDS; hanya instans EC2 yang terhubung ke basis data RDS.
- Saat Anda menggunakan fitur koneksi otomatis untuk mengizinkan lalu lintas antara instans EC2 dan basis data RDS, grup keamanan berikut secara otomatis dibuat dan ditambahkan:
  - Grup keamanan ec2-rds- ***x*** dibuat dan ditambahkan ke instans EC2. Ini memiliki satu aturan keluar yang merujuk grup *x* keamanan rds-ec2- sebagai tujuannya. Ini memungkinkan lalu lintas dari instans EC2 untuk mencapai database RDS dengan grup keamanan rds-ec2 -. *x*
  - Grup keamanan rds-ec2- ***x*** dibuat dan ditambahkan ke database RDS. Ini memiliki satu aturan masuk yang merujuk kelompok *x* keamanan ec2-rds sebagai sumbernya. Ini memungkinkan lalu lintas dari instans EC2 dengan grup *x* keamanan ec2-rds- untuk mencapai database RDS.

  Dengan grup keamanan terpisah (satu untuk instans EC2, dan satu untuk basis data RDS), Anda memiliki kontrol yang lebih baik atas keamanan instans dan basis data. Jika Anda menggunakan grup keamanan yang sama pada instans dan basis data, kemudian memodifikasi grup keamanan agar sesuai dengan, katakanlah, hanya basis data, modifikasi akan memengaruhi instans dan basis data. Dengan kata lain, jika Anda menggunakan satu grup keamanan, Anda dapat secara tidak sengaja memodifikasi keamanan sumber daya (baik instans atau basis data) karena Anda lupa bahwa grup keamanan telah dilampirkan padanya.

  Grup keamanan yang dibuat secara otomatis juga menghormati hak akses paling rendah karena mereka hanya mengizinkan koneksi timbal balik untuk beban kerja ini pada port basis data dengan membuat pasangan grup keamanan yang spesifik beban kerja.

Pertimbangan-pertimbangan

Pertimbangkan hal-hal berikut saat Anda menyelesaikan tugas dalam tutorial ini:

- Dua konsol – Anda akan menggunakan dua konsol berikut untuk tutorial ini:
  - Konsol Amazon EC2 — Anda akan menggunakan konsol EC2 untuk meluncurkan instans, untuk secara otomatis menghubungkan instans EC2 ke basis data RDS, dan sebagai opsi manual untuk mengonfigurasi koneksi dengan membuat grup keamanan.
  - Konsol Amazon RDS — Anda akan menggunakan konsol RDS untuk membuat basis data RDS dan menghubungkan instans EC2 secara otomatis ke basis data RDS.
- Satu VPC — Untuk menggunakan fitur koneksi otomatis, instans EC2 dan basis data RDS Anda harus berada dalam VPC yang sama.

Jika Anda secara manual mengonfigurasi koneksi antara instans EC2 dan basis data RDS, Anda dapat meluncurkan instans EC2 dalam satu VPC dan basis data RDS Anda di VPC lain; namun, Anda perlu menyiapkan perutean tambahan dan konfigurasi VPC. Skenario ini tidak dibahas dalam tutorial ini.

- Satu AWS Region — Instans EC2 dan database RDS harus terletak di Wilayah yang sama.
- Dua grup keamanan – Konektivitas antara instans EC2 dan basis data RDS dikonfigurasikan oleh dua grup keamanan—grup keamanan untuk instans EC2 Anda dan grup keamanan untuk basis data RDS.

  Saat Anda menggunakan fitur koneksi otomatis di konsol EC2 atau konsol RDS untuk mengonfigurasi konektivitas (Opsi 1 dan Opsi 2 tutorial ini), grup keamanan secara otomatis dibuat dan ditetapkan ke instans EC2 dan basis data RDS.

  Jika Anda tidak menggunakan fitur koneksi otomatis, Anda harus membuat dan menetapkan grup keamanan secara manual. Anda melakukan ini di Opsi 3 dari tutorial ini.

Waktu untuk menyelesaikan tutorial

30 menit

Anda dapat menyelesaikan seluruh tutorial dalam sekali duduk, atau Anda dapat menyelesaikan tugas satu per satu.

Biaya

Dengan menyelesaikan tutorial ini, Anda mungkin dikenakan biaya untuk AWS sumber daya yang Anda buat.

Anda dapat menggunakan Amazon EC2 di bawah Tingkat Gratis asalkan AWS akun Anda memenuhi syarat untuk Tingkat Gratis dan Anda mengonfigurasi sumber daya sesuai dengan persyaratan Tingkat Gratis. Untuk informasi selengkapnya, lihat Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025.

Jika instans EC2 dan basis data RDS Anda berada di Zona Ketersediaan yang berbeda, Anda akan dikenai biaya transfer data. Untuk menghindari biaya ini, instans EC2 dan basis data RDS harus berada dalam Zona Ketersediaan yang sama. Untuk informasi tentang biaya transfer data, lihat Transfer Data di halaman Harga Sesuai Permintaan Amazon EC2.

Untuk mencegah timbulnya biaya setelah Anda menyelesaikan tutorial, pastikan untuk menghapus sumber daya jika tidak lagi diperlukan. Untuk langkah-langkah menghapus sumber daya, lihat Tugas 4 (Opsional): Bersihkan.

Opsi 1: Secara otomatis menghubungkan instance ke database RDS menggunakan konsol EC2

Tujuan Opsi 1 adalah mengeksplorasi fitur koneksi otomatis di konsol EC2 yang secara otomatis mengonfigurasi koneksi antara instans EC2 dan basis data RDS Anda untuk memungkinkan lalu lintas antara instans EC2 dan basis data RDS. Di Opsi 3, Anda akan mempelajari cara mengonfigurasi koneksi secara manual.

Tugas

- Sebelum Anda mulai
- Tugas 1 (Opsional): Buat database RDS
- Tugas 2 (Opsional): Luncurkan instans EC2
- Tugas 3: Hubungkan instans EC2 Anda secara otomatis ke basis data RDS Anda
- Tugas 4: Verifikasi konfigurasi koneksi
- Tugas 5 (Opsional): Bersihkan

Sebelum Anda mulai

Anda memerlukan hal berikut ini untuk menyelesaikan tutorial ini:

- Basis data RDS yang berada dalam VPC yang sama dengan instans EC2. Anda dapat menggunakan basis data RDS yang ada atau mengikuti langkah-langkah di Tugas 1 untuk membuat basis data RDS baru.
- Instans EC2 yang berada dalam VPC yang sama dengan basis data RDS. Anda dapat menggunakan instans EC2 yang ada atau mengikuti langkah-langkah di Tugas 2 untuk membuat instans EC2 baru.
- Izin untuk memanggil operasi berikut ini:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`

- `ec2:CreateSecurityGroup`
- `ec2:CreateSubnet`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Tugas 1 (Opsional): Buat database RDS

> **Note**
>
> Membuat basis data Amazon RDS bukanlah fokus dari tutorial ini. Jika sudah memiliki basis data RDS dan ingin menggunakannya dalam tutorial ini, Anda dapat melewati tugas ini. Jika Anda menggunakan basis data RDS yang ada, pastikan basis data berada di VPC yang sama dengan instans EC2 Anda sehingga Anda dapat menggunakan fitur koneksi otomatis.

Tujuan dari tugas ini adalah untuk membuat basis data RDS sehingga Anda dapat menyelesaikan Tugas 3 di mana Anda akan mengonfigurasi koneksi antara instans EC2 dan basis data RDS Anda. Langkah-langkah dalam tugas ini mengonfigurasi basis data RDS sebagai berikut:

- Tipe mesin: MySQL
- Templat: Tingkat gratis
- Pengidentifikasi instans DB: **`tutorial-database-1`**
- Kelas instans DB: `db.t3.micro`

> **Important**
>
> Dalam lingkungan produksi, Anda harus mengonfigurasi basis data Anda untuk memenuhi kebutuhan spesifik Anda.

Untuk membuat basis data MySQL RDS

1. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.
2. Dari pemilih Wilayah (di kanan atas), pilih sebuah AWS Region. Basis data dan instans EC2 harus berada di Wilayah yang sama untuk menggunakan fitur koneksi otomatis di konsol EC2.
3. Pada dasbor, pilih Buat basis data.
4. Pada Pilih metode pembuatan basis data, periksa apakah Pembuatan Standar dipilih. Jika Anda memilih Easy create, pemilih VPC tidak tersedia. Anda harus memastikan bahwa basis data Anda berada di VPC yang sama dengan instans EC2 Anda untuk menggunakan fitur koneksi otomatis di konsol EC2.
5. Pada Opsi mesin, untuk Tipe mesin, pilih MySQL.
6. Pada Templat, pilih contoh templat untuk memenuhi kebutuhan Anda. Untuk tutorial ini, pilih Tingkat gratis untuk membuat basis data RDS tanpa biaya. Namun, perhatikan bahwa Tingkat Gratis hanya tersedia untuk akun yang memenuhi syarat untuk Tingkat Gratis. Anda dapat membaca lebih lanjut dengan memilih tautan Info di kotak Tingkat gratis.
7. Pada Pengaturan, lakukan hal berikut:

   a. Untuk Pengidentifikasi instans DB, masukkan nama untuk basis data. Untuk tutorial ini, masukkan **`tutorial-database-1`**.

   b. Untuk Nama pengguna master, biarkan nama default, yaitu **`admin`**.

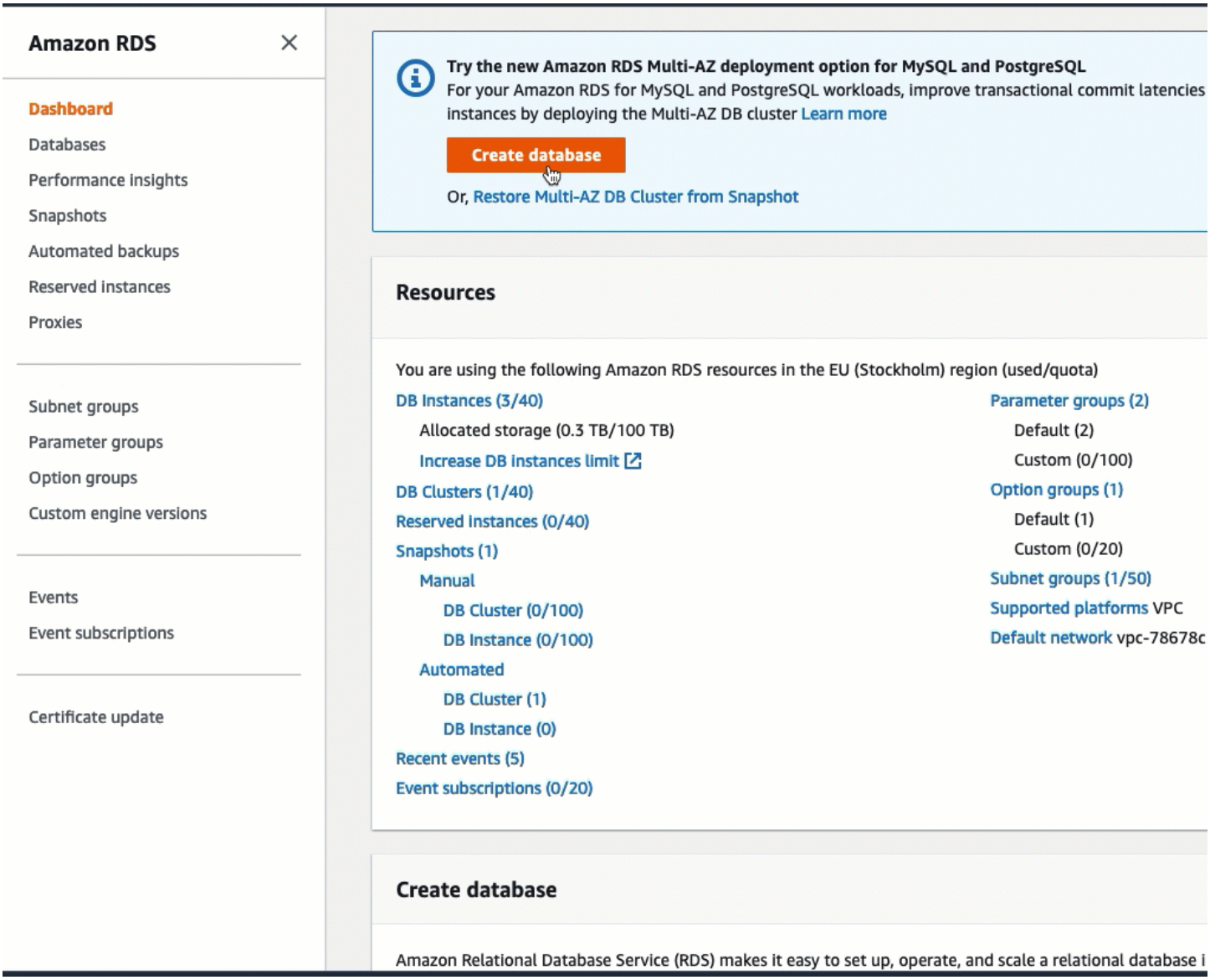
   c. Untuk Kata sandi master, masukkan kata sandi yang dapat Anda ingat untuk tutorial ini, kemudian untuk Konfirmasi kata sandi, masukkan kata sandi lagi.
8. Di bawah konfigurasi Instance, untuk kelas instans DB, biarkan default, yaitu db.t3.micro. Jika akun Anda memenuhi syarat untuk Tingkat Gratis, Anda dapat menggunakan kelas database ini secara gratis. Untuk informasi selengkapnya, lihat AWS Tingkat Gratis.
9. Di bawah Konektivitas, untuk Sumber daya komputasi, pilih Jangan hubungkan ke sumber daya komputasi EC2 karena Anda akan menghubungkan instans EC2 dan basis data RDS nanti di Tugas 3.

   (Nantinya, di Opsi 2 tutorial ini, Anda akan mencoba fitur koneksi otomatis di konsol RDS dengan memilih Terhubung ke sumber daya komputasi EC2.)
10. Untuk cloud privat virtual (VPC), pilih VPC. VPC harus memiliki grup subnet DB. Untuk menggunakan fitur koneksi otomatis, instans EC2 dan basis data RDS harus berada di VPC yang sama.
11. Simpan semua nilai default untuk bidang lain di halaman ini.

12. Pilih Buat basis data.

    Pada layar Basis Data, Status basis data baru adalah Membuat sampai basis data siap digunakan. Saat statusnya berubah menjadi Tersedia, Anda dapat terhubung ke basis data. Tergantung pada kelas basis data dan jumlah penyimpanan, diperlukan waktu hingga 20 menit sebelum basis data baru tersedia.

Lihat animasi: Membuat basis data RDS



Tugas 2 (Opsional): Luncurkan instans EC2

> **Note**
>
> Meluncurkan sebuah instans bukanlah fokus dari tutorial ini. Jika Anda sudah memiliki instans Amazon EC2 dan ingin menggunakannya dalam tutorial ini, Anda dapat melewati tugas ini. Jika Anda menggunakan basis data RDS yang ada, pastikan basis data berada di VPC yang sama dengan basis data RDS Anda sehingga Anda dapat menggunakan fitur koneksi otomatis.

Tujuan dari tugas ini adalah untuk meluncurkan instans EC2 sehingga Anda dapat menyelesaikan Tugas 3 di mana Anda akan mengonfigurasi koneksi antara instans EC2 dan basis data Amazon RDS Anda. Langkah-langkah dalam tugas ini mengonfigurasi instans EC2 sebagai berikut:

- Nama instans: **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- Tipe instans: `t2.micro`
- Penetapan otomatis IP publik: Aktif
- Grup keamanan dengan tiga aturan berikut:
  - Izinkan SSH dari alamat IP Anda
  - Izinkan lalu lintas HTTPS dari mana saja
  - Izinkan lalu lintas HTTP dari mana saja

> **Important**
>
> Dalam lingkungan produksi, Anda harus mengonfigurasi instans Anda untuk memenuhi kebutuhan spesifik Anda.

Cara meluncurkan instans EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari pemilih Wilayah (di kanan atas), pilih sebuah AWS Region. Instans dan basis data RDS harus berada di Wilayah yang sama untuk menggunakan fitur koneksi otomatis di konsol EC2.
3. Dari Dasbor EC2, pilih Luncurkan instans.

4. Pada Nama dan tanda, masukkan nama untuk mengidentifikasi instans Anda pada Nama. Untuk tutorial ini, beri nama instans **`tutorial-instance-1`**. Meskipun nama instans tidak wajib, ketika Anda memilih instans Anda di konsol EC2, nama tersebut akan membantu Anda mengidentifikasinya dengan mudah.
5. Pada Gambar Aplikasi dan OS, pilih AMI yang memenuhi kebutuhan server web Anda. Tutorial ini menggunakan Amazon Linux 2.
6. Pada Tipe instans, pilih tipe instans yang memenuhi kebutuhan server web Anda pada Tipe instans. Tutorial ini menggunakan `t2.micro`.

> **Note**
>
> Bergantung pada saat Anda membuat akun, Anda mungkin memenuhi syarat untuk menggunakan Amazon EC2 di bawah Tingkat Gratis.
> Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan usianya kurang dari 12 bulan, Anda dapat menggunakan Amazon EC2 di bawah Tingkat Gratis dengan memilih jenis instans t2.micro, atau jenis instans t3.micro di Wilayah di mana t2.micro tidak tersedia. Ketahuilah bahwa ketika Anda meluncurkan instans t3.micro, default ke mode Tidak Terbatas, yang mungkin dikenakan biaya tambahan berdasarkan penggunaan CPU.
> Jika jenis instans dapat digunakan di bawah Tingkat Gratis, itu diberi label Tingkat Gratis yang memenuhi syarat.
> Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, Anda dapat menggunakan jenis instans t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large, dan m7i-flex.large selama 6 bulan atau sampai kredit Anda habis.
> Untuk informasi selengkapnya, lihat Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025.

7. Pada Pasangan kunci (login), untuk Nama pasangan kunci, pilih pasangan kunci Anda.
8. Pada Pengaturan jaringan, lakukan hal berikut:

   a. Untuk Jaringan dan Subnet, jika Anda belum membuat perubahan pada VPC atau subnet default Anda, Anda dapat mempertahankan pengaturan default.

      Jika Anda telah membuat perubahan pada VPC atau subnet default Anda, periksa hal berikut:

      i. Instans harus berada dalam VPC yang sama dengan basis data RDS untuk menggunakan fitur koneksi otomatis. Secara default, Anda hanya memiliki satu VPC.

ii. VPC tempat Anda meluncurkan instans harus memiliki gateway internet yang melekat padanya, sehingga Anda dapat mengakses server web dari internet. VPC default Anda secara otomatis disiapkan dengan gateway internet.

iii. Untuk memastikan bahwa instans Anda menerima alamat IP publik, untuk Tetapkan otomatis IP publik, periksa apakah Aktifkan dipilih. Jika Nonaktifkan dipilih, pilih Edit (di sebelah kanan Pengaturan Jaringan), lalu untuk Tetapkan otomatis IP publik, pilih Aktifkan.

b. Untuk terhubung ke instans Anda dengan menggunakan SSH, Anda memerlukan aturan grup keamanan yang mengotorisasi lalu lintas SSH (Linux) atau RDP (Windows) dari alamat publik komputer Anda. IPv4 Secara default, saat Anda meluncurkan sebuah instans, grup keamanan baru dibuat dengan aturan yang memungkinkan lalu lintas SSH masuk dari mana saja.

   Untuk memastikan bahwa hanya alamat IP Anda yang dapat terhubung ke instans Anda, di bawah Firewall (grup keamanan), dari daftar drop-down di sebelah kotak centang Izinkan lalu lintas SSH dari, pilih IP Saya.

c. Untuk mengizinkan lalu lintas dari internet ke instans Anda, pilih kotak centang berikut:

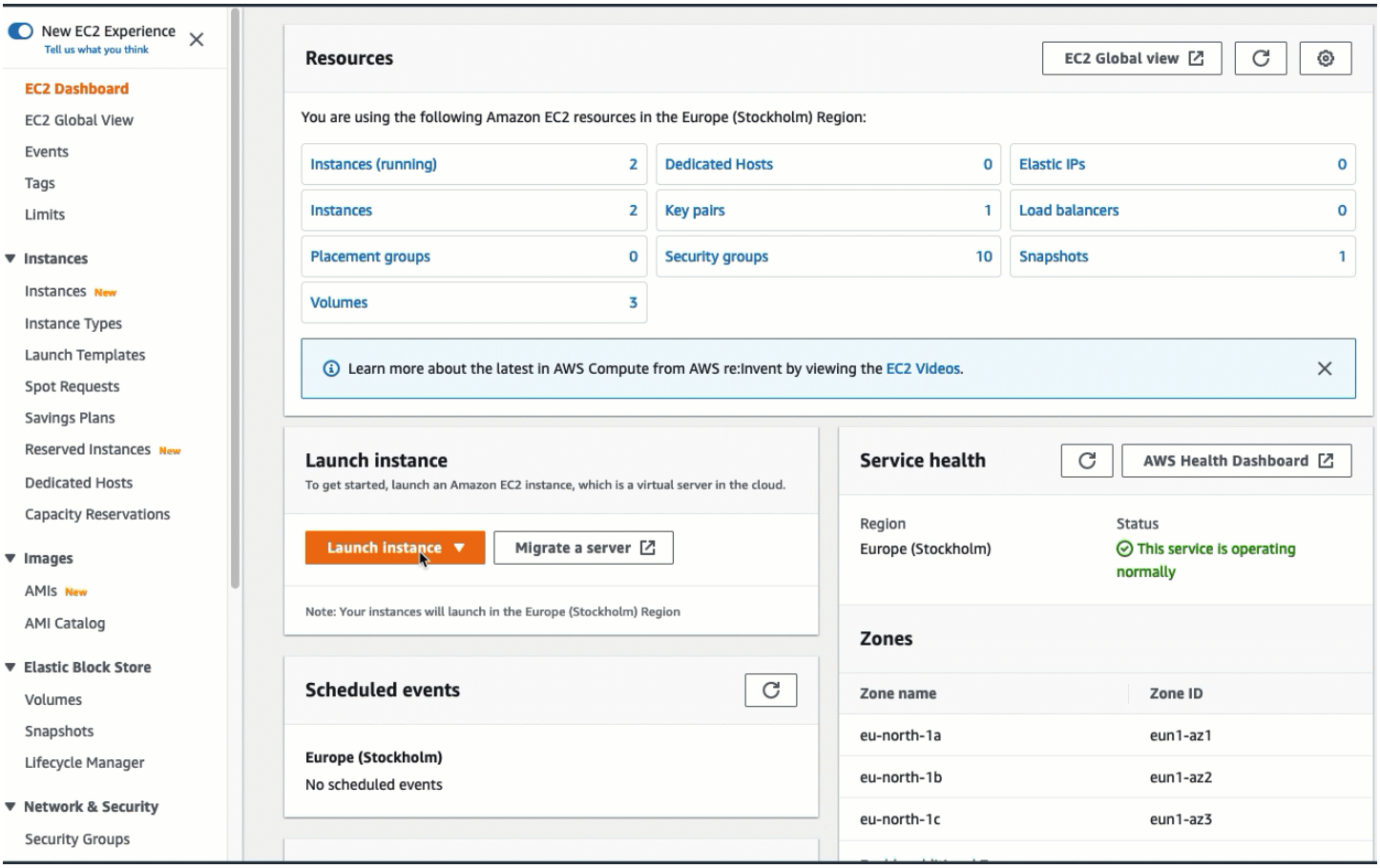
   - Izinkan HTTPs lalu lintas dari internet
   - Izinkan lalu lintas HTTP dari internet

9. Di panel Ringkasan, tinjau konfigurasi instans Anda dan pilih Luncurkan instans.
10. Biarkan halaman konfirmasi tetap terbuka. Anda akan membutuhkannya untuk tugas berikutnya saat Anda secara otomatis menghubungkan instans Anda ke basis data Anda.

    Jika instans gagal diluncurkan atau status langsung menjadi `terminated`, bukan `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

Untuk informasi tentang peluncuran instans, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

Lihat animasi: Luncurkan instans EC2



Tugas 3: Hubungkan instans EC2 Anda secara otomatis ke basis data RDS Anda

Tujuan dari tugas ini adalah untuk menggunakan fitur koneksi otomatis di konsol EC2 untuk secara otomatis mengonfigurasi koneksi antara instans EC2 Anda dan basis data RDS Anda.

Untuk secara otomatis menghubungkan instans EC2 ke basis data RDS menggunakan konsol EC2

1. Pada halaman konfirmasi peluncuran instans (harus terbuka dari tugas sebelumnya), pilih Hubungkan basis data RDS.

   Jika Anda menutup halaman konfirmasi, ikuti langkah-langkah berikut:

   a. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

   b. Di panel navigasi, pilih Instans.

   c. Pilih instans EC2 yang baru saja Anda buat, lalu pilih Actions, Jaringan, basis data Connect RDS.

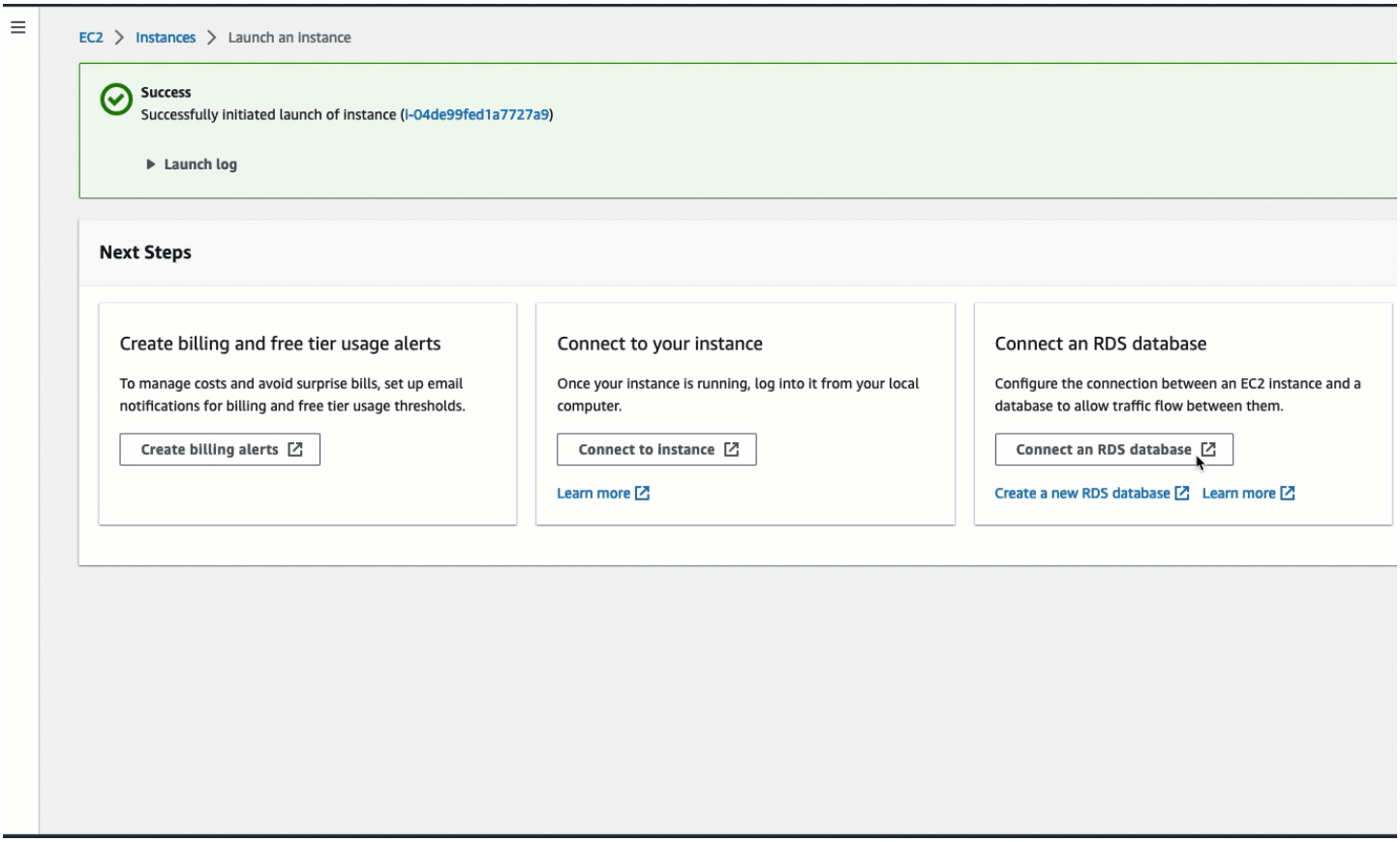
Jika Hubungkan basis data RDS tidak tersedia, periksa apakah instans EC2 berada dalam status Berjalan.

2. Untuk Peran basis data, pilih Instans. Instans dalam hal ini mengacu pada instans basis data.
3. Untuk basis data RDS, pilih basis data RDS yang Anda buat di Tugas 1.

> **Note**
>
> Instans EC2 dan basis data RDS harus dalam VPC yang sama agar dapat saling terhubung.

4. Pilih Hubungkan.

Lihat animasi: Menghubungkan instans EC2 yang baru diluncurkan ke basis data RDS



Tugas 4: Verifikasi konfigurasi koneksi

Tujuan dari tugas ini adalah untuk memverifikasi bahwa dua kelompok keamanan dibuat dan ditetapkan ke instans dan basis data.

Saat Anda menggunakan fitur koneksi otomatis di konsol untuk mengonfigurasi konektivitas, grup keamanan secara otomatis dibuat dan ditetapkan ke instance dan database, sebagai berikut:

- Grup keamanan rds-ec2- ***x*** dibuat dan ditambahkan ke database RDS. Ini memiliki satu aturan masuk yang merujuk kelompok *x* keamanan ec2-rds sebagai sumbernya. Ini memungkinkan lalu lintas dari instans EC2 dengan grup *x* keamanan ec2-rds- untuk mencapai database RDS.
- Grup keamanan ec2-rds- ***x*** dibuat dan ditambahkan ke instans EC2. Ini memiliki satu aturan keluar yang merujuk grup *x* keamanan rds-ec2- sebagai tujuannya. Ini memungkinkan lalu lintas dari instans EC2 untuk mencapai database RDS dengan grup keamanan rds-ec2 -. *x*

Untuk memverifikasi konfigurasi koneksi menggunakan konsol

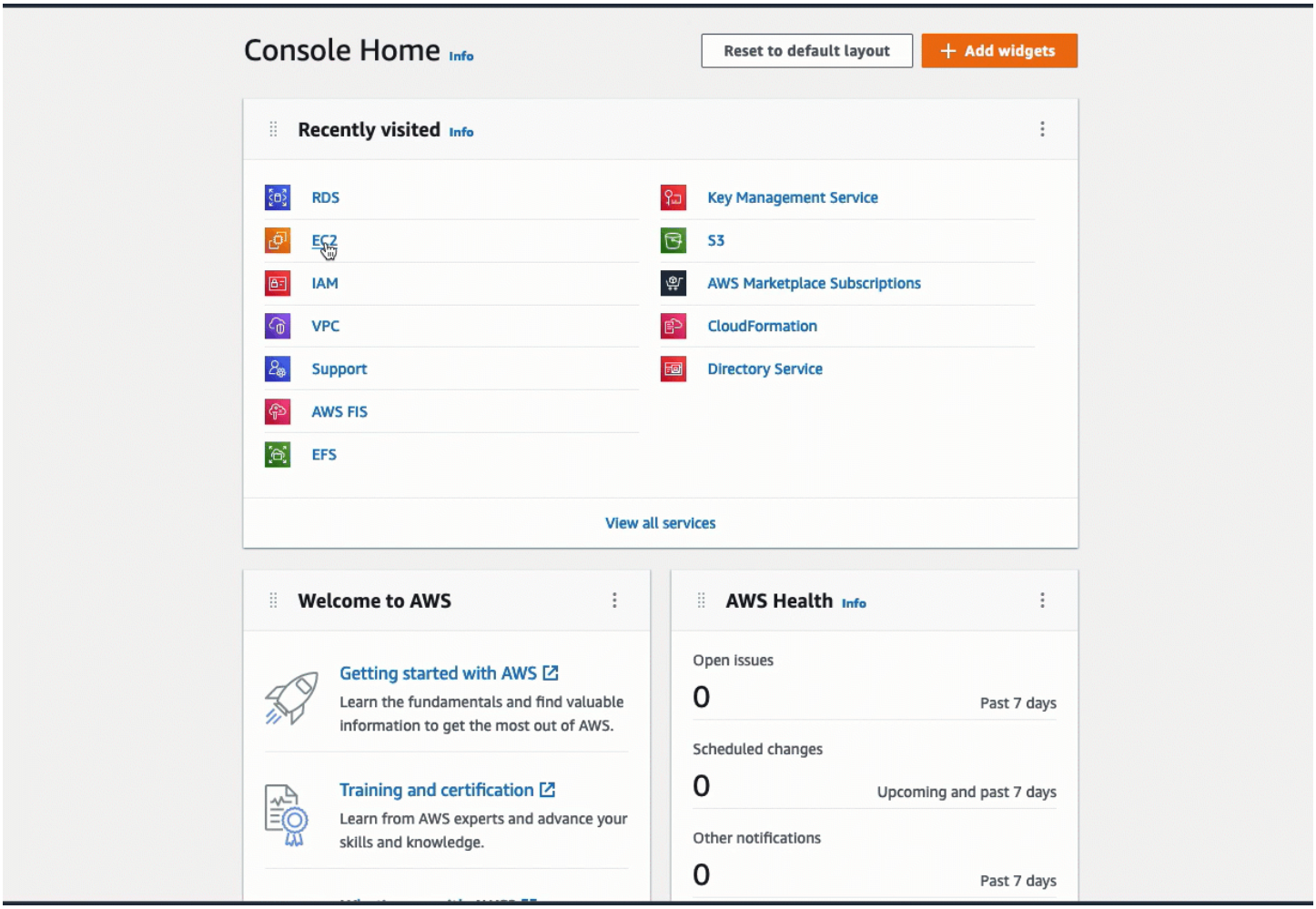
1. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.
2. Di halaman navigasi, pilih Basis Data.
3. Pilih basis data RDS yang Anda buat untuk tutorial ini.
4. Pada tab Konektivitas & keamanan, di bawah Keamanan, grup keamanan VPC, verifikasi bahwa grup keamanan yang disebut rds-ec2 - ditampilkan. *x*
5. Pilih grup keamanan rds-ec2 -. *x* Layar Grup Keamanan di konsol EC2 terbuka.
6. Pilih grup *x* keamanan rds-ec2- untuk membukanya.
7. Pilih tab Aturan masuk.
8. Verifikasi bahwa aturan grup keamanan berikut ada, sebagai berikut:
   - Tipe: MYSQL/Aurora
   - Rentang port: 3306
   - Sumber: ***sg-0987654321example***/ec2-rds- ***x*** — Ini adalah grup keamanan yang ditetapkan ke instans EC2 yang Anda verifikasi pada langkah-langkah sebelumnya.
   - Deskripsi: Aturan untuk mengizinkan koneksi dari instans EC2 dengan terlampir *sg-1234567890example*
9. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
10. Di panel navigasi, pilih Instans.
11. Pilih instans EC2 yang Anda pilih untuk terhubung ke basis data RDS di tugas sebelumnya, dan pilih tab Keamanan.
12. Di bawah Rincian keamanan, Grup keamanan, memverifikasi bahwa grup keamanan yang disebut ec2-rds- ***x*** ada dalam daftar. *x*adalah angka.

13. Pilih grup *x* keamanan ec2-rds- untuk membukanya.
14. Pilih tab Aturan keluar.
15. Verifikasi bahwa aturan grup keamanan berikut ada, sebagai berikut:

    - Tipe: MYSQL/Aurora
    - Rentang port: 3306
    - Tujuan: ***sg-1234567890example***/rds-ec2 - *x*
    - Deskripsi: Aturan untuk mengizinkan koneksi ke **`database-tutorial`** dari setiap instans grup keamanan ini dilampirkan ke

Dengan memverifikasi bahwa grup keamanan dan aturan grup keamanan ini ada dan bahwa masing-masing ditetapkan ke basis data RDS dan instans EC2 seperti yang dijelaskan dalam prosedur ini, Anda dapat memverifikasi bahwa koneksi secara otomatis dikonfigurasi dengan menggunakan fitur koneksi otomatis.

Lihat animasi: Verifikasi konfigurasi koneksi



Anda telah menyelesaikan Opsi 1 dari tutorial ini. Anda sekarang dapat menyelesaikan Opsi 2, yang mengajarkan Anda cara menggunakan konsol RDS untuk secara otomatis menghubungkan instans EC2 ke basis data RDS, atau Anda dapat menyelesaikan Opsi 3, yang mengajarkan Anda cara mengonfigurasi secara manual grup keamanan yang dibuat di Opsi 1 secara otomatis.

Tugas 5 (Opsional): Bersihkan

Warning

Mengakhiri sebuah instance bersifat permanen dan ireversibel.
Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.

Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Sekarang setelah Anda menyelesaikan tutorial, itu adalah praktik yang baik untuk membersihkan (menghapus) sumber daya apa pun yang tidak ingin Anda gunakan lagi. Membersihkan AWS sumber daya mencegah akun Anda dikenakan biaya lebih lanjut.

Jika Anda membuat basis data RDS khusus untuk tutorial ini, Anda dapat mengakhirinya untuk menghentikan biaya apa pun yang terkait dengannya.

Untuk mengakhiri instans menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans yang Anda buat untuk tutorial ini, dan pilih Status instans, Akhiri instans.
4. Pilih Akhiri saat diminta untuk konfirmasi.

Jika Anda membuat basis data RDS khusus untuk tutorial ini, Anda dapat menghapusnya untuk menghentikan biaya apa pun yang terkait dengannya.

Untuk menghapus basis data RDS menggunakan konsol

1. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.
2. Di panel navigasi, pilih Basis Data.
3. Pilih basis data RDS yang Anda buat untuk tutorial ini, dan pilih Tindakan, Hapus.
4. Masukkan **`delete me`** di dalam kotak, lalu pilih Hapus.

Opsi 2: Secara otomatis menghubungkan instance ke database RDS menggunakan konsol RDS

Tujuan Opsi 2 adalah mengeksplorasi fitur koneksi otomatis di konsol RDS yang secara otomatis mengonfigurasi koneksi antara instans EC2 dan basis data RDS Anda untuk memungkinkan lalu lintas antara instans EC2 dan basis data RDS. Di Opsi 3, Anda akan mempelajari cara mengonfigurasi koneksi secara manual.

Tugas

- Sebelum Anda mulai
- Tugas 1 (Opsional): Luncurkan instans EC2
- Tugas 2: Buat basis data RDS dan secara otomatis hubungkan ke instans EC2 Anda
- Tugas 3: Verifikasi konfigurasi koneksi
- Tugas 4 (Opsional): Bersihkan

Sebelum Anda mulai

Anda memerlukan hal berikut ini untuk menyelesaikan tutorial ini:

- Instans EC2 yang berada dalam VPC yang sama dengan basis data RDS. Anda dapat menggunakan instans EC2 yang ada atau mengikuti langkah-langkah di Tugas 1 untuk membuat instans baru.
- Izin untuk memanggil operasi berikut ini:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tugas 1 (Opsional): Luncurkan instans EC2

> **Note**
>
> Meluncurkan sebuah instans bukanlah fokus dari tutorial ini. Jika Anda sudah memiliki instans Amazon EC2 dan ingin menggunakannya dalam tutorial ini, Anda dapat melewati tugas ini.

Tujuan dari tugas ini adalah untuk meluncurkan instans EC2 sehingga Anda dapat menyelesaikan Tugas 2 di mana Anda akan mengonfigurasi koneksi antara instans EC2 dan basis data Amazon RDS Anda. Langkah-langkah dalam tugas ini mengonfigurasi instans EC2 sebagai berikut:

- Nama instans: **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- Tipe instans: `t2.micro`
- Penetapan otomatis IP publik: Aktif
- Grup keamanan dengan tiga aturan berikut:
  - Izinkan SSH dari alamat IP Anda
  - Izinkan lalu lintas HTTPS dari mana saja
  - Izinkan lalu lintas HTTP dari mana saja

> **Important**
>
> Dalam lingkungan produksi, Anda harus mengonfigurasi instans Anda untuk memenuhi kebutuhan spesifik Anda.

Cara meluncurkan instans EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari Dasbor EC2, pilih Luncurkan instans.
3. Pada Nama dan tanda, masukkan nama untuk mengidentifikasi instans Anda pada Nama. Untuk tutorial ini, beri nama instans **`tutorial-instance-2`**. Meskipun nama instans tidak wajib, ketika Anda memilih instans Anda di konsol RDS, nama tersebut akan membantu Anda mengidentifikasinya dengan mudah.
4. Pada Gambar Aplikasi dan OS, pilih AMI yang memenuhi kebutuhan server web Anda. Tutorial ini menggunakan Amazon Linux.
5. Pada Tipe instans, pilih tipe instans yang memenuhi kebutuhan server web Anda pada Tipe instans. Tutorial ini menggunakan `t2.micro`.

> **Note**
>
> Bergantung pada saat Anda membuat akun, Anda mungkin memenuhi syarat untuk menggunakan Amazon EC2 di bawah Tingkat Gratis.
> Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan usianya kurang dari 12 bulan, Anda dapat menggunakan Amazon EC2 di bawah Tingkat Gratis dengan memilih jenis instans t2.micro, atau jenis instans t3.micro di Wilayah di mana t2.micro tidak tersedia. Ketahuilah bahwa ketika Anda meluncurkan instans t3.micro, default ke mode Tidak Terbatas, yang mungkin dikenakan biaya tambahan berdasarkan penggunaan CPU.
> Jika jenis instans dapat digunakan di bawah Tingkat Gratis, itu diberi label Tingkat Gratis yang memenuhi syarat.
> Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, Anda dapat menggunakan jenis instans t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large, dan m7i-flex.large selama 6 bulan atau sampai kredit Anda habis.
> Untuk informasi selengkapnya, lihat Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025.

6. Pada Pasangan kunci (login), untuk Nama pasangan kunci, pilih pasangan kunci Anda.
7. Pada Pengaturan jaringan, lakukan hal berikut:

   a. Untuk Jaringan dan Subnet, jika Anda belum membuat perubahan pada VPC atau subnet default Anda, Anda dapat mempertahankan pengaturan default.

      Jika Anda telah membuat perubahan pada VPC atau subnet default Anda, periksa hal berikut:

      i. Instans harus berada dalam VPC yang sama dengan basis data RDS untuk menggunakan konfigurasi koneksi otomatis. Secara default, Anda hanya memiliki satu VPC.

      ii. VPC tempat Anda meluncurkan instans harus memiliki gateway internet yang melekat padanya, sehingga Anda dapat mengakses server web dari internet. VPC default Anda secara otomatis disiapkan dengan gateway internet.

      iii. Untuk memastikan bahwa instans Anda menerima alamat IP publik, untuk Tetapkan otomatis IP publik, periksa apakah Aktifkan dipilih. Jika Nonaktifkan dipilih, pilih Edit (di sebelah kanan Pengaturan Jaringan), lalu untuk Tetapkan otomatis IP publik, pilih Aktifkan.

b. Untuk terhubung ke instans Anda dengan menggunakan SSH, Anda memerlukan aturan grup keamanan yang mengotorisasi lalu lintas SSH (Linux) atau RDP (Windows) dari alamat publik komputer Anda. IPv4 Secara default, saat Anda meluncurkan sebuah instans, grup keamanan baru dibuat dengan aturan yang memungkinkan lalu lintas SSH masuk dari mana saja.

   Untuk memastikan bahwa hanya alamat IP Anda yang dapat terhubung ke instans Anda, di bawah Firewall (grup keamanan), dari daftar drop-down di sebelah kotak centang Izinkan lalu lintas SSH dari, pilih IP Saya.

c. Untuk mengizinkan lalu lintas dari internet ke instans Anda, pilih kotak centang berikut:

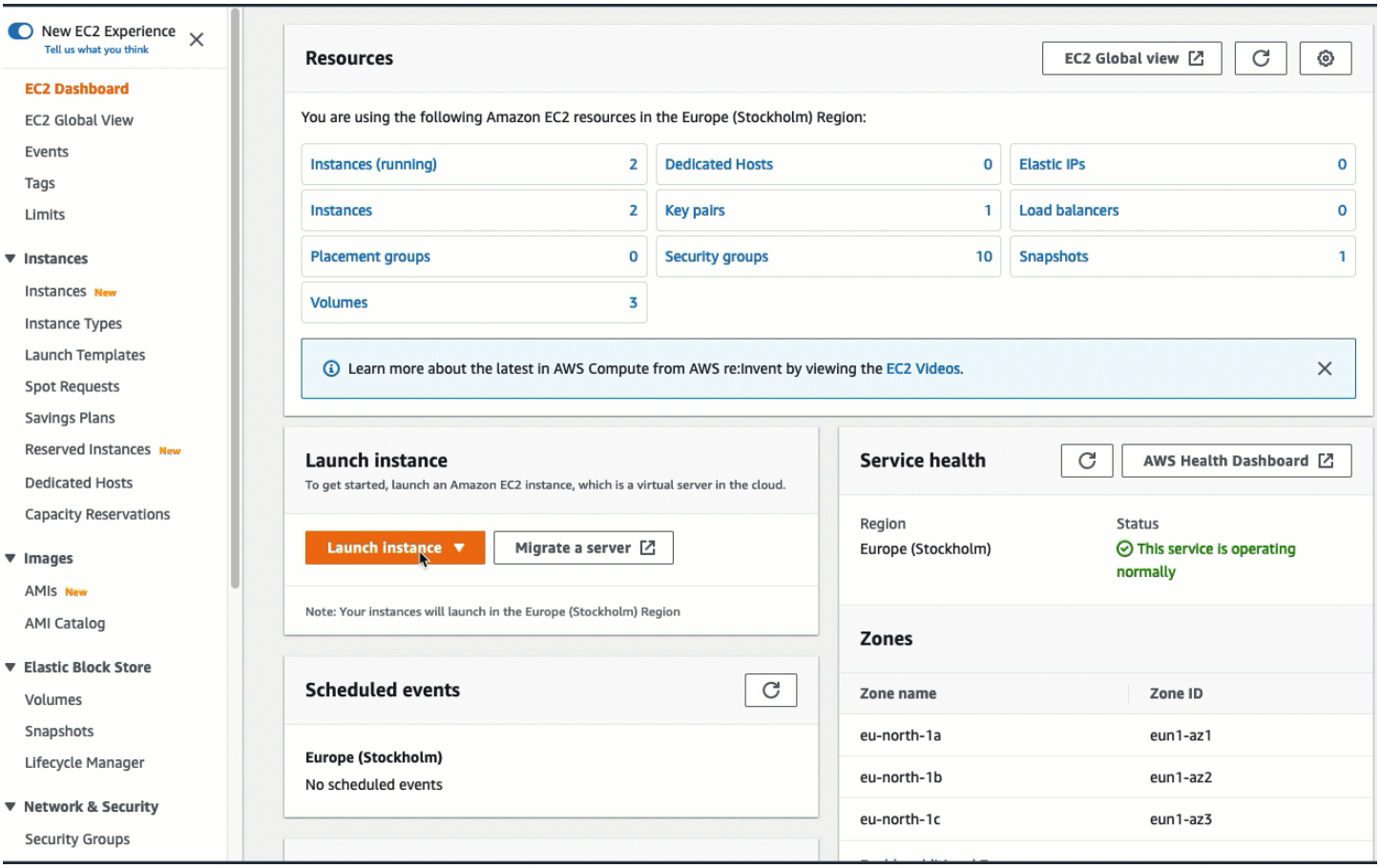
   - Izinkan HTTPs lalu lintas dari internet
   - Izinkan lalu lintas HTTP dari internet

8. Di panel Ringkasan, tinjau konfigurasi instans Anda dan pilih Luncurkan instans.
9. Pilih Lihat semua instans untuk menutup halaman konfirmasi dan kembali ke konsol. Instans Anda pertama-tama akan berada dalam status `pending`, kemudian akan masuk ke status `running`.

   Jika instans gagal diluncurkan atau status langsung menjadi `terminated`, bukan `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

Untuk informasi tentang peluncuran instans, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

Lihat animasi: Luncurkan instans EC2



Tugas 2: Buat basis data RDS dan secara otomatis hubungkan ke instans EC2 Anda

Tujuan dari tugas ini adalah untuk membuat basis data RDS dan menggunakan fitur koneksi otomatis di konsol EC2 untuk secara otomatis mengonfigurasi koneksi antara instans EC2 Anda dan basis data RDS Anda. Langkah-langkah dalam tugas ini mengonfigurasi instans DB sebagai berikut:

- Tipe mesin: MySQL
- Templat: Tingkat gratis
- Pengidentifikasi instans DB: **`tutorial-database`**
- Kelas instans DB: `db.t3.micro`

> **Important**
>
> Dalam lingkungan produksi, Anda harus mengonfigurasi instans Anda untuk memenuhi kebutuhan spesifik Anda.

Untuk membuat basis data RDS dan secara otomatis menghubungkannya ke instans EC2

1. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.
2. Dari pemilih Region (di kanan atas), pilih AWS Region tempat Anda membuat instans EC2. Instans EC2 dan basis data RDS harus berada di Wilayah yang sama.
3. Pada dasbor, pilih Buat basis data.
4. Pada Pilih metode pembuatan basis data, periksa apakah Pembuatan Standar dipilih. Jika Anda memilih Mudah buat, fitur koneksi otomatis tidak tersedia.
5. Pada Opsi mesin, untuk Tipe mesin, pilih MySQL.
6. Pada Templat, pilih contoh templat untuk memenuhi kebutuhan Anda. Untuk tutorial ini, pilih Tingkat gratis untuk membuat basis data RDS tanpa biaya. Namun, perhatikan bahwa Tingkat Gratis hanya tersedia jika akun Anda memenuhi syarat untuk Tingkat Gratis. Anda dapat membaca lebih lanjut dengan memilih tautan Info di kotak Tingkat gratis.
7. Pada Pengaturan, lakukan hal berikut:
   a. Untuk Pengidentifikasi instans DB, masukkan nama untuk basis data. Untuk tutorial ini, masukkan **`tutorial-database`**.
   b. Untuk Nama pengguna master, biarkan nama default, yaitu **`admin`**.
   c. Untuk Kata sandi master, masukkan kata sandi yang dapat Anda ingat untuk tutorial ini, kemudian untuk Konfirmasi kata sandi, masukkan kata sandi lagi.
8. Di bawah konfigurasi Instance, untuk kelas instans DB, biarkan default, yaitu db.t3.micro. Jika akun Anda memenuhi syarat untuk Tingkat Gratis, Anda dapat menggunakan instance ini secara gratis. Untuk informasi selengkapnya, lihat AWS Tingkat Gratis.
9. Untuk Konektivitas, Sumber daya komputasi, pilih Hubungkan ke sumber daya komputasi EC2. Ini adalah fitur koneksi otomatis di konsol RDS.
10. Untuk instans EC2, pilih instans EC2 yang ingin Anda connect. Untuk keperluan tutorial ini, Anda dapat memilih instans yang Anda buat di tugas sebelumnya, yang Anda beri nama**`tutorial-instance`**, atau memilih instans lain yang ada. Jika Anda tidak melihat instans Anda dalam daftar, pilih ikon refresh di sebelah kanan Konektivitas.

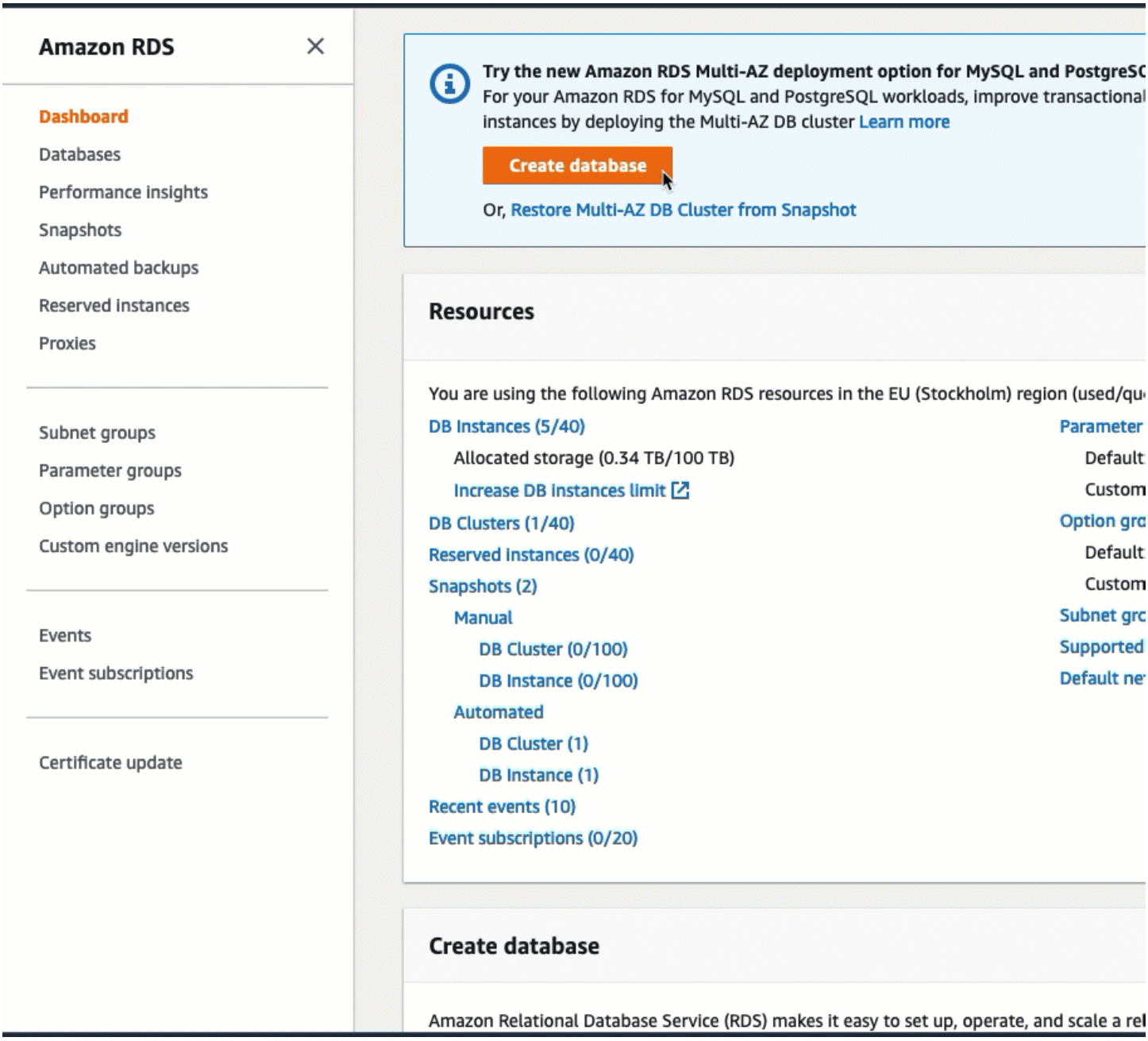
Saat Anda menggunakan fitur koneksi otomatis, grup keamanan ditambahkan ke instans EC2 ini, dan grup keamanan lain ditambahkan ke basis data RDS. Grup keamanan secara otomatis dikonfigurasi untuk memungkinkan lalu lintas antara instans EC2 dan basis data RDS. Pada tugas berikutnya, Anda akan memverifikasi bahwa grup keamanan telah dibuat dan ditetapkan ke instans EC2 dan basis data RDS.

11. Pilih Buat basis data.

    Pada layar Basis Data, Status basis data baru adalah Membuat sampai basis data siap digunakan. Saat statusnya berubah menjadi Tersedia, Anda dapat terhubung ke basis data. Tergantung pada kelas basis data dan jumlah penyimpanan, diperlukan waktu hingga 20 menit sebelum basis data baru tersedia.

Untuk mempelajari selengkapnya, lihat Mengonfigurasi konektivitas jaringan otomatis dengan instans EC2 di Panduan Pengguna Amazon RDS.

Lihat animasi: Membuat basis data RDS dan secara otomatis menghubungkannya ke instans EC2.



Tugas 3: Verifikasi konfigurasi koneksi

Tujuan dari tugas ini adalah untuk memverifikasi bahwa dua kelompok keamanan dibuat dan ditetapkan ke instans dan basis data.

Saat Anda menggunakan fitur koneksi otomatis di konsol untuk mengonfigurasi konektivitas, grup keamanan secara otomatis dibuat dan ditetapkan ke instance dan database, sebagai berikut:

- Grup keamanan rds-ec2- ***x*** dibuat dan ditambahkan ke database RDS. Ini memiliki satu aturan masuk yang merujuk kelompok *x* keamanan ec2-rds sebagai sumbernya. Ini memungkinkan lalu lintas dari instans EC2 dengan grup *x* keamanan ec2-rds- untuk mencapai database RDS.
- Grup keamanan ec2-rds- ***x*** dibuat dan ditambahkan ke instans EC2. Ini memiliki satu aturan keluar yang merujuk grup *x* keamanan rds-ec2- sebagai tujuannya. Ini memungkinkan lalu lintas dari instans EC2 untuk mencapai database RDS dengan grup keamanan rds-ec2 -. *x*

Untuk memverifikasi konfigurasi koneksi menggunakan konsol

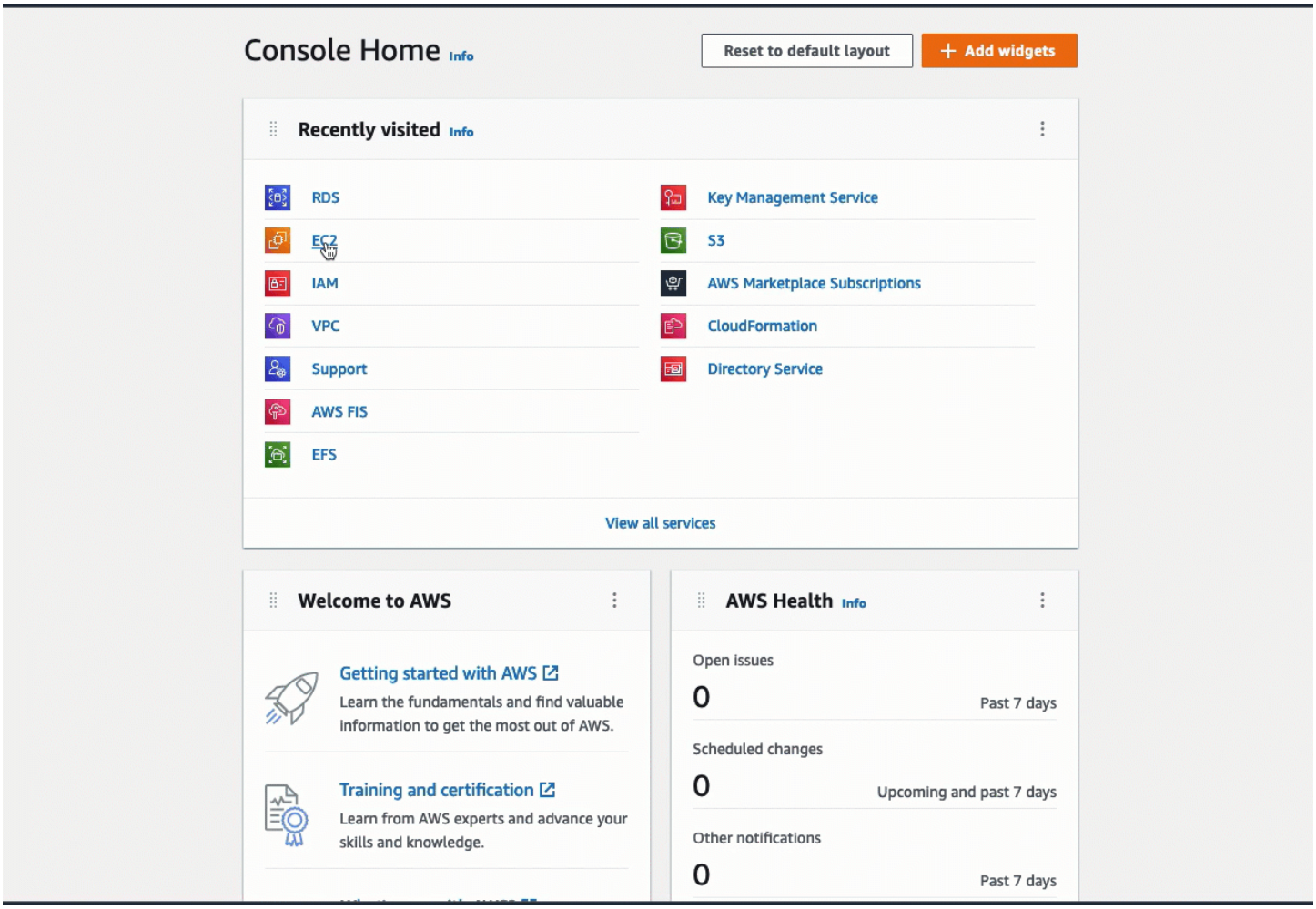
1. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.
2. Di halaman navigasi, pilih Basis Data.
3. Pilih basis data RDS yang Anda buat untuk tutorial ini.
4. Pada tab Konektivitas & keamanan, di bawah Keamanan, grup keamanan VPC, verifikasi bahwa grup keamanan yang disebut rds-ec2 - ditampilkan. *x*
5. Pilih grup keamanan rds-ec2 -. *x* Layar Grup Keamanan di konsol EC2 terbuka.
6. Pilih grup *x* keamanan rds-ec2- untuk membukanya.
7. Pilih tab Aturan masuk.
8. Verifikasi bahwa aturan grup keamanan berikut ada, sebagai berikut:
   - Tipe: MYSQL/Aurora
   - Rentang port: 3306
   - Sumber: ***sg-0987654321example***/ec2-rds- ***x*** — Ini adalah grup keamanan yang ditetapkan ke instans EC2 yang Anda verifikasi pada langkah-langkah sebelumnya.
   - Deskripsi: Aturan untuk mengizinkan koneksi dari instans EC2 dengan terlampir *sg-1234567890example*
9. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
10. Di panel navigasi, pilih Instans.
11. Pilih instans EC2 yang Anda pilih untuk terhubung ke basis data RDS di tugas sebelumnya, dan pilih tab Keamanan.
12. Di bawah Rincian keamanan, Grup keamanan, memverifikasi bahwa grup keamanan yang disebut ec2-rds- ***x*** ada dalam daftar. *x*adalah angka.
13. Pilih grup *x* keamanan ec2-rds- untuk membukanya.
14. Pilih tab Aturan keluar.

15. Verifikasi bahwa aturan grup keamanan berikut ada, sebagai berikut:

    - Tipe: MYSQL/Aurora
    - Rentang port: 3306
    - Tujuan: ***sg-1234567890example***/rds-ec2 - *x*
    - Deskripsi: Aturan untuk mengizinkan koneksi ke **`database-tutorial`** dari setiap instans grup keamanan ini dilampirkan ke

Dengan memverifikasi bahwa grup keamanan dan aturan grup keamanan ini ada dan bahwa masing-masing ditetapkan ke basis data RDS dan instans EC2 seperti yang dijelaskan dalam prosedur ini, Anda dapat memverifikasi bahwa koneksi secara otomatis dikonfigurasi dengan menggunakan fitur koneksi otomatis.

Lihat animasi: Verifikasi konfigurasi koneksi



Anda telah menyelesaikan Opsi 2 dari tutorial ini. Anda sekarang dapat menyelesaikan Opsi 3, yang mengajarkan Anda cara untuk mengonfigurasi secara manual grup keamanan yang dibuat di Opsi 2 secara otomatis.

Tugas 4 (Opsional): Bersihkan

> **Warning**
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
> Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Sekarang setelah Anda menyelesaikan tutorial, itu adalah praktik yang baik untuk membersihkan (menghapus) sumber daya apa pun yang tidak ingin Anda gunakan lagi. Membersihkan AWS sumber daya mencegah akun Anda dikenakan biaya lebih lanjut.

Jika Anda membuat basis data RDS khusus untuk tutorial ini, Anda dapat mengakhirinya untuk menghentikan biaya apa pun yang terkait dengannya.

Untuk mengakhiri instans menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans yang Anda buat untuk tutorial ini, dan pilih Status instans, Akhiri instans.
4. Pilih Akhiri saat diminta untuk konfirmasi.

Jika Anda membuat basis data RDS khusus untuk tutorial ini, Anda dapat menghapusnya untuk menghentikan biaya apa pun yang terkait dengannya.

Untuk menghapus basis data RDS menggunakan konsol

1. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.

2. Di panel navigasi, pilih Basis Data.
3. Pilih basis data RDS yang Anda buat untuk tutorial ini, dan pilih Tindakan, Hapus.
4. Masukkan **`delete me`** di dalam kotak, lalu pilih Hapus.

Opsi 3: Hubungkan instance secara manual ke database RDS dengan membuat grup keamanan

Tujuan dari Opsi 3 adalah untuk mempelajari cara mengonfigurasi koneksi secara manual antara instans EC2 dan basis data RDS dengan mereproduksi konfigurasi fitur koneksi otomatis secara manual.

Tugas

- Sebelum Anda mulai
- Tugas 1 (Opsional): Luncurkan instans EC2
- Tugas 2 (Opsional): Buat database RDS
- Tugas 3: Hubungkan instans EC2 Anda secara manual ke basis data RDS Anda dengan membuat grup keamanan dan menetapkannya ke instans
- Tugas 4 (Opsional): Bersihkan

Sebelum Anda mulai

Anda memerlukan hal berikut ini untuk menyelesaikan tutorial ini:

- Instans EC2 yang berada dalam VPC yang sama dengan basis data RDS. Anda dapat menggunakan instans EC2 yang ada atau mengikuti langkah-langkah di Tugas 1 untuk membuat instans baru.
- Basis data RDS yang berada dalam VPC yang sama dengan instans EC2. Anda dapat menggunakan basis data RDS yang ada atau mengikuti langkah-langkah di Tugas 2 untuk membuat basis data baru.
- Izin untuk memanggil operasi berikut ini:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`

- `ec2:CreateSubnet`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Tugas 1 (Opsional): Luncurkan instans EC2

> **Note**
>
> Meluncurkan sebuah instans bukanlah fokus dari tutorial ini. Jika Anda sudah memiliki instans Amazon EC2 dan ingin menggunakannya dalam tutorial ini, Anda dapat melewati tugas ini.

Tujuan dari tugas ini adalah untuk meluncurkan instans EC2 sehingga Anda dapat menyelesaikan Tugas 3 di mana Anda akan mengonfigurasi koneksi antara instans EC2 dan basis data Amazon RDS Anda. Langkah-langkah dalam tugas ini mengonfigurasi instans EC2 sebagai berikut:

- Nama instans: **`tutorial-instance`**
- AMI: Amazon Linux 2
- Tipe instans: `t2.micro`
- Penetapan otomatis IP publik: Aktif
- Grup keamanan dengan tiga aturan berikut:
  - Izinkan SSH dari alamat IP Anda
  - Izinkan lalu lintas HTTPS dari mana saja
  - Izinkan lalu lintas HTTP dari mana saja

> **Important**
>
> Dalam lingkungan produksi, Anda harus mengonfigurasi instans Anda untuk memenuhi kebutuhan spesifik Anda.

Cara meluncurkan instans EC2

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari Dasbor EC2, pilih Luncurkan instans.
3. Pada Nama dan tanda, masukkan nama untuk mengidentifikasi instans Anda pada Nama. Untuk tutorial ini, beri nama instans **`tutorial-instance-manual-1`**. Meskipun nama instans tidak wajib, nama tersebut akan membantu Anda mengidentifikasinya dengan mudah.
4. Pada Gambar Aplikasi dan OS, pilih AMI yang memenuhi kebutuhan server web Anda. Tutorial ini menggunakan Amazon Linux.
5. Pada Tipe instans, pilih tipe instans yang memenuhi kebutuhan server web Anda pada Tipe instans. Tutorial ini menggunakan `t2.micro`.

   > **Note**
   >
   > Bergantung pada saat Anda membuat akun, Anda mungkin memenuhi syarat untuk menggunakan Amazon EC2 di bawah Tingkat Gratis.
   > Jika Anda membuat Akun AWS sebelum 15 Juli 2025 dan usianya kurang dari 12 bulan, Anda dapat menggunakan Amazon EC2 di bawah Tingkat Gratis dengan memilih jenis instans t2.micro, atau jenis instans t3.micro di Wilayah di mana t2.micro tidak tersedia. Ketahuilah bahwa ketika Anda meluncurkan instans t3.micro, default ke mode Tidak Terbatas, yang mungkin dikenakan biaya tambahan berdasarkan penggunaan CPU.
   > Jika jenis instans dapat digunakan di bawah Tingkat Gratis, itu diberi label Tingkat Gratis yang memenuhi syarat.
   > Jika Anda membuat Akun AWS pada atau setelah 15 Juli 2025, Anda dapat menggunakan jenis instans t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large, dan m7i-flex.large selama 6 bulan atau sampai kredit Anda habis.
   > Untuk informasi selengkapnya, lihat Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025.
6. Pada Pasangan kunci (login), untuk Nama pasangan kunci, pilih pasangan kunci Anda.

7. Pada Pengaturan jaringan, lakukan hal berikut:

   a. Untuk Jaringan dan Subnet, jika Anda belum membuat perubahan pada VPC atau subnet default Anda, Anda dapat mempertahankan pengaturan default.

      Jika Anda telah membuat perubahan pada VPC atau subnet default Anda, periksa hal berikut:

      i. Instans harus berada dalam VPC yang sama dengan basis data RDS. Secara default, Anda hanya memiliki satu VPC.

      ii. VPC tempat Anda meluncurkan instans harus memiliki gateway internet yang melekat padanya, sehingga Anda dapat mengakses server web dari internet. VPC default Anda secara otomatis disiapkan dengan gateway internet.

      iii. Untuk memastikan bahwa instans Anda menerima alamat IP publik, untuk Tetapkan otomatis IP publik, periksa apakah Aktifkan dipilih. Jika Nonaktifkan dipilih, pilih Edit (di sebelah kanan Pengaturan Jaringan), lalu untuk Tetapkan otomatis IP publik, pilih Aktifkan.

   b. Untuk terhubung ke instans Anda dengan menggunakan SSH, Anda memerlukan aturan grup keamanan yang mengotorisasi lalu lintas SSH (Linux) atau RDP (Windows) dari alamat publik komputer Anda. IPv4 Secara default, saat Anda meluncurkan sebuah instans, grup keamanan baru dibuat dengan aturan yang memungkinkan lalu lintas SSH masuk dari mana saja.

      Untuk memastikan bahwa hanya alamat IP Anda yang dapat terhubung ke instans Anda, di bawah Firewall (grup keamanan), dari daftar drop-down di sebelah kotak centang Izinkan lalu lintas SSH dari, pilih IP Saya.

   c. Untuk mengizinkan lalu lintas dari internet ke instans Anda, pilih kotak centang berikut:

      - Izinkan HTTPs lalu lintas dari internet
      - Izinkan lalu lintas HTTP dari internet

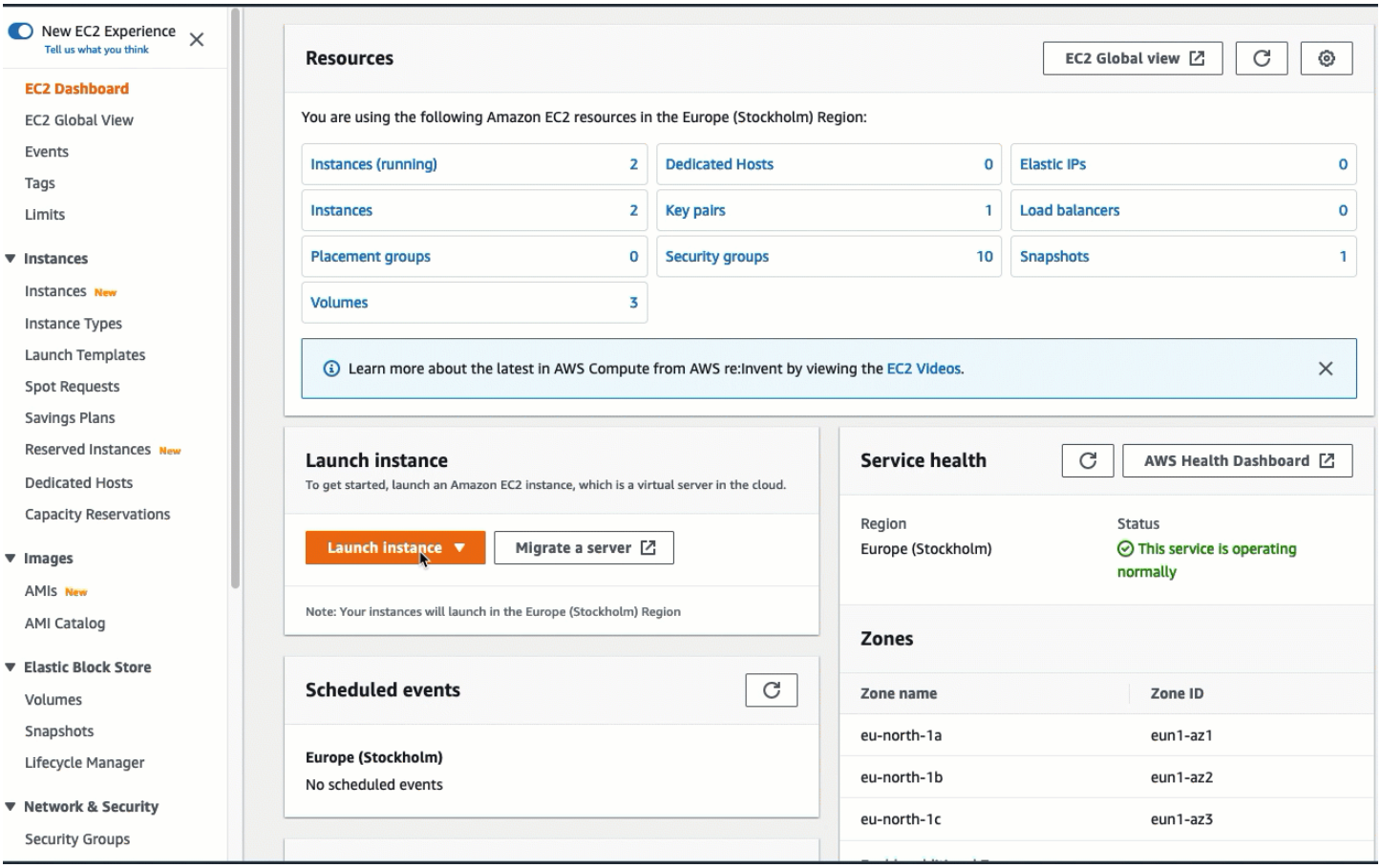
8. Di panel Ringkasan, tinjau konfigurasi instans Anda dan pilih Luncurkan instans.

9. Pilih Lihat semua instans untuk menutup halaman konfirmasi dan kembali ke konsol. Instans Anda pertama-tama akan berada dalam status `pending`, kemudian akan masuk ke status `running`.

   Jika instans gagal diluncurkan atau status langsung menjadi `terminated`, bukan `running`, lihat Memecahkan masalah peluncuran instans Amazon EC2.

Untuk informasi tentang peluncuran instans, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

Lihat animasi: Luncurkan instans EC2



Tugas 2 (Opsional): Buat database RDS

> **Note**
>
> Membuat basis data Amazon RDS bukanlah fokus dari tutorial ini. Jika sudah memiliki basis data RDS dan ingin menggunakannya untuk tutorial ini, Anda dapat melewati tugas ini.

Tujuan dari tugas ini adalah untuk membuat basis data RDS. Anda akan menggunakan instans ini di Tugas 3 saat Anda menghubungkannya ke instans EC2 Anda. Langkah-langkah dalam tugas ini mengonfigurasi basis data RDS sebagai berikut:

- Tipe mesin: MySQL

- Templat: Tingkat gratis
- Pengidentifikasi instans DB: **`tutorial-database-manual`**
- Kelas instans DB: `db.t3.micro`

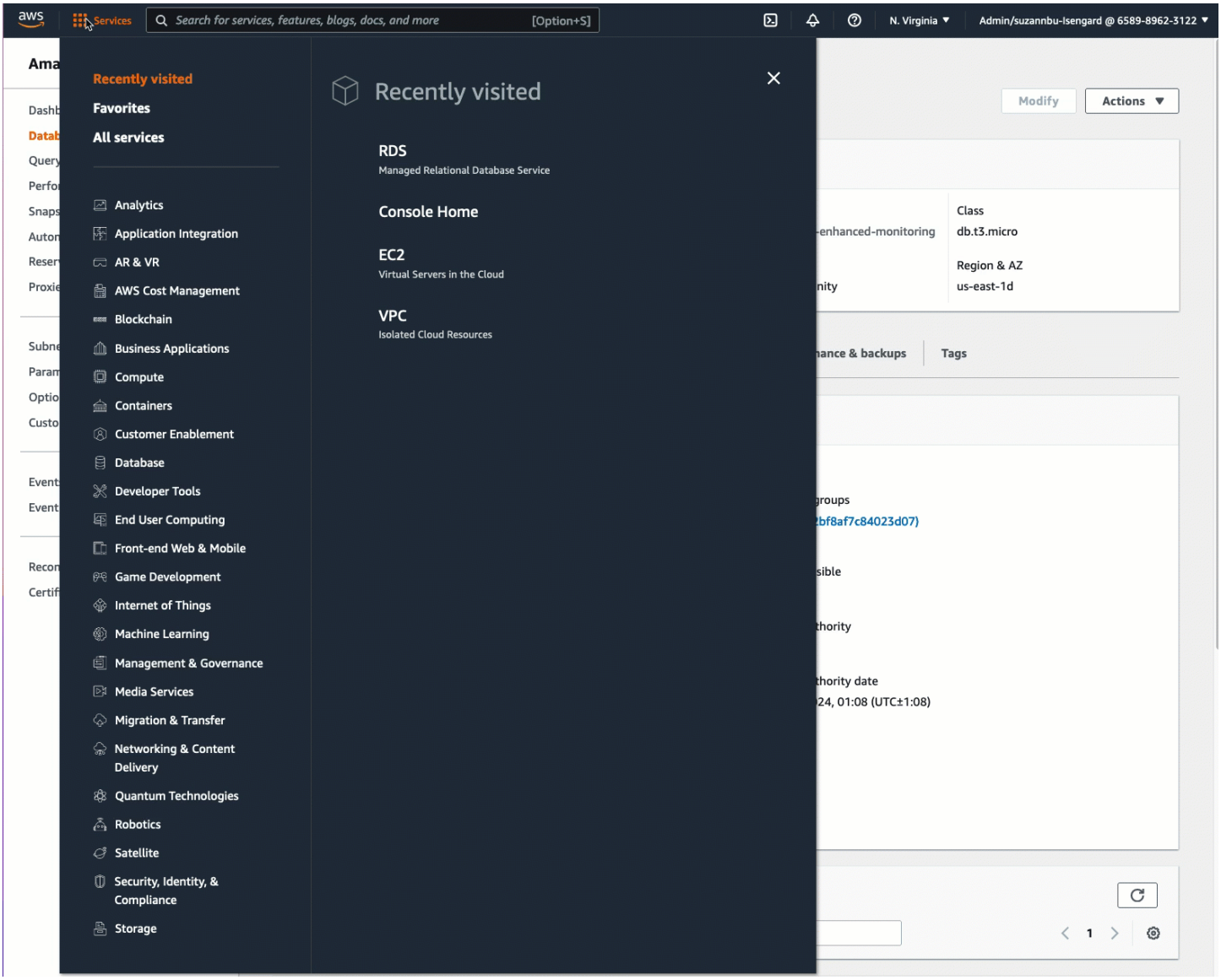
> **Important**
>
> Dalam lingkungan produksi, Anda harus mengonfigurasi instans Anda untuk memenuhi kebutuhan spesifik Anda.

Untuk membuat instans DB MySQL

1. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.
2. Dari pemilih Region (di kanan atas), pilih AWS Region tempat Anda membuat instans EC2. Instans EC2 dan instans DB harus berada di Wilayah yang sama.
3. Pada dasbor, pilih Buat basis data.
4. Di bawah Pilih metode pembuatan basid data, pilih Pembuatan mudah. Ketika Anda memilih opsi ini, fitur koneksi otomatis untuk secara otomatis mengonfigurasi koneksi tidak tersedia.
5. Pada Opsi mesin, untuk Tipe mesin, pilih MySQL.
6. Untuk Ukuran instans DB, pilih Tingkat gratis.
7. Untuk Pengidentifikasi instans DB masukkan nama untuk basis data RDS. Untuk tutorial ini, masukkan **`tutorial-database-manual`**.
8. Untuk Nama pengguna master, biarkan nama default, yaitu **`admin`**.
9. Untuk Kata sandi master, masukkan kata sandi yang dapat Anda ingat untuk tutorial ini, kemudian untuk Konfirmasi kata sandi, masukkan kata sandi lagi.
10. Pilih Buat basis data.

    Pada layar Basis Data, Status instans DB baru adalah Membuat sampai instans DB siap digunakan. Saat statusnya berubah menjadi Tersedia, Anda dapat terhubung ke instans DB. Tergantung pada kelas instans DB dan jumlah penyimpanan, diperlukan waktu hingga 20 menit sebelum instans baru tersedia.

Lihat animasi: Membuat instans DB



Tugas 3: Hubungkan instans EC2 Anda secara manual ke basis data RDS Anda dengan membuat grup keamanan dan menetapkannya ke instans

Tujuan dari tugas ini adalah untuk mereproduksi konfigurasi koneksi dari fitur koneksi otomatis dengan melakukan hal berikut secara manual: Anda membuat dua grup keamanan baru, kemudian menambahkan grup keamanan masing-masing ke instans EC2 dan basis data RDS.

Untuk membuat dua grup keamanan baru dan menetapkan masing-masing ke instans EC2 dan basis data RDS

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Pertama buat grup keamanan untuk ditambahkan ke instans EC2, sebagai berikut:

   a. Pada panel navigasi, pilih Grup Keamanan.

   b. Pilih Buat grup keamanan.

   c. Untuk Nama grup keamanan, masukkan nama deskriptif untuk grup keamanan. Untuk tutorial ini, masukkan **`ec2-rds-manual-configuration`**.

   d. Untuk Deskripsi, masukkan deskripsi singkat. Untuk tutorial ini, masukkan **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`**.

   e. Pilih Buat grup keamanan. Anda akan kembali ke grup keamanan ini untuk menambahkan aturan keluar setelah Anda membuat grup keamanan basis data RDS.

3. Sekarang, buat grup keamanan untuk ditambahkan ke basis data RDS, sebagai berikut:

   a. Pada panel navigasi, pilih Grup Keamanan.

   b. Pilih Buat grup keamanan.

   c. Untuk Nama grup keamanan, masukkan nama deskriptif untuk grup keamanan. Untuk tutorial ini, masukkan **`rds-ec2-manual-configuration`**.

   d. Untuk Deskripsi, masukkan deskripsi singkat. Untuk tutorial ini, masukkan **`RDS database security group to allow EC2 instance to securely connect to RDS database`**.

   e. Pada Aturan masuk, pilih Tambahkan aturan, lalu lakukan hal berikut:

      i. Untuk Tipe, pilih MySQL/Aurora.

      ii. Untuk Sumber, pilih grup keamanan instans EC2 ec2- rds-manual-configuration yang Anda buat di Langkah 2 prosedur ini.

   f. Pilih Buat grup keamanan.

4. Edit grup keamanan instans EC2 untuk menambahkan aturan keluar, sebagai berikut:

   a. Pada panel navigasi, pilih Grup Keamanan.

   b. Pilih grup keamanan instans EC2 (sebut saja **`ec2-rds-manual-configuration`**), dan pilih tab Aturan keluar.

   c. Pilih Edit aturan keluar.

   d. Pilih Tambahkan aturan, dan lakukan hal-hal berikut:

      i. Untuk Tipe, pilih MySQL/Aurora.

ii. Untuk Tujuan, pilih grup keamanan database RDS rds-ec2-manual-configuration yang Anda buat di Langkah 3 prosedur ini.

iii. Pilih Simpan aturan.

5. Tambahkan grup keamanan instans EC2 ke instans EC2 sebagai berikut:

   a. Di panel navigasi, pilih Instans.

   b. Pilih instans EC2 Anda, kemudian pilih Tindakan, Keamanan, Ubah grup keamanan.

   c. Di bawah Grup keamanan terkait, pilih bidang Pilih grup keamanan, pilih ec2- rds-manual-configuration yang Anda buat sebelumnya, lalu pilih Tambahkan grup keamanan.

   d. Pilih Simpan.

6. Tambahkan grup keamanan basis data RDS ke basis data RDS sebagai berikut:

   a. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.

   b. Di panel navigasi, pilih Basis daya dan plih basis data Anda.

   c. Pilih Ubah.

   d. Di bawah Konektivitas, untuk grup Keamanan, pilih rds-ec2-manual-configuration yang Anda buat sebelumnya, lalu pilih Lanjutkan.

   e. Di bawah Penjadwalan Modifikasi, pilih Terapkan segera.

   f. Pilih Ubah instans DB.

   Anda sekarang telah menyelesaikan langkah manual yang meniru langkah otomatis yang terjadi ketika Anda menggunakan fitur koneksi otomatis.

Anda telah menyelesaikan Opsi 3 dari tutorial ini. Jika Anda telah menyelesaikan Opsi 1, 2, dan 3, dan Anda tidak lagi membutuhkan sumber daya yang dibuat dalam tutorial ini, Anda harus menghapusnya untuk mencegah timbulnya biaya yang tidak perlu. Untuk informasi selengkapnya, lihat Tugas 4 (Opsional): Bersihkan.

Tugas 4 (Opsional): Bersihkan

> **Warning**
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi

untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Sekarang setelah Anda menyelesaikan tutorial, itu adalah praktik yang baik untuk membersihkan (menghapus) sumber daya apa pun yang tidak ingin Anda gunakan lagi. Membersihkan AWS sumber daya mencegah akun Anda dikenakan biaya lebih lanjut.

Jika Anda membuat basis data RDS khusus untuk tutorial ini, Anda dapat mengakhirinya untuk menghentikan biaya apa pun yang terkait dengannya.

Untuk mengakhiri instans menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans yang Anda buat untuk tutorial ini, dan pilih Status instans, Akhiri instans.
4. Pilih Akhiri saat diminta untuk konfirmasi.

Jika Anda membuat basis data RDS khusus untuk tutorial ini, Anda dapat menghapusnya untuk menghentikan biaya apa pun yang terkait dengannya.

Untuk menghapus basis data RDS menggunakan konsol

1. Buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.
2. Di panel navigasi, pilih Basis Data.
3. Pilih basis data RDS yang Anda buat untuk tutorial ini, dan pilih Tindakan, Hapus.
4. Masukkan **`delete me`** di dalam kotak, lalu pilih Hapus.

Armada EC2 dan Armada Spot

Armada EC2 dan Armada Spot dirancang untuk menjadi cara yang berguna untuk meluncurkan armada puluhan, ratusan, atau ribuan instans Amazon EC2 dalam satu operasi. Setiap instance dalam armada dikonfigurasi oleh template peluncuran atau serangkaian parameter peluncuran yang Anda konfigurasikan secara manual saat peluncuran.

Topik

- Fitur dan manfaat
- yang merupakan metode armada terbaik untuk digunakan?
- Opsi konfigurasi untuk Armada EC2 atau Armada Spot
- Bekerja dengan Armada EC2
- Bekerja dengan Armada Spot
- Pantau Armada EC2 atau Armada Spot
- Tutorial untuk Armada EC2
- Contoh konfigurasi CLI untuk Armada EC2
- Contoh konfigurasi CLI Spot Fleet
- Kuota untuk Armada EC2 dan Armada Spot

Fitur dan manfaat

Armada menyediakan fitur dan manfaat berikut, memungkinkan Anda memaksimalkan penghematan biaya dan mengoptimalkan ketersediaan dan kinerja saat menjalankan aplikasi pada beberapa instans EC2.

Beberapa jenis instance

> Armada dapat meluncurkan beberapa jenis instans, memastikannya tidak bergantung pada ketersediaan jenis instans tunggal apa pun. Ini meningkatkan ketersediaan instance secara keseluruhan di armada Anda.

Mendistribusikan instans di seluruh Zona Ketersediaan

> Armada dapat diluncurkan ke beberapa Availability Zone, memungkinkan Anda mengurangi biaya dan meningkatkan ketersediaan. Jika armada Anda menyertakan Instans Spot, armada secara otomatis memilih Availability Zone berdasarkan preferensi Anda terkait harga dan interupsi.

Beberapa opsi pembelian

Armada dapat meluncurkan beberapa opsi pembelian (Instans Spot dan Sesuai Permintaan), memungkinkan Anda mengoptimalkan biaya melalui penggunaan Instans Spot. Anda juga dapat memanfaatkan diskon Instans Cadangan dan Savings Plans dengan menggunakannya bersama dengan Instans Sesuai Permintaan di armada.

Penggantian otomatis Instans Spot

Jika armada Anda menyertakan Instans Spot, maka secara otomatis dapat meminta penggantian kapasitas Spot jika Instans Spot Anda terganggu. Melalui Penyeimbangan Kembali Kapasitas, armada juga dapat memantau dan secara proaktif mengganti Instans Spot Anda yang berisiko tinggi mengalami gangguan.

Kapasitas Cadangan Sesuai Permintaan

Armada dapat menggunakan Reservasi Kapasitas Sesuai Permintaan untuk memesan kapasitas Sesuai Permintaan. Armada juga dapat menyertakan Blok Kapasitas untuk ML, memungkinkan Anda untuk memesan instans GPU di masa mendatang untuk mendukung beban kerja machine learning (ML) berdurasi pendek.

yang merupakan metode armada terbaik untuk digunakan?

Sebagai praktik terbaik secara umum, kami merekomendasikan peluncuran armada Instans Spot dan Sesuai Permintaan dengan Amazon EC2 Auto Scaling yang menyediakan fitur tambahan yang dapat digunakan untuk mengelola armada Anda. Daftar fitur tambahan mencakup penggantian pemeriksaan kondisi otomatis untuk Instans Spot dan Sesuai Permintaan, pemeriksaan kondisi berbasis aplikasi, dan integrasi dengan Elastic Load Balancing untuk memastikan distribusi lalu lintas aplikasi yang merata ke instans berkondisi baik milik Anda. Anda juga dapat menggunakan grup Auto Scaling saat menggunakan AWS layanan seperti Amazon ECS, Amazon EKS (grup node yang dikelola sendiri), dan Amazon VPC Lattice. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon EC2 Auto Scaling.

Jika Anda tidak dapat menggunakan Amazon EC2 Auto Scaling, Anda dapat mempertimbangkan untuk menggunakan Armada EC2 atau Armada Spot. Armada EC2 dan Armada Spot menawarkan fungsionalitas inti yang sama. Namun, Armada EC2 hanya tersedia menggunakan baris perintah dan tidak menyediakan dukungan konsol. Spot Fleet menyediakan dukungan konsol, tetapi didasarkan pada API lama tanpa investasi yang direncanakan.

Gunakan tabel berikut untuk menentukan metode armada mana yang akan digunakan.

Metode armada	Kapan harus menggunakan?	Kasus penggunaan
Amazon EC2 Auto Scaling	• Anda memerlukan beberapa instans dengan konfigurasi tunggal atau konfigurasi campuran. • Anda ingin mengotoma tiskan manajemen siklus hidup instans Anda.	Buat grup Auto Scaling yang mengelola siklus hidup instans Anda sambil mempertahankan jumlah instans yang diinginka n. Mendukung penskalaan horizontal (menambahkan lebih banyak instans) antara batas minimum dan maksimum yang ditentukan.
Armada EC2	• Anda memerlukan beberapa instans dengan konfigurasi tunggal atau konfigurasi campuran. • Anda ingin mengelola sendiri siklus hidup instans Anda. • Jika Anda tidak memerluka n penskalaan otomatis, kami sarankan Anda menggunakan Armada EC2 `instant` tipe.	Buat `instant` armada Instans Sesuai Permintaan dan Instans Spot dalam satu operasi, dengan beberapa spesifika si peluncuran yang bervarias i menurut jenis instans, AMI, Availability Zone, atau subnet. Strategi alokasi Instans Spot default `lowest-price` per unit, tetapi kami sarankan untuk mengubahnya menjadi. `price-capacity-opt imized`
Armada Spot	• Kami sangat tidak menyarankan menggunak an Spot Fleet karena didasarkan pada API lama tanpa investasi yang direncanakan. • Jika Anda ingin mengelola siklus hidup instans Anda, gunakan Armada EC2.	Gunakan Armada Spot hanya jika Anda memerlukan dukungan konsol untuk kasus penggunaan kapan Anda akan menggunakan Armada EC2.

Metode armada	Kapan harus menggunakan?	Kasus penggunaan
	• Jika Anda tidak ingin mengelola siklus hidup instans, gunakan grup Auto Scaling.	

Opsi konfigurasi untuk Armada EC2 atau Armada Spot

Saat merencanakan Armada EC2 atau Armada Spot, sebaiknya Anda mempertimbangkan opsi berikut saat memutuskan cara mengonfigurasi armada Anda.

Opsi Konfigurasi	Pertanyaan	Dokumentasi
Jenis permintaan armada	Apakah Anda menginginkan armada yang mengajukan permintaan satu kali untuk kapasitas target yang diinginkan, atau armada yang mempertahankan kapasitas target dari waktu ke waktu?	Jenis permintaan Armada EC2 dan Armada Spot
Instans Spot	Apakah Anda berencana untuk memasukkan Instans Spot dalam armada Anda? Tinjau praktik terbaik Spot dan gunakan saat merencanakan armada sehingga Anda dapat menyediakan instans dengan harga serendah mungkin.	Praktik terbaik untuk Amazon EC2 Spot
Batas pengeluaran untuk armada Anda	Apakah Anda ingin membatasi berapa banyak yang akan Anda bayar untuk armada Anda per jam?	Tetapkan batas pengeluaran untuk Armada EC2 atau Armada Spot
Jenis instans dan pemilihan	Apakah Anda ingin menentukan jenis instans di armada Anda, atau membiarkan Amazon EC2 memilih jenis instans yang memenuhi persyaratan aplikasi Anda?	Tentukan atribut untuk pemilihan tipe contoh untuk Armada EC2 atau Armada Spot

Opsi Konfigurasi	Pertanyaan	Dokumentasi
tipe instans berbasis atribut		
Pembobotan instans	Apakah Anda ingin menetapkan bobot ke setiap jenis instans untuk mewakili kapasitas komputasi dan kinerjanya, sehingga Amazon EC2 dapat memilih kombinasi jenis instans yang tersedia untuk memenuhi kapasitas target yang Anda inginkan?	Gunakan pembobotan instans untuk mengelola biaya dan kinerja Armada EC2 atau Armada Spot Anda
Strategi alokasi	Apakah Anda ingin memutuskan apakah akan mengoptimalkan kapasitas, harga, atau jenis instans yang tersedia untuk digunakan untuk Instans Spot dan Instans Sesuai Permintaan di armada Anda?	Gunakan strategi alokasi untuk menentukan bagaimana Armada EC2 atau Armada Spot memenuhi kapasitas Spot dan Sesuai Permintaan
Penyeimbangan Ulang Kapasitas	Apakah Anda ingin armada Anda mengganti Instans Spot yang berisiko secara otomatis?	Gunakan Rebalancing Kapasitas di Armada EC2 dan Armada Spot untuk mengganti Instans Spot yang berisiko
Reservasi Kapasitas Sesuai Permintaan	Apakah Anda ingin memesan kapasitas untuk Instans Sesuai Permintaan di armada Anda?	Gunakan Reservasi Kapasitas untuk memesan kapasitas Sesuai Permintaan di Armada EC2

Jenis permintaan Armada EC2 dan Armada Spot

Jenis permintaan untuk Armada EC2 atau Armada Spot menentukan apakah permintaan tersebut sinkron atau asinkron, dan apakah itu permintaan satu kali untuk kapasitas target yang diinginkan atau upaya berkelanjutan untuk mempertahankan kapasitas dari waktu ke waktu. Saat mengonfigurasi armada Anda, Anda harus menentukan jenis permintaan.

Armada EC2 dan Armada Spot menawarkan dua jenis permintaan: `request` dan`maintain`. Selain itu, Armada EC2 menawarkan jenis permintaan ketiga yang disebut`instant`.

Jenis permintaan armada

`instant`(Hanya Armada EC2)

Jika Anda mengonfigurasi tipe permintaan sebagai `instant`, Armada EC2 akan mengajukan permintaan satu kali sinkron untuk kapasitas yang Anda inginkan. Dalam respons API, ia mengembalikan instance yang diluncurkan dan memberikan kesalahan untuk instance yang tidak dapat diluncurkan. Untuk informasi selengkapnya, lihat Konfigurasikan jenis Armada EC2 instant.

`request`

Jika Anda mengonfigurasi jenis permintaan sebagai`request`, armada menempatkan permintaan satu kali asinkron untuk kapasitas yang Anda inginkan. Jika kapasitas berkurang karena gangguan Spot, armada tidak berupaya mengisi Instans Spot, juga tidak mengirimkan permintaan di kumpulan kapasitas Spot alternatif jika kapasitas tidak tersedia. Saat membuat Armada Spot tipe `request` menggunakan konsol, kosongkan kotak centang Pertahankan kapasitas target.

`maintain` (default)

Jika Anda mengonfigurasi jenis permintaan sebagai`maintain`, armada akan menempatkan permintaan asinkron untuk kapasitas yang Anda inginkan, dan mempertahankannya dengan mengisi ulang Instans Spot yang terputus secara otomatis. Saat membuat Armada Spot tipe `maintain` menggunakan konsol, pilih kotak centang Pertahankan kapasitas target

Konfigurasikan jenis Armada EC2 instant

Armada EC2 tipe instan adalah permintaan satu kali sinkron yang hanya membuat satu upaya untuk meluncurkan kapasitas yang Anda inginkan. Respons API mencantumkan instans yang diluncurkan, bersama dengan kesalahan untuk instans yang tidak dapat diluncurkan. Terdapat beberapa keuntungan dari penggunaan Armada EC2 tipe instan, yang dijelaskan dalam artikel ini. Contoh konfigurasi disediakan di akhir artikel.

Untuk beban kerja yang memerlukan API khusus peluncuran untuk meluncurkan instans EC2, Anda dapat menggunakan API. RunInstances Namun, dengan RunInstances, Anda hanya dapat meluncurkan Instans Sesuai Permintaan atau Instans Spot, tetapi tidak keduanya dalam permintaan yang sama. Selanjutnya, ketika Anda menggunakan RunInstances untuk meluncurkan Instans Spot, permintaan Instans Spot Anda terbatas pada satu jenis instans dan satu Availability Zone. API ini

menargetkan kolam kapasitas Spot (set instans yang tidak digunakan dengan tipe instans dan Zona ketersediaan yang sama). Jika kumpulan kapasitas Spot tidak memiliki kapasitas Instans Spot yang memadai untuk permintaan Anda, RunInstances panggilan gagal.

Alih-alih menggunakan RunInstances untuk meluncurkan Instans Spot, sebaiknya gunakan CreateFleet API dengan `type` parameter yang disetel `instant` untuk manfaat berikut:

- Luncurkan Instans Sesuai Permintaan dan Instans Spot dalam satu permintaan. Armada EC2 dapat meluncurkan Instans Sesuai Permintaan, Instans Spot, atau keduanya. Permintaan Instans Spot terpenuhi jika terdapat kapasitas yang tersedia dan harga maksimum per jam untuk permintaan Anda melebihi harga Spot.
- Menambah ketersediaan Instans Spot. Dengan menggunakan Armada EC2 tipe `instant`, Anda dapat meluncurkan Instans Spot mengikuti praktik terbaik Spot dengan keuntungan yang dihasilkan:
  - Praktik terbaik Spot: Bersikaplah fleksibel terkait tipe instans dan Zona Ketersediaan.

    Keuntungan: Dengan menentukan beberapa tipe instans dan Zona Ketersediaan, Anda menambah jumlah kolam kapasitas Spot. Hal ini memberi layanan Spot kesempatan yang lebih baik untuk menemukan dan mengalokasikan kapasitas komputasi Spot yang Anda inginkan. Praktik terbaiknya adalah fleksibel pada setidaknya 10 tipe instans untuk setiap beban kerja dan memastikan semua Zona Ketersediaan dikonfigurasi untuk digunakan di VPC Anda.
  - Spot best practice: Gunakan strategi price-capacity-optimized alokasi.

    Manfaat: Strategi `price-capacity-optimized` alokasi mengidentifikasi instance dari kumpulan kapasitas Spot yang paling tersedia, dan kemudian secara otomatis menyediakan instance dari harga terendah dari kumpulan ini. Karena kapasitas Instans Spot Anda bersumber dari kolam dengan kapasitas optimal, hal ini mengurangi kemungkinan bahwa Instans Spot Anda akan terinterupsi saat Amazon EC2 membutuhkan kapasitas kembali.
- Dapatkan akses ke set kemampuan yang lebih luas. Untuk beban kerja yang memerlukan API khusus peluncuran, dan di mana Anda lebih suka mengelola siklus hidup instans Anda daripada membiarkan Armada EC2 mengelolanya untuk Anda, gunakan jenis Armada EC2 alih-alih API. `instant` RunInstances Armada EC2 menyediakan serangkaian kemampuan yang lebih luas daripada RunInstances, seperti yang ditunjukkan dalam contoh berikut. Untuk semua beban kerja lainnya, Anda harus menggunakan Amazon EC2 Auto Scaling karena menyediakan set fitur yang lebih komprehensif untuk berbagai macam beban kerja, seperti aplikasi yang didukung ELB, beban kerja terkontainerisasi, dan tugas pemrosesan antrean.

Anda dapat menggunakan Armada EC2 tipe instan untuk meluncurkan instans ke Blok Kapasitas. Untuk informasi selengkapnya, lihat Tutorial: Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Blok Kapasitas.

AWS layanan seperti Amazon EC2 Auto Scaling dan Amazon EMR menggunakan EC2 Fleet tipe instan untuk meluncurkan instans EC2.

Prasyarat untuk Armada EC2 tipe instan

Untuk prasyarat guna membuat Armada EC2, lihat Prasyarat Armada EC2.

Cara kerja Armada EC2

Saat bekerja dengan Armada EC2 tipe `instant`, urutan peristiwanya adalah sebagai berikut:

1. Konfigurasi: Konfigurasikan jenis CreateFleetpermintaan sebagai`instant`. Untuk informasi selengkapnya, lihat Membuat Armada EC2. Perhatikan bahwa setelah melakukan panggilan API, Anda tidak dapat memodifikasinya.
2. Permintaan: Saat Anda melakukan panggilan API, Amazon EC2 menempatkan permintaan satu kali sinkron untuk kapasitas yang Anda inginkan.
3. Respons: Respons API mencantumkan instance yang diluncurkan, bersama dengan kesalahan untuk instance yang tidak dapat diluncurkan.
4. Jelaskan: Anda dapat mendeskripsikan Armada EC2 Anda, daftar instans yang terkait dengan Armada EC2 Anda, dan melihat riwayat Armada EC2 Anda.
5. Mengakhiri instance: Anda dapat menghentikan instance kapan saja.
6. Hapus permintaan armada: Permintaan armada dapat dihapus secara manual atau otomatis:
   - Petunjuk: Anda dapat menghapus permintaan armada setelah instans diluncurkan.

     Perhatikan bahwa `instant` armada yang dihapus dengan instance yang sedang berjalan tidak didukung. Saat Anda menghapus `instant` armada, Amazon EC2 secara otomatis menghentikan semua instance-nya. Untuk armada dengan lebih dari 1000 instance, permintaan penghapusan mungkin gagal. Jika armada Anda memiliki lebih dari 1000 instans, pertama-tama hentikan sebagian besar instans secara manual, sisakan 1000 atau kurang. Kemudian hapus armada, dan instance yang tersisa akan dihentikan secara otomatis.
   - Otomatis: Amazon EC2 menghapus permintaan armada beberapa saat setelah:
     - Semua instance dihentikan.
     - Armada gagal meluncurkan instance apa pun.

Contoh

Contoh berikut menunjukkan cara menggunakan Armada EC2 tipe `instant` pada berbagai kasus penggunaan. Untuk informasi selengkapnya tentang penggunaan parameter CreateFleet API EC2, lihat CreateFleetdi Referensi API Amazon EC2.

Contoh

- Contoh 1: Meluncurkan Instans Spot dengan strategi alokasi yang dioptimalkan kapasitas
- Contoh 2: Meluncurkan satu Instans Spot dengan strategi alokasi yang dioptimalkan kapasitas
- Contoh 3: Meluncurkan Instans Spot menggunakan pembobotan instans
- Contoh 4: Luncurkan Instans Spot dalam Zona Ketersediaan tunggal
- Contoh 5: Meluncurkan Instans Spot satu tipe instans dalam satu Zona Ketersediaan
- Contoh 6: Meluncurkan Instans Spot hanya jika kapasitas target minimum dapat diluncurkan
- Contoh 7: Meluncurkan Instans Spot hanya jika kapasitas target minimum dapat diluncurkan dari Tipe Instans yang sama dalam satu Zona Ketersediaan
- Contoh 8: Meluncurkan instans dengan banyak Templat Peluncuran
- Contoh 9: Meluncurkan Instans Spot dengan basis Instans Sesuai Permintaan
- Contoh 10: Meluncurkan Instans Spot menggunakan strategi alokasi yang dioptimalkan kapasitas dengan basis Instans Sesuai Permintaan menggunakan Reservasi Kapasitas dan strategi alokasi yang diprioritaskan
- Contoh 11: Luncurkan Instans Spot menggunakan strategi capacity-optimized-prioritized alokasi
- Contoh 12: Menentukan parameter Systems Manager, bukan ID AMI

Contoh 1: Meluncurkan Instans Spot dengan strategi alokasi yang dioptimalkan kapasitas

Contoh berikut menentukan parameter yang diperlukan dalam Armada EC2 tipe `instant`: templat peluncuran, kapasitas target, opsi pembelian default, dan penimpaan templat peluncuran.

- Templat peluncuran diidentifikasi dengan nama templat dan nomor versi peluncurannya.
- 12 penggantian templat peluncuran menentukan 4 tipe instans yang berbeda dan 3 subnet berbeda, masing-masing di Zona Ketersediaan terpisah. Setiap tipe instans dan kombinasi subnet menentukan kolam kapasitas Spot, sehingga menghasilkan 12 kolam kapasitas Spot.
- Kapasitas target untuk armada adalah 20 instans.

- Opsi pembelian default adalah `spot`, yang menghasilkan armada yang berupaya meluncurkan 20 Instans Spot ke kolam kapasitas Spot dengan kapasitas optimal untuk jumlah instans yang diluncurkan.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 2: Meluncurkan satu Instans Spot dengan strategi alokasi yang dioptimalkan kapasitas

Anda dapat meluncurkan satu Instans Spot secara optimal pada satu waktu dengan melakukan beberapa jenis panggilan API Armada EC2`instant`, dengan menyetel TotalTargetCapacity ke 1.

Contoh berikut menentukan parameter yang diperlukan dalam Armada EC2 tipe instan: templat peluncuran, kapasitas target, opsi pembelian default, dan penimpaan templat peluncuran. Templat peluncuran diidentifikasi dengan nama templat dan nomor versi peluncurannya. 12 penimpaan templat peluncuran memiliki 4 tipe instans yang berbeda dan 3 subnet yang berbeda, masing-masing di Zona Ketersediaan yang terpisah. Kapasitas target untuk armada adalah 1 instans, dan opsi pembelian default adalah spot, yang mengakibatkan armada berupaya meluncurkan Instans

Spot dari salah satu dari 12 kolam kapasitas Spot berdasarkan strategi alokasi yang dioptimalkan kapasitas, untuk meluncurkan Instans Spot dari kolam kapasitas dengan ketersediaan paling tinggi.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 3: Meluncurkan Instans Spot menggunakan pembobotan instans

Contoh berikut menggunakan pembobotan instans, yang berarti harga adalah per unit jam, bukan per jam instans. Setiap konfigurasi peluncuran mencantumkan jenis instans yang berbeda dan bobot yang berbeda berdasarkan berapa banyak unit beban kerja yang dapat dijalankan pada instance dengan asumsi unit beban kerja memerlukan memori 15 GB dan 4 v. CPUs Misalnya m5.xlarge (memori 4 v CPUs dan 16 GB) dapat menjalankan satu unit dan berbobot 1, m5.2xlarge (8 v CPUs dan 32 GB memori) dapat menjalankan 2 unit dan berbobot 2, dan seterusnya. Total kapasitas target diatur ke 40 unit. Opsi pembelian default adalah spot, dan strategi alokasi dioptimalkan kapasitas, yang menghasilkan 40 m5.xlarge (40 dibagi 1), 20 m5.2xlarge (40 dibagi 2), 10 m5.4xlarge (40 dibagi 4), 5 m5.8xlarge (40 dibagi 8), atau campuran tipe instans dengan bobot yang ditambahkan ke kapasitas yang diinginkan berdasarkan kapasitas strategi alokasi yang dioptimalkan kapasitas.

Untuk informasi selengkapnya, lihat Gunakan pembobotan instans untuk mengelola biaya dan kinerja Armada EC2 atau Armada Spot Anda.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":2
```

```
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

Contoh 4: Luncurkan Instans Spot dalam Zona Ketersediaan tunggal

Anda dapat mengonfigurasi armada untuk meluncurkan semua instance dalam satu Availability Zone dengan menyetel opsi Spot SingleAvailabilityZone ke true.

12 penimpaan templat peluncuran memiliki tipe dan subnet instans yang berbeda (masing–masing di Zona Ketersediaan terpisah), tetapi kapasitas tertimbangnya sama. Total kapasitas target adalah 20 instans, opsi pembelian default adalah spot, dan strategi alokasi Spot dioptimalkan kapasitas. Armada EC2 meluncurkan 20 Instans Spot semuanya dalam satu AZ, dari kolam kapasitas Spot dengan kapasitas optimal menggunakan spesifikasi peluncuran.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
```

```
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 5: Meluncurkan Instans Spot satu tipe instans dalam satu Zona Ketersediaan

Anda dapat mengonfigurasi armada untuk meluncurkan semua instance dari jenis instans yang sama dan dalam Availability Zone tunggal dengan menyetel SpotOptions SingleInstanceType ke true dan SingleAvailabilityZone true.

12 penimpaan templat peluncuran memiliki tipe dan subnet instans yang berbeda (masing–masing di Zona Ketersediaan terpisah), tetapi kapasitas tertimbangnya sama. Total kapasitas target adalah 20 instans, opsi pembelian default adalah spot, strategi alokasi Spot dioptimalkan kapasitas. Armada EC2 meluncurkan 20 Instans Spot dengan tipe instans yang sama, semuanya dalam satu AZ dari kolam Instans Spot dengan kapasitas optimal menggunakan spesifikasi peluncuran.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
```

```
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 6: Meluncurkan Instans Spot hanya jika kapasitas target minimum dapat diluncurkan

Anda dapat mengonfigurasi armada untuk meluncurkan instance hanya jika kapasitas target minimum dapat diluncurkan dengan menyetel opsi Spot MinTargetCapacity ke kapasitas target minimum yang ingin Anda luncurkan bersama.

Saat menentukan MinTargetCapacity, Anda harus menentukan setidaknya satu dari parameter ini: SingleInstanceType atau SingleAvailabilityZone. Dalam contoh ini, SingleInstanceType ditentukan, sehingga semua 20 instance harus menggunakan jenis instance yang sama.

12 penimpaan templat peluncuran memiliki tipe dan subnet instans yang berbeda (masing–masing di Zona Ketersediaan terpisah), tetapi kapasitas tertimbangnya sama. Total kapasitas target dan kapasitas target minimum keduanya disetel ke 20 instance, opsi pembelian default adalah spot, dan strategi alokasi Spot dioptimalkan kapasitas. Armada EC2 meluncurkan 20 Instans Spot dari kolam kapasitas Spot dengan kapasitas optimal menggunakan penimpaan templat peluncuran, hanya jika dapat meluncurkan semua 20 instans pada saat yang bersamaan.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
```

```
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 7: Meluncurkan Instans Spot hanya jika kapasitas target minimum dapat diluncurkan dari Tipe Instans yang sama dalam satu Zona Ketersediaan

Anda dapat mengonfigurasi armada untuk meluncurkan instance hanya jika kapasitas target minimum dapat diluncurkan dengan satu jenis instans dalam satu Availability Zone dengan menyetel opsi Spot MinTargetCapacity ke kapasitas target minimum yang ingin Anda luncurkan bersama SingleInstanceType dan SingleAvailabilityZone opsi.

12 spesifikasi peluncuran yang menimpa templat peluncuran, memiliki tipe instans dan subnet yang berbeda (masing-masing di Zona Ketersediaan yang terpisah), tetapi kapasitas tertimbangnya sama. Total kapasitas target dan kapasitas target minimum keduanya disetel ke 20 instance, opsi pembelian default adalah spot, strategi alokasi Spot dioptimalkan kapasitas, benar dan benar SingleInstanceType . SingleAvailabilityZone Armada EC2 meluncurkan 20 Instans Spot dengan tipe instans yang sama, semuanya dalam satu AZ dari kolam kapasitas Spot dengan kapasitas optimal menggunakan spesifikasi peluncuran, hanya jika dapat meluncurkan semua 20 instans pada saat yang bersamaan.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
```

```
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 8: Meluncurkan instans dengan banyak Templat Peluncuran

Anda dapat mengonfigurasi armada untuk meluncurkan instans dengan spesifikasi peluncuran yang berbeda untuk berbagai tipe instans atau grup tipe instans, dengan menentukan banyak templat

peluncuran. Dalam contoh ini kita ingin agar memiliki ukuran volume EBS yang berbeda untuk tipe instans yang berbeda dan dikonfigurasi dalam templat peluncuran ec2-fleet-lt-4xl, ec2-fleet-lt-9xl, dan ec2-fleet-lt-18xl.

Dalam contoh ini, kita menggunakan 3 templat peluncuran yang berbeda untuk 3 tipe instans berdasarkan ukurannya. Spesifikasi peluncuran yang ditimpa pada semua templat peluncuran menggunakan bobot instans berdasarkan vCPU pada tipe instans. Total kapasitas target adalah 144 instans, opsi pembelian default adalah spot, dan strategi alokasi Spot dioptimalkan kapasitas. Armada EC2 dapat meluncurkan 9 c5n.4xlarge (144 dibagi 16) menggunakan templat peluncuran ec2-fleet-4xl atau 4 c5n.9xlarge (144 dibagi 36) menggunakan template peluncuran ec2-fleet-9xl, atau 2 c5n.18xlarge (144 dibagi 72) menggunakan templat peluncuran ec2-fleet-18xl, atau campuran tipe instans dengan bobot yang ditambahkan ke kapasitas yang diinginkan berdasarkan strategi alokasi yang dioptimalkan kapasitas.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":72
            }
         ]
      },
```

```
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-9xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":36
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-4xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":16
            }
```

```
        ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 144,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 9: Meluncurkan Instans Spot dengan basis Instans Sesuai Permintaan

Contoh berikut menentukan total kapasitas target dari 20 instans untuk armada tersebut dan kapasitas target dari 5 Instans Sesuai Permintaan. Opsi pembelian default adalah spot. Armada meluncurkan 5 Instans Sesuai Permintaan sebagaimana ditentukan, tetapi perlu meluncurkan 15 instans lagi untuk memenuhi total kapasitas target. Opsi pembelian untuk selisih dihitung sebagai TotalTargetCapacity — OnDemandTargetCapacity = DefaultTargetCapacityType, yang menghasilkan peluncuran armada 15 Instans Spot membentuk salah satu dari 12 kumpulan kapasitas Spot berdasarkan strategi alokasi yang dioptimalkan kapasitas.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
```

```
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
   "TargetCapacitySpecification": {
       "TotalTargetCapacity": 20,
       "OnDemandTargetCapacity": 5,
       "DefaultTargetCapacityType": "spot"
```

```
    },
    "Type": "instant"
}
```

Contoh 10: Meluncurkan Instans Spot menggunakan strategi alokasi yang dioptimalkan kapasitas dengan basis Instans Sesuai Permintaan menggunakan Reservasi Kapasitas dan strategi alokasi yang diprioritaskan

Anda dapat mengonfigurasi armada untuk menggunakan Reservasi Kapasitas Sesuai Permintaan terlebih dahulu saat meluncurkan basis Instans Sesuai Permintaan dengan tipe kapasitas target default sebagai spot dengan menyetel strategi penggunaan untuk Reservasi Kapasitas. use-capacity-reservations-first Jika lebih dari satu kolam instans memiliki Reservasi Kapasitas yang tidak terpakai, strategi alokasi Sesuai Permintaan akan diterapkan. Dalam contoh ini, strategi alokasi Sesuai Permintaan diprioritaskan.

Dalam contoh ini, terdapat 6 Reservasi Kapasitas yang tidak terpakai yang tersedia. Jumlah tersebut kurang dari kapasitas Sesuai Permintaan target armada 10 instans Sesuai Permintaan.

Akun tersebut memiliki 6 Reservasi Kapasitas yang tidak terpakai dalam 2 kolam. Jumlah Cadangan Kapasitas di setiap kumpulan ditunjukkan dengan AvailableInstanceCount.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Konfigurasi armada berikut hanya menampilkan konfigurasi terkait untuk contoh ini. Strategi alokasi On-Demand diprioritaskan, dan strategi penggunaan untuk Reservasi Kapasitas adalah. use-capacity-reservations-first Strategi alokasi Spot dioptimalkan kapasitas. Total kapasitas target adalah 20, kapasitas target Sesuai Permintaan adalah 10, dan tipe kapasitas target default adalah spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
```

```
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 5.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 6.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 7.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 8.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 9.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 10.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 11.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 12.0
         }
      ]
   }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
```

```
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Setelah Anda membuat armada instan menggunakan konfigurasi sebelumnya, 20 instans berikut ini diluncurkan untuk memenuhi kapasitas target:

- 7 Instans Sesuai Permintaan c5.large di us-east-1a – c5.large di us-east-1a diprioritaskan terlebih dahulu, dan terdapat 3 Reservasi Kapasitas c5.large yang tidak terpakai. Reservasi Kapasitas digunakan terlebih dahulu untuk meluncurkan 3 Instans Sesuai Permintaan dan 4 Instans Sesuai Permintaan tambahan diluncurkan sesuai dengan strategi alokasi Sesuai Permintaan, yang diprioritaskan dalam contoh ini.
- 3 m5.large Instans Sesuai Permintaan di us-east-1a — m5.large di us-east-1a diprioritaskan kedua, dan ada 3 Reservasi Kapasitas m5.large yang tidak terpakai yang tersedia.
- 10 Instans Spot dari salah satu dari 12 kolam kapasitas Spot yang memiliki kapasitas optimal sesuai dengan strategi alokasi yang dioptimalkan kapasitas.

Setelah armada diluncurkan, Anda dapat berlari describe-capacity-reservationsuntuk melihat berapa banyak Reservasi Kapasitas yang tidak terpakai yang tersisa. Dalam contoh ini, Anda akan melihat respons berikut, yang menunjukkan bahwa semua Reservasi Kapasitas c5.large dan m5.large telah digunakan.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

Contoh 11: Luncurkan Instans Spot menggunakan strategi capacity-optimized-prioritized alokasi

Contoh berikut menentukan parameter yang diperlukan dalam Armada EC2 tipe instan: templat peluncuran, kapasitas target, opsi pembelian default, dan penimpaan templat peluncuran. Templat peluncuran diidentifikasi dengan nama templat dan nomor versi peluncurannya. 12 spesifikasi peluncuran yang menimpa templat peluncuran memiliki 4 tipe instans berbeda dengan prioritas yang ditetapkan, dan 3 subnet berbeda, masing–masing di Zona Ketersediaan yang terpisah. Kapasitas target untuk armada adalah 20 instance, dan opsi pembelian default adalah spot, yang mengakibatkan armada mencoba meluncurkan 20 Instans Spot dari salah satu dari 12 kumpulan kapasitas Spot berdasarkan strategi capacity-optimized-prioritized alokasi, yang menerapkan prioritas berdasarkan upaya terbaik, tetapi mengoptimalkan kapasitas terlebih dahulu.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 2.0
```

```
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 2.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 4.0
            }
         ]
      }
   ],
```

```
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 12: Menentukan parameter Systems Manager, bukan ID AMI

Contoh berikut menggunakan template peluncuran untuk menentukan konfigurasi untuk instance di armada. Dalam contoh ini, untuk`ImageId`, alih-alih menentukan ID AMI, AMI direferensikan dengan parameter Manajer Sistem. Pada peluncuran instance, parameter Systems Manager akan diselesaikan ke ID AMI.

Dalam contoh ini, parameter Systems Manager ditentukan dalam format yang valid:`resolve:ssm:golden-ami`. Ada format lain yang valid untuk parameter Systems Manager. Untuk informasi selengkapnya, lihat Gunakan parameter Systems Manager alih-alih ID AMI.

> **Note**
>
> Tipe armada harus bertipe `instant`. Jenis armada lainnya tidak mendukung penetapan parameter Manajer Sistem, bukan ID AMI.

```
{
    "LaunchTemplateData": {
        "ImageId": "resolve:ssm:golden-ami",
        "InstanceType": "m5.4xlarge",
        "TagSpecifications": [{
            "ResourceType": "instance",
            "Tags": [{
                "Key": "Name",
                "Value": "webserver"
            }]
        }]
    }
}
```

Tetapkan batas pengeluaran untuk Armada EC2 atau Armada Spot

Anda dapat menetapkan batas berapa banyak yang bersedia Anda belanjakan per jam untuk Armada EC2 atau Armada Spot Anda. Ketika batas pengeluaran Anda tercapai, armada berhenti meluncurkan instance, bahkan jika kapasitas target belum tercapai.

Ada batasan pengeluaran terpisah untuk Instans On-Demand dan Instans Spot.

Untuk mengonfigurasi batas pengeluaran untuk Instans Sesuai Permintaan dan Instans Spot di Armada EC2 Anda

Gunakan perintah create-fleet dan parameter berikut:

- Untuk Instans Sesuai Permintaan: Dalam `OnDemandOptions` struktur, tentukan batas pengeluaran Anda di lapangan. `MaxTotalPrice`
- Untuk Instans Spot: Dalam `SpotOptions` struktur, tentukan batas pengeluaran Anda di `MaxTotalPrice` bidang.

Untuk mengonfigurasi batas pengeluaran untuk Instans Sesuai Permintaan dan Instans Spot di Armada Spot Anda

Anda dapat menggunakan konsol Amazon EC2 atau AWS CLI untuk mengonfigurasi batas pengeluaran Anda.

(Konsol) Saat membuat Armada Spot, pilih kotak centang Setel biaya maksimum untuk Instans Spot, lalu masukkan nilai untuk Tetapkan biaya maksimal Anda (per jam). Untuk informasi lebih lanjut, lihat langkah 6.e. diMembuat permintaan Armada Spot menggunakan parameter yang ditentukan.

(AWS CLI) Gunakan request-spot-fleetperintah dan parameter berikut:

- Untuk Instans Sesuai Permintaan: Tentukan batas pengeluaran Anda di bidang. `OnDemandMaxTotalPrice`
- Untuk Instans Spot: Tentukan batas pengeluaran Anda di `SpotMaxTotalPrice` bidang.

Contoh

Contoh berikut menunjukkan dua skenario berbeda. Pada contoh pertama, armada berhenti meluncurkan Instans Sesuai Permintaan ketika telah memenuhi kapasitas target yang ditetapkan

untuk Instans On-Demand (). `OnDemandTargetCapacity` Pada contoh kedua, armada berhenti meluncurkan Instans Sesuai Permintaan ketika telah mencapai jumlah maksimum yang bersedia Anda bayarkan per jam untuk Instans Sesuai Permintaan (). `MaxTotalPrice`

Contoh: Berhenti meluncurkan Instans Sesuai Permintaan saat kapasitas target tercapai

Dengan pertimbangan permintaan untuk Instans Sesuai Permintaan `m4.large`, jika:

- Harga Sesuai Permintaan: 0,10 USD per jam
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

Armada meluncurkan 10 Instans Sesuai Permintaan karena total $1,00 (10 instans x $0,10) tidak melebihi $1,50 untuk Instans Sesuai Permintaan. `MaxTotalPrice`

Contoh: Berhenti meluncurkan Instans Sesuai Permintaan ketika total harga maksimum tercapai

Dengan pertimbangan permintaan untuk Instans Sesuai Permintaan `m4.large`, jika:

- Harga Sesuai Permintaan: 0,10 USD per jam
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Jika armada meluncurkan kapasitas target On-Demand (10 Instans On-Demand), total biaya per jam akan menjadi $1,00. Ini lebih dari jumlah (0,80 USD) yang ditentukan untuk `MaxTotalPrice` untuk Instans Sesuai Permintaan. Untuk mencegah pengeluaran lebih dari yang Anda bayarkan, armada hanya meluncurkan 8 Instans Sesuai Permintaan (di bawah kapasitas target On-Demand) karena peluncuran lebih banyak akan melebihi untuk Instans Sesuai `MaxTotalPrice` Permintaan.

Instance kinerja yang dapat melonjak

Jika Anda meluncurkan Instans Spot menggunakan tipe instans performa yang dapat melonjak, serta jika Anda berencana untuk segera menggunakan Instans Spot performa yang dapat melonjak dan untuk durasi yang singkat, tanpa waktu idle untuk memperoleh kredit CPU, kami menyarankan Anda untuk meluncurkannya dalam mode Standar guna menghindari pembayaran biaya yang lebih tinggi. Jika Anda meluncurkan Instans Spot performa yang dapat melonjak dalam Mode tak terbatas dan langsung melonjakkan CPU, Anda akan menghabiskan kredit surplus untuk lonjakan. Jika Anda menggunakan instans untuk durasi yang singkat, instans tersebut tidak memiliki waktu untuk

mengkumulasi kredit CPU untuk membayar kredit surplus, dan Anda akan dikenai biaya untuk kredit surplus saat Anda mengakhiri instans.

Mode tidak terbatas cocok untuk Instans Spot dengan performa yang dapat melonjak hanya jika instans tersebut berjalan cukup lama untuk mengakumlasi kredit CPU untuk lonjakan. Jika tidak, pembayaran kredit surplus membuat Instans Spot performa yang dapat melonjak lebih mahal daripada menggunakan instans lain. Untuk informasi selengkapnya, lihat Kapan menggunakan mode tak terbatas versus CPU tetap.

Kredit peluncuran dimaksudkan untuk memberikan pengalaman peluncuran awal yang produktif bagi instans T2 dengan menyediakan sumber daya komputasi yang memadai untuk mengonfigurasi instans. Peluncuran berulang dari instans T2 untuk mengakses kredit peluncuran baru tidak diizinkan. Jika Anda memerlukan CPU berkelanjutan, Anda dapat memperoleh kredit (dengan berhenti selama beberapa periode), menggunakan mode Tak Terbatas untuk Instans Spot T2, atau menggunakan tipe instans dengan CPU khusus.

Tentukan atribut untuk pemilihan tipe contoh untuk Armada EC2 atau Armada Spot

Saat membuat Armada EC2 atau Armada Spot, Anda harus menentukan satu atau beberapa jenis instans untuk mengonfigurasi Instans Sesuai Permintaan dan Instans Spot di armada. Sebagai alternatif untuk menentukan tipe instans secara manual, Anda dapat menentukan atribut yang harus dimiliki instans, dan Amazon EC2 akan mengidentifikasi semua tipe instans dengan atribut tersebut. Hal ini dikenal sebagai pemilihan tipe instans berbasis atribut. Misalnya, Anda dapat menentukan jumlah minimum dan maksimum v yang CPUs diperlukan untuk instans Anda, dan armada akan meluncurkan instans menggunakan jenis instans yang tersedia yang memenuhi persyaratan vCPU tersebut.

Pemilihan tipe instans berbasis atribut sangat ideal untuk beban kerja dan kerangka kerja yang fleksibel dalam menentukan tipe instans yang digunakan, seperti ketika menjalankan kontainer atau armada web, memproses big data, dan mengimplementasikan alat integrasi dan deployment berkelanjutan (CI/CD).

Keuntungan

Pemilihan tipe instans berbasis atribut memiliki keuntungan berikut:

- Mudah menggunakan jenis instans yang tepat — Dengan begitu banyak jenis instans yang tersedia, menemukan jenis instans yang tepat untuk beban kerja Anda dapat memakan waktu.

Saat Anda menentukan atribut instans, tipe instans akan secara otomatis memiliki atribut yang diperlukan untuk beban kerja Anda.

- Konfigurasi yang disederhanakan — Untuk menentukan beberapa tipe instance secara manual untuk armada, Anda harus membuat penggantian template peluncuran terpisah untuk setiap jenis instans. Namun, dengan pemilihan tipe instans berbasis atribut, untuk menyediakan banyak tipe instans, Anda hanya perlu menentukan atribut instans dalam templat peluncuran atau dalam penimpaan templat peluncuran.
- Penggunaan otomatis tipe instans baru — Saat Anda menentukan atribut instance daripada tipe instans, armada Anda dapat menggunakan tipe instance generasi yang lebih baru saat dirilis, "pemeriksaan masa depan" konfigurasi armada.
- Fleksibilitas tipe instans — Saat Anda menentukan atribut instance daripada tipe instans, armada dapat memilih dari berbagai jenis instans untuk meluncurkan Instans Spot, yang mengikuti praktik terbaik Spot dari fleksibilitas tipe instans.

Topik

- Cara kerja pemilihan tipe instans berbasis atribut
- Perlindungan harga
- Perlindungan kinerja
- Pertimbangan-pertimbangan
- Membuat Armada EC2 dengan pemilihan tipe instans berbasis atribut
- Buat Armada Spot dengan pemilihan tipe instans berbasis atribut
- Contoh konfigurasi Armada EC2 yang valid dan tidak valid
- Contoh konfigurasi Armada Spot yang valid dan tidak valid
- Melihat pratinjau tipe instans dengan atribut tertentu

Cara kerja pemilihan tipe instans berbasis atribut

Untuk menggunakan pemilihan tipe instans berbasis atribut dalam konfigurasi armada, Anda mengganti daftar tipe instans dengan daftar atribut instans yang dibutuhkan oleh instans Anda. Armada EC2 atau Armada Spot akan meluncurkan instans pada setiap jenis instans yang tersedia yang memiliki atribut instans tertentu.

Topik

- Tipe atribut instans

- Tempat mengonfigurasi pemilihan tipe instans berbasis atribut
- Bagaimana Armada EC2 atau Armada Spot menggunakan pemilihan tipe instans berbasis atribut saat menyediakan armada

Tipe atribut instans

Ada beberapa atribut instance yang dapat Anda tentukan untuk mengekspresikan persyaratan komputasi Anda, seperti:

- Jumlah vCPU — Jumlah minimum dan maksimum v CPUs per instance.
- Memori — Minimum dan GiBs maksimum memori per instance.
- Penyimpanan lokal — Apakah akan menggunakan EBS atau volume penyimpanan instans untuk penyimpanan lokal.
- Kinerja burstable — Apakah akan menggunakan keluarga instans T, termasuk tipe T4G, T3a, T3, dan T2.

Untuk deskripsi setiap atribut dan nilai default, lihat InstanceRequirementsdi Referensi API Amazon EC2.

Tempat mengonfigurasi pemilihan tipe instans berbasis atribut

Bergantung pada apakah Anda menggunakan konsol atau konsol AWS CLI, Anda dapat menentukan atribut instance untuk pemilihan jenis instans berbasis atribut sebagai berikut:

Di konsol, Anda dapat menentukan atribut instance dalam komponen konfigurasi armada berikut:

- Dalam templat peluncuran, lalu referensikan templat peluncuran dalam permintaan armada
- (Hanya Armada Spot) Dalam permintaan armada

Dalam AWS CLI, Anda dapat menentukan atribut instance dalam satu atau semua komponen konfigurasi armada berikut:

- Dalam templat peluncuran, lalu referensikan templat peluncuran dalam permintaan armada
- Dalam penimpaan templat peluncuran

Jika Anda menginginkan campuran instance yang menggunakan berbeda AMIs, Anda dapat menentukan atribut instance dalam beberapa penggantian template peluncuran. Misalnya, tipe instans yang berbeda dapat menggunakan prosesor berbasis x86 dan Arm.

- (Hanya Armada Spot) Dalam spesifikasi peluncuran

Bagaimana Armada EC2 atau Armada Spot menggunakan pemilihan tipe instans berbasis atribut saat menyediakan armada

Armada EC2 atau Armada Spot menyediakan armada dengan cara berikut:

- Ini mengidentifikasi jenis instance yang memiliki atribut tertentu.
- Ini menggunakan perlindungan harga untuk menentukan jenis instance mana yang akan dikecualikan.
- Ini menentukan kumpulan kapasitas dari mana ia akan mempertimbangkan untuk meluncurkan instance berdasarkan AWS Wilayah atau Zona Ketersediaan yang memiliki jenis instans yang cocok.
- Ini menerapkan strategi alokasi yang ditentukan untuk menentukan dari kumpulan kapasitas mana untuk meluncurkan instance.

  Perhatikan bahwa pemilihan jenis instans berbasis atribut tidak memilih kumpulan kapasitas untuk menyediakan armada; itulah tugas strategi alokasi.

  Jika Anda menentukan strategi alokasi, armada akan meluncurkan instance sesuai dengan strategi alokasi yang ditentukan.

  - Untuk Instans Spot, pemilihan jenis instans berbasis atribut mendukung kapasitas harga yang dioptimalkan, dioptimalkan kapasitas, dan strategi alokasi harga terendah. Perhatikan bahwa kami tidak merekomendasikan strategi alokasi Spot harga terendah karena memiliki risiko interupsi tertinggi untuk Instans Spot Anda.
  - Untuk Instans Sesuai Permintaan, pemilihan jenis instans berbasis atribut mendukung strategi alokasi harga terendah.
- Jika tidak ada kapasitas untuk tipe instans dengan atribut instans yang ditentukan, tidak ada instans yang dapat diluncurkan, dan armada akan mengembalikan kesalahan.

Perlindungan harga

Perlindungan harga adalah fitur yang mencegah Armada EC2 atau Armada Spot Anda menggunakan jenis instans yang Anda anggap terlalu mahal meskipun sesuai dengan atribut yang Anda tentukan. Untuk menggunakan perlindungan harga, Anda menetapkan ambang harga. Kemudian, ketika Amazon EC2 memilih jenis instans dengan atribut Anda, itu mengecualikan jenis instans dengan harga di atas ambang batas Anda.

Cara Amazon EC2 menghitung ambang harga adalah sebagai berikut:

- Amazon EC2 pertama-tama mengidentifikasi jenis instans dengan harga terendah dari yang cocok dengan atribut Anda.
- Amazon EC2 kemudian mengambil nilai (dinyatakan sebagai persentase) yang Anda tentukan untuk parameter perlindungan harga dan mengalikannya dengan harga jenis instans yang diidentifikasi. Hasilnya adalah harga yang digunakan sebagai ambang harga.

Ada ambang harga terpisah untuk Instans On-Demand dan Instans Spot.

Saat Anda membuat armada dengan pemilihan jenis instans berbasis atribut, perlindungan harga diaktifkan secara default. Anda dapat menyimpan nilai default, atau Anda dapat menentukan sendiri.

Anda juga dapat mematikan perlindungan harga. Untuk menunjukkan tidak ada ambang perlindungan harga, tentukan nilai persentase tinggi, seperti`999999`.

Topik

- Bagaimana jenis instans dengan harga terendah diidentifikasi
- Perlindungan harga Instans Sesuai Permintaan
- Perlindungan harga Spot Instance
- Tentukan ambang batas perlindungan harga

Bagaimana jenis instans dengan harga terendah diidentifikasi

Amazon EC2 menentukan harga untuk mendasarkan ambang harga dengan mengidentifikasi jenis instans dengan harga terendah dari yang cocok dengan atribut yang Anda tentukan. Ia melakukan ini dengan cara berikut:

- Ini pertama kali melihat jenis instance C, M, atau R generasi saat ini yang cocok dengan atribut Anda. Jika menemukan kecocokan, itu mengidentifikasi jenis instance dengan harga terendah.

- Jika tidak ada kecocokan, maka akan terlihat jenis instance generasi saat ini yang cocok dengan atribut Anda. Jika menemukan kecocokan, itu mengidentifikasi jenis instance dengan harga terendah.
- Jika tidak ada kecocokan, maka akan melihat jenis instance generasi sebelumnya yang cocok dengan atribut Anda, dan mengidentifikasi jenis instance dengan harga terendah.

Perlindungan harga Instans Sesuai Permintaan

Ambang batas perlindungan harga untuk jenis instans On-Demand dihitung sebagai persentase yang lebih tinggi daripada jenis instans On-Demand dengan harga terendah yang diidentifikasi (). `OnDemandMaxPricePercentageOverLowestPrice` Anda menentukan persentase yang lebih tinggi yang bersedia Anda bayar. Jika Anda tidak menentukan parameter ini, maka nilai default `20` digunakan untuk menghitung ambang perlindungan harga 20% lebih tinggi dari harga yang diidentifikasi.

Misalnya, jika harga instans On-Demand yang teridentifikasi adalah`0.4271`, dan Anda tentukan`25`, maka ambang harga 25% lebih tinggi dari`0.4271`. Itu dihitung sebagai berikut:`0.4271 * 1.25 = 0.533875`. Harga yang dihitung adalah maksimum yang bersedia Anda bayarkan untuk Instans Sesuai Permintaan, dan, dalam contoh ini, Amazon EC2 akan mengecualikan jenis instans On-Demand yang harganya lebih dari. `0.533875`

Perlindungan harga Spot Instance

Secara default, Amazon EC2 akan secara otomatis menerapkan perlindungan harga Instans Spot yang optimal untuk secara konsisten memilih dari berbagai jenis instans. Anda juga dapat mengatur sendiri perlindungan harga secara manual. Namun, membiarkan Amazon EC2 melakukannya untuk Anda dapat meningkatkan kemungkinan kapasitas Spot Anda terpenuhi.

Anda dapat menentukan perlindungan harga secara manual menggunakan salah satu opsi berikut. Jika Anda secara manual mengatur perlindungan harga, kami sarankan menggunakan opsi pertama.

- Persentase dari jenis instans On-Demand dengan harga terendah yang diidentifikasi [] `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`

  Misalnya, jika harga jenis instans On-Demand yang diidentifikasi adalah`0.4271`, dan Anda tentukan`60`, maka ambang harga adalah 60% dari. `0.4271` Itu dihitung sebagai berikut:`0.4271 * 0.60 = 0.25626`. Harga yang dihitung adalah maksimum yang bersedia Anda bayarkan untuk Instans Spot, dan, dalam contoh ini, Amazon EC2 akan mengecualikan jenis instans Spot apa pun yang harganya lebih dari. `0.25626`

- Persentase lebih tinggi dari jenis instans Spot dengan harga terendah yang diidentifikasi [] `SpotMaxPricePercentageOverLowestPrice`

  Misalnya, jika harga jenis instans Spot yang diidentifikasi adalah`0.1808`, dan Anda tentukan`25`, maka ambang harga 25% lebih tinggi dari harga`0.1808`. Itu dihitung sebagai berikut:`0.1808 * 1.25 = 0.226`. Harga yang dihitung adalah maksimum yang bersedia Anda bayarkan untuk Instans Spot, dan, dalam contoh ini, Amazon EC2 akan mengecualikan jenis instans Spot apa pun yang harganya lebih dari. `0.266` Kami tidak menyarankan menggunakan parameter ini karena harga Spot dapat berfluktuasi, dan oleh karena itu ambang batas perlindungan harga Anda mungkin juga berfluktuasi.

Tentukan ambang batas perlindungan harga

Untuk menentukan ambang perlindungan harga menggunakan AWS CLI

Saat membuat Armada EC2 atau Armada Spot menggunakan AWS CLI, konfigurasikan armada untuk pemilihan jenis instans berbasis atribut, lalu lakukan hal berikut:

- Untuk menentukan ambang batas perlindungan harga Instans Sesuai Permintaan, dalam file konfigurasi JSON, dalam struktur `InstanceRequirements`, untuk `OnDemandMaxPricePercentageOverLowestPrice`, masukkan ambang batas perlindungan harga sebagai persentase.
- Untuk menentukan ambang perlindungan harga Instans Spot, dalam file konfigurasi JSON, dalam `InstanceRequirements` struktur, tentukan salah satu parameter berikut:
  - Untuk`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, masukkan ambang perlindungan harga sebagai persentase.
  - Untuk`SpotMaxPricePercentageOverLowestPrice`, masukkan ambang perlindungan harga sebagai persentase.

Untuk informasi selengkapnya, lihat Membuat Armada EC2 dengan pemilihan tipe instans berbasis atribut atau Buat Armada Spot dengan pemilihan tipe instans berbasis atribut.

(Hanya Armada Spot) Untuk menentukan ambang perlindungan harga menggunakan konsol

Saat membuat Armada Spot di konsol, konfigurasikan armada untuk pemilihan jenis instans berbasis atribut, lalu lakukan hal berikut:

- Untuk menentukan ambang perlindungan harga Instans Sesuai Permintaan, di bawah atribut Instans tambahan, pilih Perlindungan harga sesuai permintaan, pilih Tambah atribut, lalu masukkan ambang perlindungan harga sebagai persentase.
- Untuk menentukan ambang perlindungan harga Instans Spot, atribut instance tambahan, pilih Perlindungan harga Spot, pilih Tambah atribut, pilih nilai dasar yang menjadi dasar harga Anda, lalu masukkan ambang perlindungan harga sebagai persentase.

> **Note**
>
> Saat membuat armada, jika Anda menyetel `TargetCapacityUnitType` ke `vcpu` atau`memory-mib`, ambang perlindungan harga diterapkan berdasarkan harga per vCPU atau per-memori, bukan harga per instans.

Perlindungan kinerja

Perlindungan kinerja adalah fitur yang memastikan Armada EC2 atau Armada Spot Anda menggunakan tipe instans yang mirip atau melebihi garis dasar kinerja yang ditentukan. Untuk menggunakan perlindungan kinerja, Anda menentukan keluarga instance sebagai referensi dasar. Kemampuan keluarga instance yang ditentukan menetapkan tingkat kinerja terendah yang dapat diterima. Saat Amazon EC2 memilih jenis instans untuk armada Anda, Amazon EC2 mempertimbangkan atribut yang Anda tentukan dan garis dasar performa. Jenis instans yang berada di bawah garis dasar kinerja secara otomatis dikecualikan dari seleksi, meskipun cocok dengan atribut tertentu Anda yang lain. Ini memastikan bahwa semua jenis instans yang dipilih menawarkan kinerja yang mirip atau lebih baik daripada baseline yang ditetapkan oleh keluarga instance yang ditentukan. Amazon EC2 menggunakan baseline ini untuk memandu pemilihan jenis instans, tetapi tidak ada jaminan bahwa jenis instans yang dipilih akan selalu melebihi baseline untuk setiap aplikasi.

Saat ini, fitur ini hanya mendukung kinerja CPU sebagai faktor kinerja dasar. Kinerja CPU dari prosesor CPU keluarga instance yang ditentukan berfungsi sebagai baseline kinerja, memastikan bahwa jenis instans yang dipilih mirip dengan atau melebihi baseline ini. Keluarga instance dengan prosesor CPU yang sama menghasilkan hasil penyaringan yang sama, bahkan jika kinerja jaringan atau disk mereka berbeda. Misalnya, menentukan salah satu `c6in` atau `c6i` sebagai referensi dasar akan menghasilkan hasil penyaringan berbasis kinerja yang identik karena kedua keluarga instance menggunakan prosesor CPU yang sama.

Keluarga instans yang tidak didukung

Contoh keluarga berikut tidak didukung untuk perlindungan kinerja:

- Tujuan umum: Mac1 | Mac2 | Mac2-M1Ultra | Mac2-m2 | Mac2-M2Pro | M1 | M2 | T1
- Komputasi dioptimalkan: C1
- Memori dioptimalkan: U-3TB1 | U-6TB1 | U-9tb1 | U-12tb1 | U-18tb1 | u-24tb1 | U7i-12tb | U7in-16tb | U7in-24tb | U7in-32tb
- Komputasi dipercepat: G3 | G3s | P3dn | P4d | P5
- Komputasi kinerja tinggi: hPC7g

Jika Anda mengaktifkan perlindungan performa dengan menentukan keluarga instans yang didukung, tipe instans yang dikembalikan akan mengecualikan keluarga instance yang tidak didukung di atas.

Jika Anda menetapkan keluarga instans yang tidak didukung sebagai nilai untuk kinerja dasar, API akan menampilkan respons kosong untuk GetInstanceTypesFromInstanceRequirementsdan pengecualian untuk CreateFleet,, RequestSpotFleet, ModifyFleetdan. ModifySpotFleetRequest

Contoh: Tetapkan baseline kinerja CPU

Dalam contoh berikut, persyaratan instance adalah meluncurkan dengan tipe instance yang memiliki core CPU yang berkinerja sama seperti keluarga `c6i` instance. Ini akan menyaring jenis instans dengan prosesor CPU yang kurang berkinerja, bahkan jika mereka memenuhi persyaratan instans tertentu lainnya seperti jumlah vCPUs. Misalnya, jika atribut instance yang Anda tentukan menyertakan memori 4 v CPUs dan 16 GB, tipe instans dengan atribut ini tetapi dengan kinerja CPU yang lebih rendah `c6i` akan dikecualikan dari seleksi.

```
"BaselinePerformanceFactors": {
        "Cpu": {
            "References": [
                {
                    "InstanceFamily": "c6i"
                }
            ]
        }
```

Pertimbangan-pertimbangan

- Anda dapat menentukan jenis instans atau atribut instans dalam Armada EC2 atau Armada Spot, tetapi tidak keduanya pada saat yang bersamaan.

  Saat menggunakan CLI, penimpaan templat peluncuran akan menimpa templat peluncuran. Misalnya, jika templat peluncuran berisi tipe instans dan penimpaan templat peluncuran berisi atribut instans, instans yang diidentifikasi oleh atribut instans akan menimpa tipe instans dalam templat peluncuran.
- Saat menggunakan CLI, saat Anda menentukan atribut instans sebagai penimpaan, Anda juga tidak dapat menentukan bobot atau prioritas.
- Anda dapat menentukan maksimum empat struktur `InstanceRequirements` dalam konfigurasi permintaan.

Membuat Armada EC2 dengan pemilihan tipe instans berbasis atribut

Anda dapat mengonfigurasi Armada EC2 untuk menggunakan pemilihan jenis instans berbasis atribut. Tidak mungkin membuat Armada EC2 menggunakan konsol Amazon EC2.

Atribut untuk pemilihan tipe instans berbasis atribut ditentukan dalam struktur `InstanceRequirements`. `InstanceRequirements`Kapan disertakan dalam konfigurasi armada, `InstanceType` dan `WeightedCapacity` harus dikecualikan; mereka tidak dapat menentukan konfigurasi armada pada saat yang sama dengan atribut instance.

Dalam AWS CLI dan PowerShell contoh, atribut berikut ditentukan:

- `VCpuCount`— Minimal 2 v CPUs dan maksimal 4 vCPUs. Jika Anda tidak membutuhkan batas maksimum, Anda dapat menghilangkan nilai maksimum.
- `MemoryMiB`— Minimal 8 GiB memori dan maksimal 16 GiB. Jika Anda tidak membutuhkan batas maksimum, Anda dapat menghilangkan nilai maksimum.

Konfigurasi ini mengidentifikasi setiap jenis instance dengan memori 2 hingga 4 v CPUs dan 8 hingga 16 GiB. Namun, perlindungan harga dan strategi alokasi mungkin akan mengecualikan beberapa tipe instans jika Armada EC2 menyediakan armada.

AWS CLI

Untuk membuat Armada EC2 dengan pemilihan tipe instans berbasis atribut

Gunakan perintah create-fleet untuk membuat Armada EC2. Tentukan konfigurasi armada dalam file JSON.

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

file_name.jsonFile contoh berikut berisi parameter yang mengonfigurasi Armada EC2 untuk menggunakan pemilihan tipe instans berbasis atribut.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized"
    },
    "LaunchTemplateConfigs": [{
        "LaunchTemplateSpecification": {
            "LaunchTemplateName": "my-launch-template",
            "Version": "1"
        },
        "Overrides": [{
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 2,
                    "Max": 4
                },
                "MemoryMiB": {
                    "Min": 8192,
                    "Max": 16384
                }
            }
        }]
    }],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

PowerShell

Untuk membuat Armada EC2 dengan pemilihan tipe instans berbasis atribut

Gunakan New-EC2Fleetcmdlet.

```
$vcpuCount = New-Object Amazon.EC2.Model.VCpuCountRangeRequest
$vcpuCount.Min = 2
$vcpuCount.Max = 4
$memoryMiB = New-Object Amazon.EC2.Model.MemoryMiBRequest
$memoryMiB.Min = 8192
$memoryMiB.Max = 16384
$instanceRequirements = New-Object Amazon.EC2.Model.InstanceRequirementsRequest
$instanceRequirements.VCpuCount = $vcpuCount
$instanceRequirements.MemoryMiB = $memoryMiB

$launchTemplateSpec = New-Object
 Amazon.EC2.Model.FleetLaunchTemplateSpecificationRequest
$launchTemplateSpec.LaunchTemplateName = "my-launch-template"
$launchTemplateSpec.Version = "1"
$override = New-Object Amazon.EC2.Model.FleetLaunchTemplateOverridesRequest
$override.InstanceRequirements = $instanceRequirements
$launchTemplateConfig = New-Object Amazon.EC2.Model.FleetLaunchTemplateConfigRequest
$launchTemplateConfig.LaunchTemplateSpecification = $launchTemplateSpec
$launchTemplateConfig.Overrides = @($override)

New-EC2Fleet `
    -SpotOptions_AllocationStrategy "price-capacity-optimized" `
    -LaunchTemplateConfig @($launchTemplateConfig) `
    -TargetCapacitySpecification_DefaultTargetCapacityType "spot" `
    -TargetCapacitySpecification_TotalTargetCapacity 20 `
    -Type "instant"
```

Buat Armada Spot dengan pemilihan tipe instans berbasis atribut

Anda dapat mengonfigurasi armada untuk menggunakan pemilihan jenis instans berbasis atribut.

Atribut untuk pemilihan tipe instans berbasis atribut ditentukan dalam struktur `InstanceRequirements`. `InstanceRequirements`Kapan disertakan dalam konfigurasi armada, `InstanceType` dan `WeightedCapacity` harus dikecualikan; mereka tidak dapat menentukan konfigurasi armada pada saat yang sama dengan atribut instance.

Dalam AWS CLI dan PowerShell contoh, atribut berikut ditentukan:

- `VCpuCount`— Minimal 2 v CPUs dan maksimal 4 vCPUs. Jika Anda tidak membutuhkan batas maksimum, Anda dapat menghilangkan nilai maksimum.

- `MemoryMiB`— Minimal 8 GiB memori dan maksimal 16 GiB. Jika Anda tidak membutuhkan batas maksimum, Anda dapat menghilangkan nilai maksimum.

Konfigurasi ini mengidentifikasi setiap jenis instance yang memiliki 2 hingga 4 v CPUs dan 8 hingga 16 GiB memori. Namun, perlindungan harga dan strategi alokasi mungkin akan mengecualikan beberapa tipe instans jika Armada Spot menyediakan armada.

Console

Untuk mengonfigurasi Armada Spot untuk pemilihan tipe instans berbasis atribut

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot, lalu pilih Minta Instans Spot.
3. Ikuti langkah-langkah ini untuk membuat Armada Spot. Untuk informasi selengkapnya, lihat Membuat permintaan Armada Spot menggunakan parameter yang ditentukan.

   Saat membuat Armada Spot, konfigurasikan armada untuk pemilihan tipe instans berbasis atribut sebagai berikut:

   a. Untuk Persyaratan tipe instans, pilih Tentukan atribut instans yang sesuai dengan persyaratan komputasi Anda.

   b. Untuk v CPUs, masukkan jumlah minimum dan maksimum yang diinginkan vCPUs. Untuk menentukan tidak ada batas, pilih No minimum, No maximum, atau keduanya.

   c. Untuk Memori (GiB), masukkan jumlah memori minimum dan maksimum yang diinginkan. Untuk menentukan tanpa batasan, pilih Tanpa minimum, Tanpa maksimum, atau keduanya.

   d. (Opsional) Untuk atribut instans Tambahan, Anda dapat secara opsional menentukan satu atau lebih atribut untuk mengekspresikan kebutuhan komputasi Anda secara lebih mendetail. Setiap atribut tambahan menambahkan batasan lebih lanjut untuk permintaan Anda.

   e. (Opsional) Perluas Pratinjau tipe instans yang cocok untuk melihat tipe instans yang memiliki atribut yang Anda tentukan.

AWS CLI

Untuk mengonfigurasi Armada Spot untuk pemilihan tipe instans berbasis atribut

Gunakan request-spot-fleetperintah untuk membuat Armada Spot. Tentukan konfigurasi armada dalam file JSON.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

file_name.jsonFile contoh berikut berisi parameter yang mengonfigurasi Armada Spot untuk menggunakan pemilihan tipe instans berbasis atribut.

```
{
    "AllocationStrategy": "priceCapacityOptimized",
    "TargetCapacity": 20,
    "Type": "request",
    "LaunchTemplateConfigs": [{
        "LaunchTemplateSpecification": {
            "LaunchTemplateName": "my-launch-template",
            "Version": "1"
        },
        "Overrides": [{
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 2,
                    "Max": 4
                },
                "MemoryMiB": {
                    "Min": 8192,
                    "Max": 16384
                }
            }
        }]
    }]
}
```

PowerShell

Untuk mengonfigurasi Armada Spot untuk pemilihan tipe instans berbasis atribut

Gunakan Request-EC2SpotFleetcmdlet.

```
$vcpuCount = New-Object Amazon.EC2.Model.VCpuCountRange
$vcpuCount.Min = 2
$vcpuCount.Max = 4
```

```
$memoryMiB = New-Object Amazon.EC2.Model.MemoryMiB
$memoryMiB.Min = 8192
$memoryMiB.Max = 16384
$instanceRequirements = New-Object Amazon.EC2.Model.InstanceRequirements
$instanceRequirements.VCpuCount = $vcpuCount
$instanceRequirements.MemoryMiB = $memoryMiB

$launchTemplateSpec = New-Object Amazon.EC2.Model.FleetLaunchTemplateSpecification
$launchTemplateSpec.LaunchTemplateName = "my-launch-template"
$launchTemplateSpec.Version = "1"
$override = New-Object Amazon.EC2.Model.LaunchTemplateOverrides
$override.InstanceRequirements = $instanceRequirements
$launchTemplateConfig = New-Object Amazon.EC2.Model.LaunchTemplateConfig
$launchTemplateConfig.LaunchTemplateSpecification = $launchTemplateSpec
$launchTemplateConfig.Overrides = @($override)

Request-EC2SpotFleet `
    -SpotFleetRequestConfig_AllocationStrategy "PriceCapacityOptimized" `
    -SpotFleetRequestConfig_TargetCapacity 20 `
    -SpotFleetRequestConfig_Type "Request" `
    -SpotFleetRequestConfig_LaunchTemplateConfig $launchTemplateConfig
```

Contoh konfigurasi Armada EC2 yang valid dan tidak valid

Jika Anda menggunakan AWS CLI untuk membuat Armada EC2, Anda harus memastikan bahwa konfigurasi armada Anda valid. Contoh berikut menunjukkan konfigurasi yang valid dan tidak valid.

Konfigurasi dianggap tidak valid jika berisi hal berikut:

- Struktur `Overrides` tunggal dengan `InstanceRequirements` maupun `InstanceType`
- Dua struktur `Overrides`, satu dengan `InstanceRequirements` dan yang lainnya dengan `InstanceType`
- Dua struktur `InstanceRequirements` dengan nilai atribut yang tumpang tindih dalam `LaunchTemplateSpecification` yang sama

Contoh konfigurasi

- Konfigurasi yang valid: Templat peluncuran tunggal dengan penimpaan
- Konfigurasi yang valid: Template peluncuran tunggal dengan banyak InstanceRequirements
- Konfigurasi yang valid: Dua templat peluncuran, masing-masing dengan penimpaan

- Konfigurasi yang valid: Hanya InstanceRequirements yang ditentukan, tidak ada nilai atribut yang tumpang tindih
- Konfigurasi tidak valid: Overrides berisi InstanceRequirements dan InstanceType
- Konfigurasi tidak valid: Dua Overrides berisi InstanceRequirements dan InstanceType
- Konfigurasi tidak valid: Nilai atribut tumpang tindih

Konfigurasi yang valid: Templat peluncuran tunggal dengan penimpaan

Konfigurasi berikut ini valid. Konfigurasi ini berisi satu templat peluncuran dan satu struktur `Overrides` yang berisi satu struktur `InstanceRequirements`. Berikut ini adalah penjelasan teks mengenai contoh konfigurasi.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
```

```
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Untuk menggunakan pemilihan instans berbasis atribut, Anda harus menyertakan struktur `InstanceRequirements` dalam konfigurasi armada, dan menentukan atribut yang diinginkan untuk instans tersebut di armada.

Pada contoh sebelumnya, atribut instans berikut ini ditentukan:

- `VCpuCount`— Jenis instance harus memiliki minimal 2 dan maksimal 8 vCPUs.
- `MemoryMiB` – Tipe instans harus memiliki memori maksimum 10240 MiB. Minimum 0 menunjukkan bahwa tidak ada batas minimum.
- `MemoryGiBPerVCpu` – Tipe instans harus memiliki memori maksimum 10.000 GiB per vCPU. Parameter `Min` bersifat opsional. Dengan menghilangkannya, Anda mengindikasikan tidak ada batas minimum.

`TargetCapacityUnitType`

Parameter `TargetCapacityUnitType` menentukan unit untuk kapasitas target. Dalam contoh, kapasitas targetnya adalah `5000` dan tipe unit kapasitas targetnya adalah `vcpu`, yang bersama-sama menentukan kapasitas target yang diinginkan sebesar 5.000 vCPU. Armada EC2 akan meluncurkan instans yang cukup sehingga jumlah total v CPUs dalam armada adalah 5.000 v. CPUs

Konfigurasi yang valid: Template peluncuran tunggal dengan banyak InstanceRequirements

Konfigurasi berikut ini valid. Konfigurasi ini berisi satu templat peluncuran dan satu struktur `Overrides` yang berisi dua struktur `InstanceRequirements`. Atribut yang `InstanceRequirements` ditentukan dalam valid karena nilainya tidak tumpang tindih — `InstanceRequirements` struktur pertama menentukan 0-2 vCPUs, sedangkan struktur kedua `InstanceRequirements` menentukan 4-8 v. `VCpuCount` CPUs

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
```

```
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Konfigurasi yang valid: Dua templat peluncuran, masing-masing dengan penimpaan

Konfigurasi berikut ini valid. Konfigurasi ini berisi dua templat peluncuran, masing-masing dengan satu struktur `Overrides` yang berisi satu struktur `InstanceRequirements`. Konfigurasi ini berguna untuk dukungan arsitektur `arm` dan `x86` dalam armada yang sama.

```
{
```

```
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
```

```
}
```

Konfigurasi yang valid: Hanya **`InstanceRequirements`** yang ditentukan, tidak ada nilai atribut yang tumpang tindih

Konfigurasi berikut ini valid. Konfigurasi ini berisi dua struktur `LaunchTemplateSpecification`, masing-masing dengan templat peluncuran dan struktur `Overrides` yang berisi struktur `InstanceRequirements`. Atribut yang `InstanceRequirements` ditentukan dalam valid karena nilainya tidak tumpang tindih — `InstanceRequirements` struktur pertama menentukan 0-2 vCPUs, sedangkan struktur kedua `InstanceRequirements` menentukan 4-8 v. `VCpuCount` CPUs

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
```

```
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Konfigurasi tidak valid: **`Overrides`** berisi **`InstanceRequirements`** dan **`InstanceType`**

Konfigurasi berikut ini tidak valid. Struktur `Overrides` berisi `InstanceRequirements` dan`InstanceType`. Untuk `Overrides`, Anda dapat menentukan antara `InstanceRequirements` atau `InstanceType`, tetapi tidak keduanya.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
```

```
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Konfigurasi tidak valid: Dua **`Overrides`** berisi **`InstanceRequirements`** dan **`InstanceType`**

Konfigurasi berikut ini tidak valid. Struktur `Overrides` berisi `InstanceRequirements` dan`InstanceType`. Anda dapat menentukan antara `InstanceRequirements` atau `InstanceType`, tetapi tidak keduanya, meskipun berada dalam struktur `Overrides` yang berbeda.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
```

```
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Konfigurasi tidak valid: Nilai atribut tumpang tindih

Konfigurasi berikut ini tidak valid. Dua struktur `InstanceRequirements` masing-masing berisi `"VCpuCount": {"Min": 0, "Max": 2}`. Nilai untuk atribut ini tumpang tindih, yang akan mengakibatkan kolam kapasitas ganda.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
```

```
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
            }
        ]
    }
],
 "TargetCapacitySpecification": {
    "TotalTargetCapacity": 1,
    "DefaultTargetCapacityType": "spot"
}
}
}
```

Contoh konfigurasi Armada Spot yang valid dan tidak valid

Jika Anda menggunakan AWS CLI untuk membuat Armada Spot, Anda harus memastikan bahwa konfigurasi armada Anda valid. Contoh berikut menunjukkan konfigurasi yang valid dan tidak valid.

Konfigurasi dianggap tidak valid jika berisi hal berikut:

- Struktur `Overrides` tunggal dengan `InstanceRequirements` maupun `InstanceType`
- Dua struktur `Overrides`, satu dengan `InstanceRequirements` dan yang lainnya dengan `InstanceType`
- Dua struktur `InstanceRequirements` dengan nilai atribut yang tumpang tindih dalam `LaunchTemplateSpecification` yang sama

Contoh konfigurasi

- Konfigurasi yang valid: Templat peluncuran tunggal dengan penimpaan
- Konfigurasi yang valid: Template peluncuran tunggal dengan banyak InstanceRequirements
- Konfigurasi yang valid: Dua templat peluncuran, masing-masing dengan penimpaan
- Konfigurasi yang valid: Hanya InstanceRequirements yang ditentukan, tidak ada nilai atribut yang tumpang tindih
- Konfigurasi tidak valid: Overrides berisi InstanceRequirements dan InstanceType

- Konfigurasi tidak valid: Dua Overrides berisi InstanceRequirements dan InstanceType
- Konfigurasi tidak valid: Nilai atribut tumpang tindih

Konfigurasi yang valid: Templat peluncuran tunggal dengan penimpaan

Konfigurasi berikut ini valid. Konfigurasi ini berisi satu templat peluncuran dan satu struktur `Overrides` yang berisi satu struktur `InstanceRequirements`. Berikut ini adalah penjelasan teks mengenai contoh konfigurasi.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
        "TargetCapacity": 5000,
```

```
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
}
```

`InstanceRequirements`

Untuk menggunakan pemilihan instans berbasis atribut, Anda harus menyertakan struktur `InstanceRequirements` dalam konfigurasi armada, dan menentukan atribut yang diinginkan untuk instans tersebut di armada.

Pada contoh sebelumnya, atribut instans berikut ini ditentukan:

- `VCpuCount`— Jenis instance harus memiliki minimal 2 dan maksimal 8 vCPUs.
- `MemoryMiB` – Tipe instans harus memiliki memori maksimum 10240 MiB. Minimum 0 menunjukkan bahwa tidak ada batas minimum.
- `MemoryGiBPerVCpu` – Tipe instans harus memiliki memori maksimum 10.000 GiB per vCPU. Parameter `Min` bersifat opsional. Dengan menghilangkannya, Anda mengindikasikan tidak ada batas minimum.

`TargetCapacityUnitType`

Parameter `TargetCapacityUnitType` menentukan unit untuk kapasitas target. Dalam contoh, kapasitas target adalah `5000` dan tipe unit kapasitas target adalah`vcpu`, yang bersama-sama menentukan kapasitas target yang diinginkan 5.000 vCPUs. Armada Spot akan meluncurkan instance yang cukup sehingga jumlah total v CPUs dalam armada adalah 5.000 vCPUs.

Konfigurasi yang valid: Template peluncuran tunggal dengan banyak InstanceRequirements

Konfigurasi berikut ini valid. Konfigurasi ini berisi satu templat peluncuran dan satu struktur `Overrides` yang berisi dua struktur `InstanceRequirements`. Atribut yang `InstanceRequirements` ditentukan dalam valid karena nilainya tidak tumpang tindih — `InstanceRequirements` struktur pertama menentukan 0-2 vCPUs, sedangkan struktur kedua `InstanceRequirements` menentukan 4-8 v. `VCpuCount` CPUs

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Konfigurasi yang valid: Dua templat peluncuran, masing-masing dengan penimpaan

Konfigurasi berikut ini valid. Konfigurasi ini berisi dua templat peluncuran, masing-masing dengan satu struktur `Overrides` yang berisi satu struktur `InstanceRequirements`. Konfigurasi ini berguna untuk dukungan arsitektur `arm` dan `x86` dalam armada yang sama.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
```

```
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Konfigurasi yang valid: Hanya **`InstanceRequirements`** yang ditentukan, tidak ada nilai atribut yang tumpang tindih

Konfigurasi berikut ini valid. Konfigurasi ini berisi dua struktur `LaunchTemplateSpecification`, masing-masing dengan templat peluncuran dan struktur `Overrides` yang berisi struktur `InstanceRequirements`. Atribut yang `InstanceRequirements` ditentukan dalam valid karena nilainya tidak tumpang tindih — `InstanceRequirements` struktur pertama menentukan 0-2 vCPUs, sedangkan struktur kedua `InstanceRequirements` menentukan 4-8 v. `VCpuCount` CPUs

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
```

```
                            "Min": 0
                        }
                    }
                }
            ]
        },
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "MyOtherLaunchTemplate",
                "Version": "1"
            },
            "Overrides": [
            {
                "InstanceRequirements": {
                    "VCpuCount": {
                        "Min": 4,
                        "Max": 8
                    },
                    "MemoryMiB": {
                        "Min": 0
                    }
                }
            }
            ]
        }
    ],
    "TargetCapacity": 1,
    "OnDemandTargetCapacity": 0,
    "Type": "maintain"
  }
}
```

Konfigurasi tidak valid: **`Overrides`** berisi **`InstanceRequirements`** dan **`InstanceType`**

Konfigurasi berikut ini tidak valid. Struktur `Overrides` berisi `InstanceRequirements` dan`InstanceType`. Untuk `Overrides`, Anda dapat menentukan antara `InstanceRequirements` atau `InstanceType`, tetapi tidak keduanya.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Konfigurasi tidak valid: Dua **`Overrides`** berisi **`InstanceRequirements`** dan **`InstanceType`**

Konfigurasi berikut ini tidak valid. Struktur `Overrides` berisi `InstanceRequirements` dan`InstanceType`. Anda dapat menentukan antara `InstanceRequirements` atau `InstanceType`, tetapi tidak keduanya, meskipun berada dalam struktur `Overrides` yang berbeda.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Konfigurasi tidak valid: Nilai atribut tumpang tindih

Konfigurasi berikut ini tidak valid. Dua struktur `InstanceRequirements` masing-masing berisi `"VCpuCount": {"Min": 0, "Max": 2}`. Nilai untuk atribut ini tumpang tindih, yang akan mengakibatkan kolam kapasitas ganda.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
```

```
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Melihat pratinjau tipe instans dengan atribut tertentu

Anda dapat menggunakan perintah get-instance-types-from-instance-requirements untuk melihat pratinjau jenis instance yang cocok dengan atribut yang Anda tentukan. Hal ini sangat berguna untuk mengetahui atribut yang akan ditentukan dalam konfigurasi permintaan Anda tanpa meluncurkan instans apa pun. Perhatikan bahwa perintah tidak mempertimbangkan kapasitas yang tersedia.

Untuk melihat daftar jenis instance dengan menentukan atribut menggunakan AWS CLI

1. (Opsional) Untuk menghasilkan semua atribut yang mungkin yang dapat ditentukan, gunakan perintah get-instance-types-from-instance-requirements dan parameter. `--generate-cli-skeleton` Anda dapat secara opsional mengarahkan output ke file untuk menyimpannya dengan menggunakan `input > attributes.json`.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
       --generate-cli-skeleton input > attributes.json
   ```

   Output yang diharapkan

   ```
   {
       "DryRun": true,
       "ArchitectureTypes": [
           "i386"
       ],
       "VirtualizationTypes": [
           "hvm"
       ],
       "InstanceRequirements": {
           "VCpuCount": {
               "Min": 0,
               "Max": 0
           },
           "MemoryMiB": {
   ```

```
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
```

```
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Buat file konfigurasi JSON menggunakan output dari langkah sebelumnya, dan konfigurasikan sebagai berikut:

> **Note**
>
> Anda harus memberikan nilai untuk `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount`, dan `MemoryMiB`. Anda dapat menghilangkan atribut lainnya; saat dihilangkan, nilai default digunakan.
> Untuk deskripsi setiap atribut dan nilai defaultnya, lihat get-instance-types-from-instance-requirements.

a. Untuk `ArchitectureTypes`, tentukan satu atau lebih tipe arsitektur prosesor.

b. Untuk `VirtualizationTypes`, tentukan satu atau lebih tipe virtualisasi.

c. Untuk`VCpuCount`, tentukan jumlah minimum dan maksimum vCPUs. Untuk menentukan tidak ada batas minimum, untuk`Min`, tentukan`0`. Untuk menentukan tidak ada batas maksimum, hilangkan parameter `Max`.

d. Untuk `MemoryMiB`, tentukan jumlah memori minimum dan maksimum dalam MiB. Untuk menentukan tidak ada batas minimum, untuk `Min`, tentukan `0`. Untuk menentukan tidak ada batas maksimum, hilangkan parameter `Max`.

e. Anda dapat secara opsional menentukan satu atau lebih atribut lainnya untuk lebih membatasi daftar tipe instans yang dikembalikan.

3. Untuk melihat pratinjau jenis instance yang memiliki atribut yang Anda tentukan dalam file JSON, gunakan perintah get-instance-types-from-instance-requirements, dan tentukan nama dan path ke file JSON Anda dengan menggunakan parameter. `--cli-input-json` Anda dapat secara opsional memformat output untuk muncul dalam format tabel.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Contoh file *attributes.json*

Dalam contoh ini, atribut yang diperlukan disertakan dalam file JSON. Atribut tersebut adalah `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount`, dan `MemoryMiB`. Selain itu, atribut `InstanceGenerations` opsional juga disertakan. Perhatikan bahwa untuk `MemoryMiB`, nilai `Max` dapat dihilangkan untuk menunjukkan bahwa tidak ada batasan.

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
```

```
    }
}
```

Contoh output

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

4. Setelah mengidentifikasi tipe instans yang memenuhi kebutuhan Anda, catatlah atribut instans yang Anda gunakan sehingga Anda dapat menggunakannya saat mengonfigurasi permintaan armada.

Gunakan pembobotan instans untuk mengelola biaya dan kinerja Armada EC2 atau Armada Spot Anda

Dengan pembobotan instans, Anda menetapkan bobot untuk setiap jenis instans di Armada EC2 atau Armada Spot untuk mewakili kapasitas komputasi dan kinerjanya relatif satu sama lain. Berdasarkan bobot, armada dapat menggunakan kombinasi jenis instans yang ditentukan, asalkan dapat memenuhi kapasitas target yang diinginkan. Ini dapat membantu Anda mengelola biaya dan kinerja armada Anda.

Bobot mewakili unit kapasitas yang dikontribusikan oleh tipe instans terhadap total kapasitas target.

Contoh: Gunakan pembobotan contoh untuk manajemen kinerja

Misalkan armada Anda memiliki dua tipe instans, dan Anda menetapkan bobot yang berbeda untuk setiap jenis instans untuk mencerminkan berapa banyak yang Anda butuhkan untuk mencapai kinerja yang sama, sebagai berikut:

- `m5.large`- Berat: 1
- `m5.2xlarge`- Berat: 4

Dengan menetapkan bobot ini, Anda mengatakan bahwa Anda memerlukan 4 `m5.large` instance untuk mencapai kinerja yang sama dengan 1. `m5.2xlarge`

Untuk menghitung berapa banyak instance dari setiap jenis instans yang diperlukan untuk kapasitas target tertentu, gunakan rumus berikut:

```
target capacity / weight = number of instances
```

Jika kapasitas target Anda adalah 8 unit, armada dapat memenuhi kapasitas target dengan salah satu `m5.large` ataum`5.2xlarge`, atau campuran keduanya, sebagai berikut:

- 8 `m5.large` contoh (kapasitas 8/berat 1 = 8 instance)
- 2 `m5.2xlarge` contoh (kapasitas 8/berat 4 = 2 instance)
- 4 `m5.large` dan 1 `m5.2xlarge`

Contoh: Gunakan pembobotan contoh untuk manajemen biaya

Secara default, harga yang Anda tentukan adalah per jam instans. Saat Anda menggunakan fitur pembobotan instans, harga yang Anda tentukan adalah per unit jam. Anda dapat menghitung harga per unit jam dengan membagi harga tipe instans dengan jumlah unit yang diwakilinya. Armada menghitung jumlah instance yang akan diluncurkan dengan membagi kapasitas target dengan bobot instans. Jika hasilnya bukan bilangan bulat, armada akan membulatkannya ke bilangan bulat berikutnya, sehingga ukuran armada Anda tidak berada di bawah kapasitas targetnya. Armada dapat memilih kolam mana pun yang Anda tentukan dalam spesifikasi peluncuran, meskipun kapasitas instans yang diluncurkan melebihi kapasitas target yang diminta.

Tabel berikut mencakup contoh perhitungan untuk menentukan harga per unit untuk armada dengan kapasitas target 10.

Tipe instans	Bobot instans	Kapasitas target	Jumlah instans yang diluncurkan	Harga per jam instans	Harga per unit jam
`r3.xlarge`	2	10	5 (10 dibagi 2)	$0,05	$0,025 (,05 dibagi 2)
`r3.8xlarge`	8	10	2 (10 dibagi 8, hasil dibulatkan)	$0,10	$0,0125 (,10 dibagi 8)

Gunakan bobot instance armada sebagai berikut untuk menyediakan kapasitas target yang Anda inginkan di pool dengan harga per unit terendah pada saat pemenuhan:

1. Tetapkan kapasitas target untuk armada Anda baik dalam instance (default) atau dalam unit pilihan Anda, seperti vCPU, memori, penyimpanan, atau throughput.
2. Tetapkan harga per unit.
3. Untuk setiap spesifikasi peluncuran, tentukan bobot, yang merupakan jumlah unit yang diwakili oleh tipe instans terhadap kapasitas target.

Contoh pembobotan instans

Pertimbangkan permintaan armada dengan konfigurasi berikut:

- Kapasitas target 24
- Spesifikasi peluncuran dengan tipe instans `r3.2xlarge` dan bobot 6
- Spesifikasi peluncuran dengan tipe instans `c3.xlarge` dan bobot 5

Bobot mewakili jumlah unit yang diwakili oleh tipe instans terhadap kapasitas target. Jika spesifikasi peluncuran pertama memberikan harga per unit terendah (harga untuk `r3.2xlarge` per jam contoh dibagi 6), armada akan meluncurkan empat contoh ini (24 dibagi 6).

Jika spesifikasi peluncuran kedua memberikan harga terendah per unit (harga untuk `c3.xlarge` per jam contoh dibagi 5), armada akan meluncurkan lima contoh ini (24 dibagi 5, hasilnya dibulatkan).

Pembobotan instans dan strategi alokasi

Pertimbangkan permintaan armada dengan konfigurasi berikut:

- Kapasitas target 30 Instans Spot
- Spesifikasi peluncuran dengan tipe instans `c3.2xlarge` dan bobot 8
- Spesifikasi peluncuran dengan tipe instans `m3.xlarge` dan bobot 8
- Spesifikasi peluncuran dengan tipe instans `r3.xlarge` dan bobot 8

Armada akan meluncurkan empat instance (30 dibagi 8, hasilnya dibulatkan). Dengan strategi `diversified`, armada meluncurkan satu instans di masing-masing dari ketiga kolam tersebut, dan instans keempat di kolam mana pun yang memberikan harga terendah per unit.

Gunakan strategi alokasi untuk menentukan bagaimana Armada EC2 atau Armada Spot memenuhi kapasitas Spot dan Sesuai Permintaan

Bila Anda menggunakan beberapa kumpulan kapasitas (masing-masing terdiri dari tipe instans dan Availability Zone) dalam Armada EC2 atau Armada Spot, Anda dapat menggunakan strategi alokasi untuk mengelola cara Amazon EC2 memenuhi kapasitas Spot dan On-Demand Anda dari kumpulan ini. Strategi alokasi dapat mengoptimalkan kapasitas, harga, dan jenis instans yang tersedia untuk digunakan. Ada strategi alokasi yang berbeda untuk Instans Spot dan Instans Sesuai Permintaan.

Topik

- Strategi alokasi untuk Instans Spot
- Strategi alokasi untuk Instans Sesuai Permintaan
- Pilih strategi alokasi Spot yang sesuai
- Pertahankan kapasitas target untuk Instans Spot
- Memprioritaskan tipe instans untuk kapasitas Sesuai Permintaan

Strategi alokasi untuk Instans Spot

Konfigurasi peluncuran Anda menentukan semua kemungkinan kumpulan kapasitas Spot (tipe instans dan Availability Zone) dari mana Armada EC2 atau Armada Spot dapat meluncurkan Instans

Spot. Namun, saat meluncurkan instance, armada menggunakan strategi alokasi yang Anda tentukan untuk memilih kumpulan tertentu dari semua kemungkinan kumpulan Anda.

> **Note**
>
> (Hanya instans Linux) Jika Anda mengonfigurasi Instans Spot untuk diluncurkan dengan AMD SEV-SNP diaktifkan, Anda akan dikenakan biaya penggunaan tambahan per jam yang setara dengan 10% dari tarif per jam Sesuai Permintaan untuk jenis instans yang dipilih. Jika strategi alokasi menggunakan harga sebagai input, armada tidak termasuk biaya tambahan ini; hanya harga Spot yang digunakan.

Anda dapat menentukan salah satu strategi alokasi berikut untuk Instans Spot:

Kapasitas harga dioptimalkan (disarankan)

Armada mengidentifikasi kumpulan dengan ketersediaan kapasitas tertinggi untuk jumlah instance yang diluncurkan. Hal ini berarti bahwa kami akan meminta Instans Spot dari kolam yang kami yakini memiliki peluang interupsi terendah dalam waktu dekat. Armada kemudian meminta Instans Spot dari harga terendah dari kumpulan ini.

Strategi alokasi kapasitas harga yang dioptimalkan adalah pilihan terbaik untuk sebagian besar beban kerja Spot, seperti aplikasi kontainer stateless, layanan mikro, aplikasi web, pekerjaan data dan analitik, dan pemrosesan batch.

Jika Anda menggunakan AWS CLI, nama parameternya adalah untuk Armada EC2 dan `price-capacity-optimized` `priceCapacityOptimized` untuk Armada Spot.

Kapasitas dioptimalkan

Armada mengidentifikasi kumpulan dengan ketersediaan kapasitas tertinggi untuk jumlah instance yang diluncurkan. Hal ini berarti bahwa kami akan meminta Instans Spot dari kolam yang kami yakini memiliki peluang interupsi terendah dalam waktu dekat.

Dengan Instans Spot, harga berubah secara perlahan dari waktu ke waktu berdasarkan tren penawaran dan permintaan jangka panjang, tetapi kapasitas berfluktuasi secara waktu nyata. Strategi kapasitas yang dioptimalkan secara otomatis meluncurkan Instans Spot ke dalam kumpulan yang paling tersedia dengan melihat data kapasitas waktu nyata dan memprediksi mana yang paling tersedia. Ini berfungsi dengan baik untuk beban kerja yang mungkin memiliki biaya interupsi yang lebih tinggi terkait dengan memulai kembali tugas, seperti Integrasi Berkelanjutan (CI), rendering gambar dan media, beban kerja Deep Learning, dan Komputasi

Performa Tinggi (HPC) yang mungkin memiliki biaya interupsi yang lebih tinggi terkait dengan memulai ulang pekerjaan. Dengan menawarkan kemungkinan gangguan yang lebih sedikit, strategi kapasitas yang dioptimalkan dapat menurunkan biaya keseluruhan beban kerja Anda.

Atau, Anda dapat menggunakan strategi alokasi prioritas yang dioptimalkan kapasitas dengan parameter prioritas untuk mengurutkan jenis instans dari prioritas tertinggi hingga terendah. Anda dapat mengatur prioritas yang sama untuk tipe instans yang berbeda. Armada akan mengoptimalkan kapasitas terlebih dahulu, tetapi akan menghormati prioritas tipe instans berdasarkan upaya terbaik (misalnya, jika menghormati prioritas tidak akan secara signifikan mempengaruhi kemampuan armada untuk menyediakan kapasitas optimal). Ini adalah pilihan opsi yang bagus untuk beban kerja di mana kemungkinan gangguan harus diminimalkan dan preferensi untuk tipe instans tertentu menjadi penting. Perhatikan bahwa saat Anda menetapkan prioritas untuk jenis instans untuk kapasitas Spot Anda, prioritas yang sama juga diterapkan pada Instans Sesuai Permintaan jika strategi alokasi Sesuai Permintaan ditetapkan untuk diprioritaskan. Untuk Armada Spot, penggunaan prioritas hanya didukung jika armada Anda menggunakan templat peluncuran.

Jika Anda menggunakan AWS CLI, nama parameternya adalah `capacity-optimized` dan `capacity-optimized-prioritized` untuk Armada EC2 dan `capacityOptimized` dan `capacityOptimizedPrioritized` untuk Armada Spot.

Diversifikasi

Instans Spot didistribusikan di semua kolam kapasitas Spot. Jika Anda menggunakan AWS CLI, nama parameter adalah `diversified` untuk Armada EC2 dan Armada Spot.

Harga terendah (tidak disarankan)

> **Warning**
>
> Kami tidak merekomendasikan strategi alokasi harga terendah karena memiliki risiko interupsi tertinggi untuk Instans Spot Anda.

Instans Spot berasal dari kolam dengan harga terendah yang memiliki kapasitas tersedia. Saat menggunakan AWS CLI, ini adalah strategi default. Namun, kami menyarankan Anda mengganti default dengan menentukan strategi alokasi kapasitas harga yang dioptimalkan.

Dengan strategi harga terendah, jika kolam dengan harga terendah tidak memiliki kapasitas yang tersedia, Instans Spot berasal dari kumpulan harga terendah berikutnya yang memiliki kapasitas

yang tersedia. Jika kolam kehabisan kapasitas sebelum memenuhi kapasitas yang Anda inginkan, armada akan terus memenuhi permintaan Anda dengan menarik dari kolam dengan harga terendah berikutnya. Untuk memastikan bahwa kapasitas yang Anda inginkan terpenuhi, Anda mungkin menerima Instans Spot dari beberapa kolam.

Karena strategi ini hanya mempertimbangkan harga instans dan bukan ketersediaan kapasitas, hal ini dapat menyebabkan tingkat interupsi yang tinggi.

Strategi alokasi harga terendah hanya tersedia saat menggunakan. AWS CLI Nama parameter untuk Armada EC2 dan `lowest-price` `lowestPrice` untuk Armada Spot.

Jumlah kolam yang akan digunakan

Anda dapat menentukan jumlah kolam Spot untuk mengalokasikan kapasitas Spot target. Hanya berlaku jika strategi alokasi diatur ke harga terendah. Armada memilih kumpulan Spot dengan harga terendah dan mengalokasikan kapasitas Spot target Anda secara merata di seluruh jumlah kumpulan Spot yang Anda tentukan.

Perhatikan bahwa armada mencoba menarik Instans Spot dari jumlah kumpulan yang Anda tentukan berdasarkan upaya terbaik. Jika kolam kehabisan kapasitas Spot sebelum memenuhi kapasitas target Anda, armada akan terus memenuhi permintaan Anda dengan menarik dari kolam dengan harga terendah berikutnya. Untuk memastikan bahwa kapasitas target terpenuhi, Anda mungkin menerima Instans Spot dari kolam yang jumlahnya lebih dari jumlah kolam yang Anda tentukan. Demikian pula, jika sebagian besar kolam tidak memiliki kapasitas Spot, Anda mungkin menerima kapasitas target penuh dari jumlah yang lebih rendah dari kolam yang Anda tentukan.

Parameter ini hanya tersedia saat menentukan strategi alokasi harga terendah dan hanya saat menggunakan. AWS CLI Nama parameter `InstancePoolsToUseCount` untuk Armada EC2 dan Armada Spot.

Strategi alokasi untuk Instans Sesuai Permintaan

Konfigurasi peluncuran Anda menentukan semua kemungkinan kumpulan kapasitas (tipe instans dan Availability Zone) dari mana Armada EC2 atau Armada Spot dapat meluncurkan Instans Sesuai Permintaan. Namun, saat meluncurkan instance, armada menggunakan strategi alokasi yang Anda tentukan untuk memilih kumpulan tertentu dari semua kemungkinan kumpulan Anda.

Anda dapat menentukan salah satu strategi alokasi berikut untuk Instans Sesuai Permintaan:

Harga terendah

Instans On-Demand berasal dari kolam dengan harga terendah yang memiliki kapasitas yang tersedia. Ini adalah strategi default.

Jika kolam dengan harga terendah tidak memiliki kapasitas yang tersedia, Instans Sesuai Permintaan berasal dari kolam dengan harga terendah berikutnya yang memiliki kapasitas yang tersedia.

Jika kolam kehabisan kapasitas sebelum memenuhi kapasitas yang Anda inginkan, armada akan terus memenuhi permintaan Anda dengan menarik dari kolam dengan harga terendah berikutnya. Untuk memastikan kapasitas yang Anda inginkan terpenuhi, Anda mungkin menerima Instans Sesuai Permintaan dari beberapa kumpulan.

Diprioritaskan

Armada menggunakan prioritas yang Anda tetapkan untuk setiap penggantian template peluncuran, meluncurkan jenis instans dalam urutan prioritas tertinggi terlebih dahulu. Strategi ini tidak dapat digunakan dengan pemilihan tipe instans berbasis atribut. Untuk contoh cara menggunakan strategi alokasi ini, lihatMemprioritaskan tipe instans untuk kapasitas Sesuai Permintaan.

Pilih strategi alokasi Spot yang sesuai

Anda dapat mengoptimalkan armada untuk kasus penggunaan dengan memilih strategi alokasi Spot yang sesuai.

Menyeimbangkan harga terendah dan ketersediaan kapasitas

Untuk menyeimbangkan trade-off antara kumpulan kapasitas Spot dengan harga terendah dan kumpulan kapasitas Spot dengan ketersediaan kapasitas tertinggi, kami sarankan Anda menggunakan strategi alokasi kapasitas harga yang dioptimalkan. Strategi ini membuat keputusan terkait kolam yang akan meminta Instans Spot dari berdasarkan harga kolam dan ketersediaan kapasitas Instans Spot di kolam tersebut. Hal ini berarti bahwa kami akan meminta Instans Spot dari kolam yang kami yakini memiliki kemungkinan interupsi paling rendah dalam waktu dekat, dengan tetap mempertimbangkan harga.

Jika armada Anda menjalankan beban kerja yang tangguh dan tanpa kewarganegaraan, termasuk aplikasi kontainer, layanan mikro, aplikasi web, pekerjaan data dan analitik, dan pemrosesan batch,

maka gunakan strategi alokasi kapasitas harga yang dioptimalkan untuk penghematan biaya dan ketersediaan kapasitas yang optimal.

Jika armada Anda menjalankan beban kerja yang mungkin memiliki biaya interupsi yang lebih tinggi terkait dengan memulai kembali tugas, Anda harus menerapkan operasi titik pemeriksaan agar aplikasi dapat memulai kembali dari titik tersebut jika terinterupsi. Dengan menggunakan checkpointing, Anda membuat strategi alokasi kapasitas harga yang dioptimalkan cocok untuk beban kerja ini karena mengalokasikan kapasitas dari kumpulan harga terendah yang juga menawarkan tingkat interupsi Instans Spot yang rendah.

Misalnya konfigurasi JSON yang menggunakan strategi alokasi kapasitas harga yang dioptimalkan, lihat berikut ini:

- Armada EC2 — Contoh 10: Luncurkan Instans Spot di armada price-capacity-optimized
- Armada Spot — Contoh 11: Luncurkan Instans Spot di armada priceCapacityOptimized

Ketika beban kerja memiliki biaya interupsi yang tinggi

Anda dapat secara opsional menggunakan strategi yang dioptimalkan kapasitas jika Anda menjalankan beban kerja yang menggunakan jenis instans dengan harga yang sama, atau di mana biaya interupsi sangat signifikan sehingga penghematan biaya tidak memadai dibandingkan dengan peningkatan interupsi marjinal. Strategi ini mengalokasikan kapasitas dari kolam kapasitas Spot yang paling banyak tersedia yang menawarkan kemungkinan lebih sedikit interupsi, yang dapat menurunkan biaya keseluruhan beban kerja Anda.

Ketika kemungkinan interupsi harus diminimalkan tetapi preferensi untuk jenis instance tertentu penting, Anda dapat mengekspresikan prioritas kumpulan Anda dengan menggunakan strategi alokasi prioritas yang dioptimalkan kapasitas dan kemudian menetapkan urutan jenis instance untuk digunakan dari prioritas tertinggi ke prioritas terendah.

Perhatikan bahwa ketika Anda menetapkan prioritas untuk kapasitas yang dioptimalkan diprioritaskan, prioritas yang sama juga diterapkan pada Instans Sesuai Permintaan jika strategi alokasi Sesuai Permintaan ditetapkan untuk diprioritaskan. Perhatikan juga bahwa, untuk Armada Spot, penggunaan prioritas hanya didukung jika armada Anda menggunakan templat peluncuran.

Misalnya konfigurasi JSON yang menggunakan strategi alokasi kapasitas yang dioptimalkan, lihat berikut ini:

- Armada EC2 — Contoh 8: Luncurkan Instans Spot dalam armada yang dioptimalkan kapasitas

- Armada Spot — Contoh 9: Meluncurkan Instans Spot dalam armada yang dioptimalkan kapasitas

Misalnya konfigurasi JSON yang menggunakan strategi alokasi prioritas yang dioptimalkan kapasitas, lihat berikut ini:

- Armada EC2 — Contoh 9: Luncurkan Instans Spot dalam armada yang dioptimalkan kapasitas dengan prioritas
- Armada Spot — Contoh 10: Meluncurkan Instans Spot dalam armada yang dioptimalkan kapasitas dengan prioritas

Jika beban kerja Anda memiliki fleksibilitas waktu dan ketersediaan kapasitas tidak menjadi faktor

Jika armada Anda kecil atau berjalan dalam waktu singkat, Anda dapat menggunakan kapasitas harga yang dioptimalkan untuk memaksimalkan penghematan biaya sambil tetap mempertimbangkan ketersediaan kapasitas.

Jika armada Anda besar atau berjalan untuk waktu yang lama

Jika armada Anda besar atau berjalan untuk waktu yang lama, Anda dapat meningkatkan ketersediaan armada Anda dengan mendistribusikan Instans Spot di beberapa kumpulan menggunakan strategi diversifikasi. Misalnya, jika armada Anda menentukan 10 pool dan kapasitas target 100 instans, armada meluncurkan 10 Instans Spot di setiap kumpulan. Jika harga Spot untuk satu kolam melebihi harga maksimum Anda untuk kolam ini, hanya 10% armada yang terpengaruh. Penggunaan strategi ini juga membuat armada Anda kurang sensitif terhadap kenaikan harga Spot di satu kolam dari waktu ke waktu. Dengan strategi diversifikasi, armada tidak meluncurkan Instans Spot ke kolam apa pun dengan harga Spot yang sama atau lebih tinggi dari harga On-Demand.

Pertahankan kapasitas target untuk Instans Spot

Setelah Instans Spot dihentikan karena perubahan harga Spot atau kapasitas yang tersedia dari kumpulan kapasitas Spot, armada tipe `maintain` meluncurkan Instans Spot pengganti. Strategi alokasi menentukan kolam tempat instans pengganti diluncurkan, sebagai berikut:

- Jika strategi alokasi dioptimalkan kapasitas harga, armada meluncurkan instans pengganti di kumpulan yang memiliki ketersediaan kapasitas Instans Spot paling banyak sambil juga mempertimbangkan harga dan mengidentifikasi kumpulan dengan harga terendah dengan ketersediaan kapasitas tinggi.

- Jika strategi alokasi dioptimalkan kapasitas, armada meluncurkan instance pengganti di kumpulan yang memiliki ketersediaan kapasitas Instans Spot paling banyak.
- Jika strategi alokasi terdiversifikasi, armada mendistribusikan Instans Spot pengganti di seluruh kumpulan yang tersisa.

Memprioritaskan tipe instans untuk kapasitas Sesuai Permintaan

Saat Armada EC2 atau Armada Spot mencoba memenuhi kapasitas Sesuai Permintaan Anda, default meluncurkan jenis instans dengan harga terendah terlebih dahulu. Jika strategi alokasi On-Demand diatur untuk diprioritaskan, armada menggunakan prioritas untuk menentukan jenis instans mana yang akan digunakan terlebih dahulu saat memenuhi kapasitas On-Demand. Prioritas ditetapkan ke penimpaan templat peluncuran, dan prioritas tertinggi diluncurkan terlebih dahulu.

Contoh: Memprioritaskan tipe instans

Dalam contoh ini, Anda mengonfigurasi tiga penimpaan templat peluncuran, masing-masing dengan tipe instans yang berbeda.

Harga Sesuai Permintaan untuk tipe instans beragam harganya. Berikut ini adalah tipe instans yang digunakan dalam contoh ini, yang tercantum dalam urutan harga, dimulai dengan tipe instans yang paling murah:

- `m4.large` – termurah
- `m5.large`
- `m5a.large`

Jika Anda tidak menggunakan prioritas untuk menentukan urutan, armada akan memenuhi kapasitas Sesuai Permintaan dengan memulai dari tipe instans yang paling murah.

Namun, katakanlah Anda memiliki Instans Terpesan `m5.large` yang tidak terpakai yang ingin Anda gunakan terlebih dahulu. Anda dapat mengatur prioritas penimpaan templat peluncuran sehingga tipe instans digunakan dalam urutan prioritas, sebagai berikut:

- `m5.large` – prioritas 1
- `m4.large` – prioritas 2
- `m5a.large` – prioritas 3

Gunakan Rebalancing Kapasitas di Armada EC2 dan Armada Spot untuk mengganti Instans Spot yang berisiko

Dengan Penyeimbangan Kembali Kapasitas, Armada EC2 atau Armada Spot Anda dapat mempertahankan kapasitas Spot yang diinginkan dengan secara proaktif mengganti Instans Spot yang berisiko terganggu. Ketika Instans Spot berisiko tinggi mengalami gangguan, Amazon EC2 mengirimkan rekomendasi penyeimbangan kembali. Jika Capacity Rebalancing diaktifkan, rekomendasi rebalance akan memicu peluncuran Instans Spot baru sebelum instans berisiko terputus.

Penyeimbangan Kembali Kapasitas membantu Anda menjaga ketersediaan beban kerja dengan menambah armada Anda secara proaktif dengan Instans Spot baru sebelum instans yang berjalan terganggu oleh Amazon EC2.

Untuk mengonfigurasi Armada EC2 agar menggunakan Capacity Rebalancing untuk meluncurkan Instans Spot pengganti

Gunakan perintah create-fleet dan parameter yang relevan dalam struktur. `MaintenanceStrategies` Untuk contoh konfigurasi JSON, lihatContoh 7: Konfigurasikan Penyeimbangan Kembali Kapasitas untuk meluncurkan Instans Spot pengganti.

Untuk mengonfigurasi Armada Spot agar menggunakan Penyeimbangan Kembali Kapasitas untuk meluncurkan Instans Spot pengganti

Anda dapat menggunakan konsol Amazon EC2 atau AWS CLI untuk mengkonfigurasi Capacity Rebalancing.

(Konsol) Saat membuat Armada Spot, pilih kotak centang Penyeimbangan Kapasitas. Untuk informasi selengkapnya, lihat langkah 6.d. di Membuat permintaan Armada Spot menggunakan parameter yang ditentukan.

(AWS CLI) Gunakan request-spot-fleetperintah dan parameter yang relevan dalam `SpotMaintenanceStrategies` struktur. Untuk contoh konfigurasi JSON, lihatContoh 8: Mengonfigurasikan Penyeimbangan Ulang Kapasitas untuk meluncurkan Instans Spot pengganti.

Topik

- Batasan
- Opsi konfigurasi

- Pertimbangan-pertimbangan

Batasan

- Penyeimbangan Ulang Kapasitas hanya tersedia untuk armada tipe `maintain`.
- Saat armada berjalan, Anda tidak dapat mengubah pengaturan Penyeimbangan Ulang Kapasitas. Untuk mengubah pengaturan Penyeimbangan Ulang Kapasitas, Anda harus menghapus armada dan membuat armada baru.

Opsi konfigurasi

Armada `ReplacementStrategy` untuk EC2 dan Armada Spot mendukung dua nilai berikut:

`launch-before-terminate`

Amazon EC2 mengakhiri Instans Spot yang menerima notifikasi penyeimbangan ulang setelah Instans Spot pengganti baru diluncurkan. Jika Anda menentukan `launch-before-terminate`, Anda juga harus menentukan nilai untuk `termination-delay`. Setelah instans pengganti baru diluncurkan, Amazon EC2 menunggu durasi `termination-delay`, lalu mengakhiri instans lama. Untuk `termination-delay`, minimum adalah 120 detik (2 menit), dan maksimum adalah 7200 detik (2 jam).

Sebaiknya Anda menggunakan `launch-before-terminate` hanya jika Anda dapat memprediksi lamanya prosedur pematian instans Anda akan selesai. Hal ini akan memastikan bahwa instans lama diakhiri hanya setelah prosedur pematian selesai. Perhatikan bahwa Amazon EC2 dapat menginterupsi instans lama dengan peringatan dua menit sebelum `termination-delay`.

Kami sangat menyarankan agar tidak menggunakan strategi alokasi `lowest-price` (Armada EC2) atau `lowestPrice` (Armada Spot) yang dikombinasikan dengan `launch-before-terminate` untuk menghindari penggantian Instans Spot yang juga berisiko tinggi mengalami gangguan.

`launch`

Amazon EC2 meluncurkan Instans Spot pengganti saat notifikasi penyeimbangan ulang dipancarkan untuk Instans Spot yang sudah ada. Amazon EC2 tidak mengakhiri instans yang menerima notifikasi penyeimbangan ulang. Anda dapat mengakhiri instans lama, atau membiarkannya berjalan. Anda dikenai biaya untuk semua instans saat semuanya berjalan.

Pertimbangan-pertimbangan

Jika Anda mengonfigurasi Armada EC2 atau Armada Spot untuk Penyeimbangan Kembali Kapasitas, pertimbangkan hal berikut:

Berikan sebanyak mungkin kolam kapasitas Spot dalam permintaan

Konfigurasikan armada Anda untuk menggunakan beberapa jenis instans dan Availability Zone. Hal ini akan memberikan fleksibilitas untuk meluncurkan Instans Spot di berbagai kolam kapasitas Spot. Untuk informasi selengkapnya, lihat Bersikaplah fleksibel terkait tipe instans dan Zona Ketersediaan.

Hindari peningkatan risiko gangguan penggantian Instans Spot

Untuk menghindari peningkatan risiko gangguan, kami merekomendasikan strategi `capacity-optimized` atau `capacity-optimized-prioritized` alokasi. Strategi ini memastikan bahwa Instans Spot diluncurkan di kolam kapasitas Spot yang paling optimal, dan karena itu kemungkinan tidak akan terinterupsi dalam waktu dekat. Untuk informasi selengkapnya, lihat Menggunakan strategi alokasi harga dan kapasitas yang dioptimalkan.

Jika Anda menggunakan strategi `lowest-price` alokasi, Instans Spot pengganti Anda mungkin berisiko tinggi mengalami gangguan. Hal ini disebabkan karena Amazon EC2 akan selalu meluncurkan instans di kolam dengan harga terendah yang memiliki kapasitas yang tersedia pada saat itu, meskipun Instans Spot pengganti Anda kemungkinan akan terinterupsi sesaat setelah diluncurkan.

Amazon EC2 hanya akan meluncurkan instans baru jika ketersediaannya sama atau lebih baik

Salah satu tujuan dari Penyeimbangan Ulang kapasitas adalah untuk meningkatkan ketersediaan Instans Spot. Jika Instans Spot yang ada menerima rekomendasi penyeimbangan ulang, Amazon EC2 hanya akan meluncurkan instans baru jika instans baru tersebut memberikan ketersediaan yang sama atau lebih baik daripada instans yang sudah ada. Jika risiko gangguan instans baru akan lebih buruk daripada instans yang sudah ada, Amazon EC2 tidak akan meluncurkan instans baru. Namun, Amazon EC2 akan terus menilai kolam kapasitas Spot, dan akan meluncurkan instans baru jika ketersediaan membaik.

Ada kemungkinan instans Anda yang ada akan terinterupsi tanpa Amazon EC2 yang secara proaktif meluncurkan instans baru. Jika hal ini terjadi, Amazon EC2 akan berupaya meluncurkan instans baru terlepas dari apakah instans baru tersebut memiliki risiko gangguan yang tinggi.

Penyeimbangan Ulang Kapasitas tidak meningkatkan tingkat interupsi Instans Spot Anda

Saat Anda mengaktifkan Penyeimbangan Ulang Kapasitas, hal tersebut tidak meningkatkan tingkat interupsi Instans Spot Anda (jumlah Instans Spot yang diklaim kembali saat Amazon EC2 membutuhkan kapasitas kembali). Namun, jika Penyeimbangan Ulang Kapasitas mendeteksi instans yang berada pada berisiko terinterupsi, Amazon EC2 akan segera berupaya meluncurkan instans baru. Hasilnya adalah lebih banyak instans yang mungkin diganti dibandingkan jika Anda menunggu Amazon EC2 meluncurkan instans baru setelah instans yang berisiko terinterupsi.

Meskipun Anda dapat mengganti lebih banyak instans dengan Penyeimbangan Ulang Kapasitas diaktifkan, Anda akan mendapatkan keuntungan dengan bersikap proaktif daripada reaktif dengan memiliki lebih banyak waktu untuk mengambil tindakan sebelum instans Anda terinterupsi. Dengan pemberitahuan interupsi Instans Spot, Anda biasanya hanya memiliki waktu hingga dua menit untuk mematikan instans Anda dengan baik. Dengan Penyeimbangan Ulang Kapasitas meluncurkan instans baru terlebih dahulu, Anda memberikan kesempatan yang lebih baik untuk menyelesaikan proses yang sudah ada pada instans berisiko, Anda dapat memulai prosedur pematian instans, dan mencegah pekerjaan baru dijadwalkan pada instans berisiko Anda. Anda juga bisa mulai menyiapkan instans yang baru diluncurkan untuk mengambil alih aplikasi. Dengan penggantian proaktif dari Penyeimbangan Ulang Kapasitas, Anda akan mendapatkan keuntungan dari kesinambungan yang baik.

Sebagai contoh teoretis untuk menunjukkan risiko dan manfaat menggunakan Penyeimbangan Ulang Kapasitas, pertimbangkan skenario berikut:

- 14:00 – Rekomendasi penyeimbangan ulang diterima untuk instans-A, dan Amazon EC2 segera mulai berupaya meluncurkan instans-B pengganti, sehingga memberi Anda waktu untuk memulai prosedur pematian.*
- 14:30 – Rekomendasi penyeimbangan ulang diterima untuk instans-B, diganti dengan instans-C, sehingga memberi Anda waktu untuk memulai prosedur pematian.*
- 14:32 – Jika Penyeimbangan Ulang Kapasitas tidak diaktifkan, dan jika pemberitahuan interupsi Instans Spot akan diterima pada pukul 14:32 untuk instans-A, Anda hanya memiliki waktu hingga dua menit untuk mengambil tindakan, tetapi Instans-A akan berjalan hingga saat ini.

* Jika `launch-before-terminate` ditentukan, Amazon EC2 akan mengakhiri instans yang berada dalam risiko setelah instans pengganti online.

Amazon EC2 dapat meluncurkan Instans Spot pengganti yang baru hingga kapasitas yang terpenuhi adalah dua kali lipat dari kapasitas target

Ketika armada dikonfigurasi untuk Penyeimbangan Kembali Kapasitas, armada mencoba meluncurkan Instans Spot pengganti baru untuk setiap Instans Spot yang menerima rekomendasi penyeimbangan kembali. Setelah Instans Spot menerima rekomendasi penyeimbangan ulang, Instans Spot tersebut tidak lagi dianggap sebagai bagian dari kapasitas yang terpenuhi. Bergantung pada strategi penggantian, Amazon EC2 akan mengakhiri instans setelah penundaan pengakhiran yang telah dikonfigurasikan sebelumnya, atau membiarkannya tetap berjalan. Hal ini memberikan kesempatan kepada Anda untuk melakukan tindakan penyeimbangan ulang pada instans.

Jika armada Anda mencapai dua kali lipat dari kapasitas target, armada akan berhenti meluncurkan instans pengganti yang baru meskipun instans pengganti itu sendiri menerima rekomendasi penyeimbangan ulang.

Misalnya, Anda membuat armada dengan kapasitas target 100 Instans Spot. Semua Instans Spot menerima rekomendasi penyeimbangan ulang, yang menyebabkan Amazon EC2 meluncurkan 100 Instans Spot pengganti. Hal ini meningkatkan jumlah Instans Spot yang terpenuhi menjadi 200, atau dua kali lipat dari kapasitas yang ditargetkan. Beberapa instans pengganti menerima rekomendasi penyeimbangan kembali, tetapi tidak ada lagi instance pengganti yang diluncurkan karena armada tidak dapat melebihi dua kali lipat kapasitas targetnya.

Perhatikan bahwa Anda dikenai biaya untuk semua instans saat berjalan.

Kami menyarankan Anda mengonfigurasi armada Anda untuk menghentikan Instans Spot yang menerima rekomendasi penyeimbangan ulang

Jika Anda mengonfigurasi armada untuk Penyeimbangan Kembali Kapasitas, kami sarankan Anda memilih `launch-before-terminate` dengan penundaan penghentian yang sesuai hanya jika Anda dapat memprediksi berapa lama prosedur penghentian instans Anda akan selesai. Hal ini akan memastikan bahwa instans lama diakhiri hanya setelah prosedur pematian selesai.

Jika memilih untuk mengakhiri instans yang direkomendasikan untuk penyeimbangan ulang, kami menyarankan Anda untuk memantau sinyal rekomendasi penyeimbangan ulang yang diterima oleh Instans Spot di armada. Dengan memantau sinyal, Anda dapat dengan cepat melakukan tindakan penyeimbangan ulang pada instans yang terpengaruh sebelum Amazon EC2 menginterupsinya, lalu Anda dapat mengakhirinya secara manual. Jika Anda tidak mengakhiri instans tersebut, Anda akan terus membayarnya saat instans tersebut berjalan. Amazon EC2 tidak secara otomatis mengakhiri instans yang menerima notifikasi penyeimbangan ulang.

Anda dapat mengatur notifikasi menggunakan Amazon EventBridge atau metadata instans. Untuk informasi selengkapnya, lihat Pantau sinyal rekomendasi penyeimbangan kembali.

Armada tidak menghitung instance yang menerima rekomendasi penyeimbangan kembali saat menghitung kapasitas yang terpenuhi selama skala masuk atau keluar

Jika armada Anda dikonfigurasi untuk Penyeimbangan Kembali Kapasitas, dan Anda mengubah kapasitas target menjadi skala atau skala keluar, armada tidak menghitung instans yang ditandai untuk penyeimbangan kembali sebagai bagian dari kapasitas yang terpenuhi, sebagai berikut:

- Menskalakan ke dalam – Jika Anda menurunkan kapasitas target yang Anda inginkan, Amazon EC2 akan mengakhiri instans yang tidak ditandai untuk penyeimbangan ulang hingga kapasitas yang diinginkan tercapai. Instans yang ditandai untuk penyeimbangan ulang tidak diperhitungkan pada kapasitas yang terpenuhi.

  Misalnya, Anda membuat armada dengan kapasitas target 100 Instans Spot. 10 instans menerima rekomendasi penyeimbangan ulang, sehingga Amazon EC2 meluncurkan 10 instans pengganti baru, menghasilkan kapasitas terpenuhi 110 instans. Anda kemudian mengurangi kapasitas target menjadi 50 (menskalakan ke dalam), tetapi kapasitas yang terpenuhi sebenarnya adalah 60 instans karena 10 instans yang ditandai untuk penyeimbangan ulang tidak diakhiri oleh Amazon EC2. Anda harus mengakhiri instans ini secara manual, atau Anda dapat membiarkannya tetap berjalan.
- Menskalakan ke luar – Jika Anda meningkatkan kapasitas target yang diinginkan, Amazon EC2 akan meluncurkan instans baru hingga kapasitas yang diinginkan tercapai. Instans yang ditandai untuk penyeimbangan ulang tidak diperhitungkan pada kapasitas yang terpenuhi.

  Misalnya, Anda membuat armada dengan kapasitas target 100 Instans Spot. 10 instans menerima rekomendasi penyeimbangan ulang, sehingga armada meluncurkan 10 instans pengganti baru, menghasilkan kapasitas terpenuhi 110 instans. Anda kemudian meningkatkan kapasitas target menjadi 200 (menskalakan ke luar), tetapi kapasitas yang terpenuhi sebenarnya adalah 210 instans karena 10 instans yang ditandai untuk penyeimbangan ulang tidak diperhitungkan oleh armada sebagai bagian dari kapasitas target. Anda harus mengakhiri instans ini secara manual, atau Anda dapat membiarkannya tetap berjalan.

Gunakan Reservasi Kapasitas untuk memesan kapasitas Sesuai Permintaan di Armada EC2

Dengan Reservasi Kapasitas Sesuai Permintaan, Anda dapat memesan kapasitas komputasi untuk Instans Sesuai Permintaan di Zona Ketersediaan tertentu untuk durasi berapa pun. Anda dapat mengonfigurasi Armada EC2 untuk menggunakan Reservasi Kapasitas terlebih dahulu saat meluncurkan Instans Sesuai Permintaan.

Pemesanan Kapasitas Sesuai Permintaan hanya tersedia untuk Armada EC2 dengan jenis permintaan yang diatur ke. `instant`

Reservasi Kapasitas dikonfigurasi sebagai `open` atau `targeted`. Armada EC2 dapat meluncurkan Instans Sesuai Permintaan ke dalam Reservasi Kapasitas `open` atau `targeted`, sebagai berikut:

- Jika Reservasi Kapasitas adalah `open`, Instans Sesuai Permintaan yang memiliki atribut yang cocok secara otomatis akan berjalan dalam kapasitas terpesan.
- Jika Reservasi Kapasitas adalah `targeted`, Instans Sesuai Permintaan harus secara khusus menargetkannya untuk dijalankan dalam kapasitas terpesan. Hal ini berguna untuk menggunakan Reservasi Kapasitas tertentu atau untuk mengontrol kapan harus menggunakan Reservasi Kapasitas tertentu.

Jika Anda menggunakan Reservasi Kapasitas `targeted` di Armada EC2, harus ada Reservasi Kapasitas yang cukup untuk memenuhi kapasitas target Sesuai Permintaan, atau peluncuran gagal. Untuk menghindari kegagalan peluncuran, lebih baik tambahkan Reservasi Kapasitas `targeted` ke grup sumber daya, lalu targetkan grup sumber daya tersebut. Grup sumber daya tidak perlu memiliki cukup Reservasi Kapasitas; jika kehabisan Reservasi Kapasitas sebelum kapasitas target Sesuai Permintaan terpenuhi, armada dapat meluncurkan kapasitas target yang tersisa ke dalam kapasitas Sesuai Permintaan reguler.

Untuk menggunakan Reservasi Kapasitas dengan Armada EC2

1. Konfigurasikan armada sebagai tipe `instant`. Anda tidak dapat menggunakan Reservasi Kapasitas untuk armada tipe lain.
2. Konfigurasikan strategi penggunaan untuk Reservasi Kapasitas sebagai `use-capacity-reservations-first`.

3. Pada templat peluncuran, untuk Reservasi kapasitas, pilih Buka atau Target berdasarkan grup. Jika Anda memilih Target berdasarkan grup, tentukan ID grup sumber daya Reservasi Kapasitas.

Ketika armada mencoba untuk memenuhi kapasitas Sesuai Permintaan, jika armada menemukan bahwa lebih dari satu kolam instans memiliki Reservasi Kapasitas yang cocok yang tidak terpakai, armada akan menentukan kolam yang akan digunakan untuk meluncurkan Instans Sesuai Permintaan berdasarkan strategi alokasi Sesuai Permintaan (`lowest-price` atau `prioritized`).

Sumber daya terkait

- Untuk contoh CLI tentang cara mengonfigurasi armada untuk menggunakan Reservasi Kapasitas untuk memenuhi kapasitas Sesuai Permintaan, lihatContoh konfigurasi CLI untuk Armada EC2, khususnya Contoh 5 hingga 7.
- Untuk tutorial yang membawa Anda melalui langkah-langkah untuk membuat Reservasi Kapasitas, menggunakannya di armada Anda, dan melihat berapa banyak Reservasi Kapasitas yang tersisa, lihat Tutorial: Konfigurasikan Armada EC2 untuk meluncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas yang ditargetkan
- Untuk informasi tentang mengonfigurasi Reservasi Kapasitas, lihat Cadangan kapasitas komputasi dengan Reservasi Kapasitas Sesuai Permintaan EC2 dan Reservasi Kapasitas Sesuai Permintaan. FAQs

Bekerja dengan Armada EC2

Untuk mulai menggunakan Armada EC2, buat permintaan yang mencakup total kapasitas target, kapasitas Sesuai Permintaan, kapasitas Spot, dan templat peluncuran yang menentukan konfigurasi untuk instans dalam armada. Anda dapat menentukan parameter tambahan secara opsional, atau membiarkan armada menggunakan nilai default. Anda juga dapat menandai permintaan armada, serta instance dan volumenya, saat Anda membuat armada.

Armada meluncurkan Instans Sesuai Permintaan ketika ada kapasitas yang tersedia, dan meluncurkan Instans Spot ketika harga maksimum Anda melebihi harga Spot dan kapasitas yang tersedia.

Setelah armada Anda diluncurkan, Anda dapat menjelaskan permintaan armada, instance dalam armada, dan peristiwa armada apa pun. Anda juga dapat menetapkan tag tambahan sesuai kebutuhan.

Jika Anda perlu mengubah parameter armada apa pun, seperti total kapasitas target, Anda dapat memodifikasi armada, asalkan dikonfigurasi untuk mempertahankan kapasitas. Anda tidak dapat mengubah kapasitas permintaan satu kali setelah dikirimkan.

Permintaan armada tetap aktif sampai habis masa berlakunya atau Anda menghapusnya. Saat menghapus permintaan armada, Anda dapat menghentikan instance atau membiarkannya berjalan. Jika Anda memilih untuk membiarkannya berjalan, Instans Sesuai Permintaan berjalan hingga Anda menghentikannya, dan Instans Spot berjalan hingga terputus atau Anda menghentikannya.

Topik

- Status permintaan Armada EC2
- Prasyarat Armada EC2
- Membuat Armada EC2
- Tandai permintaan Armada EC2 baru atau yang sudah ada serta instans serta volume yang diluncurkan
- Jelaskan Armada EC2, instance-nya, dan kejadiannya
- Memodifikasi Armada EC2
- Menghapus permintaan Armada EC2 dan instans di armada

Status permintaan Armada EC2

Permintaan Armada EC2 dapat berupa salah satu dari berbagai status, dengan setiap status menunjukkan tahapan siklus hidup permintaan yang berbeda dan pengelolaan instansnya.

Permintaan Armada EC2 dapat berada dalam salah satu status berikut:

`submitted`

Permintaan Armada EC2 sedang dievaluasi dan Amazon EC2 sedang bersiap untuk meluncurkan jumlah target instans. Jika permintaan melebihi batas armada Anda, permintaan akan segera dihapus.

`active`

Armada EC2 telah divalidasi dan Amazon EC2 berupaya untuk mempertahankan jumlah target dari instans yang sedang berjalan. Permintaan tetap berada dalam status ini sampai dimodifikasi atau dihapus.

`modifying`

Permintaan Armada EC2 sedang dimodifikasi. Permintaan tetap berada dalam status ini sampai modifikasi diproses sepenuhnya atau permintaan dihapus. Hanya tipe armada `maintain` yang dapat dimodifikasi. Status ini tidak berlaku untuk tipe permintaan lain.

`deleted_running`

Permintaan Armada EC2 dihapus dan tidak meluncurkan Instans Spot tambahan. Instans yang ada terus berjalan sampai diinterupsi atau diakhiri secara manual. Permintaan tetap berada dalam status ini sampai semua instans diinterupsi atau diakhiri. Hanya tipe Armada EC2 `maintain` atau `request` yang dapat menjalankan instans setelah permintaan Armada EC2 dihapus. Armada `instant` yang dihapus dengan instans yang sedang berjalan tidak didukung. Status ini tidak berlaku untuk armada `instant`.

`deleted_terminating`

Permintaan Armada EC2 dihapus dan instansnya diakhiri. Permintaan tetap dalam keadaan ini sampai semua contoh dihentikan.

`deleted`

Permintaan Armada EC2 dihapus dan tidak ada instans yang berjalan. Permintaan tersebut dihapus dua hari setelah instansnya diakhiri.

Prasyarat Armada EC2

Untuk membuat Armada EC2, prasyarat berikut harus ada:

- Luncurkan templat
- Peran tertaut layanan untuk Armada EC2
- Berikan akses ke kunci yang dikelola pelanggan untuk digunakan dengan snapshot terenkripsi AMIs dan EBS
- Izin untuk pengguna Armada EC2

Luncurkan templat

Template peluncuran menentukan informasi konfigurasi tentang instance yang akan diluncurkan, seperti jenis instance dan Availability Zone. Untuk informasi selengkapnya tentang template peluncuran, lihatSimpan parameter peluncuran instans di templat peluncuran Amazon EC2.

Peran tertaut layanan untuk Armada EC2

Peran `AWSServiceRoleForEC2Fleet` memberikan izin kepada Armada EC2 untuk meminta, meluncurkan, mengakhiri, dan menandai instans atas nama Anda. Amazon EC2 menggunakan peran tertaut layanan ini untuk menyelesaikan tindakan berikut:

- `ec2:RunInstances` – Meluncurkan instans.
- `ec2:RequestSpotInstances` – Meminta Instans Spot.
- `ec2:TerminateInstances` – Mengakhiri instans.
- `ec2:DescribeImages`— Jelaskan Amazon Machine Images (AMIs) untuk instance.
- `ec2:DescribeInstanceStatus`— Jelaskan status instance.
- `ec2:DescribeSubnets`— Jelaskan subnet untuk contoh.
- `ec2:CreateTags` – Menambahkan tanda ke Armada, instans, dan volume EC2.

Pastikan peran ini ada sebelum Anda menggunakan AWS CLI atau API untuk membuat Armada EC2.

> **Note**
>
> Armada EC2 `instant` tidak membutuhkan peran ini.

Untuk membuat peran, gunakan konsol IAM sebagai berikut.

Untuk membuat AWSServiceRoleForEC2Fleet peran untuk Armada EC2

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran.
3. Pilih Buat peran.
4. Pada halaman Pilih entitas tepercaya, lakukan hal berikut:
   a. Untuk jenis entitas Tepercaya, pilih AWS layanan.
   b. Di bawah Kasus penggunaan, untuk Layanan atau kasus penggunaan, pilih EC2 - Armada.

> **Tip**
>
> Pastikan untuk memilih EC2 - Armada. Jika Anda memilih EC2, kasus penggunaan EC2 - Armada tidak muncul dalam daftar Kasus penggunaan. EC2 - Kasus penggunaan Armada akan secara otomatis membuat kebijakan dengan izin IAM yang diperlukan dan akan menyarankan AWSServiceRoleForEC2Armada sebagai nama peran.

c. Pilih Berikutnya.

5. Pada halaman Tambahkan izin, pilih Berikutnya.
6. Pada halaman Nama, tinjau, dan buat, pilih Buat peran.

Jika Anda tidak perlu lagi menggunakan Armada EC2, kami sarankan Anda menghapus peran AWSServiceRoleForEC2Armada. Setelah peran ini dihapus dari akun Anda, Anda dapat membuat peran tersebut kembali jika Anda membuat armada lain.

Untuk informasi selengkapnya, lihat Peran terkait layanan di Panduan Pengguna IAM.

Berikan akses ke kunci yang dikelola pelanggan untuk digunakan dengan snapshot terenkripsi AMIs dan EBS

Jika Anda menentukan AMI terenkripsi atau snapshot Amazon EBS terenkripsi di Armada EC2 dan Anda menggunakan AWS KMS kunci untuk enkripsi, Anda harus memberikan AWSService RoleFor EC2 izin peran Armada untuk menggunakan kunci yang dikelola pelanggan sehingga Amazon EC2 dapat meluncurkan instans atas nama Anda. Untuk melakukannya, Anda harus menambahkan pemberian izin ke kunci yang dikelola pelanggan, seperti yang ditunjukkan dalam prosedur berikut.

Ketika memberikan izin, pemberian izin merupakan alternatif dari kebijakan kunci. Untuk informasi selengkapnya, lihat Menggunakan pemberian izin dan Menggunakan kebijakan kunci di AWS KMS dalam Panduan Developer AWS Key Management Service .

Untuk memberikan izin peran AWSService RoleFor EC2 Armada untuk menggunakan kunci terkelola pelanggan

- Gunakan perintah create-grant untuk menambahkan hibah ke kunci yang dikelola pelanggan dan untuk menentukan prinsipal (peran terkait layanan AWSServiceRoleForEC2Armada) yang diberikan izin untuk melakukan operasi yang diizinkan hibah. Kunci yang dikelola

pelanggan ditentukan oleh parameter `key-id` dan ARN kunci yang dikelola pelanggan. Prinsipal ditentukan oleh `grantee-principal` parameter dan ARN dari peran terkait layanan AWSServiceRoleForEC2Armada.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Izin untuk pengguna Armada EC2

Jika pengguna Anda akan membuat atau mengelola Armada EC2, pastikan untuk memberikan izin kepada pengguna.

Untuk membuat kebijakan Armada EC2

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Di halaman Buat kebijakan, pilih tab JSON, ganti teks dengan berikut ini, dan pilih Tinjau kebijakan.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
}
```

`ec2:*` memberikan izin kepada pengguna untuk memanggil semua tindakan API Amazon EC2. Untuk membatasi pengguna pada tindakan API Amazon EC2 tertentu, tentukan tindakan tersebut.

Pengguna harus memiliki izin untuk memanggil tindakan `iam:ListRoles` untuk melakukan enumerasi peran IAM yang sudah ada, tindakan `iam:PassRole` untuk menentukan peran Armada EC2, dan tindakan `iam:ListInstanceProfiles` untuk melakukan enumerasi profil instans yang sudah ada.

(Opsional) Untuk memungkinkan pengguna membuat peran atau profil instans menggunakan konsol IAM, Anda juga harus menambahkan tindakan berikut ke kebijakan:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. Pada halaman Tinjau kebijakan, masukkan nama dan deskripsi kebijakan, dan pilih Buat kebijakan.
6. Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

   - Pengguna dan grup di AWS IAM Identity Center:

     Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Membuat Armada EC2

Untuk membuat Armada EC2, tentukan konfigurasi armada dalam file JSON dan referensikan file dengan perintah create-fleet. Dalam file JSON, Anda harus menentukan total kapasitas target untuk armada, kapasitas target terpisah untuk Instans Spot dan Instans Sesuai Permintaan, dan templat peluncuran yang menentukan konfigurasi untuk instance dalam armada, seperti AMI, tipe instans, subnet atau Availability Zone, dan satu atau beberapa grup keamanan. Anda dapat menentukan konfigurasi tambahan secara opsional, seperti parameter untuk mengganti konfigurasi template peluncuran, strategi alokasi untuk memilih Instans Spot dan Instans Sesuai Permintaan dari kumpulan kapasitas EC2, dan jumlah maksimum yang bersedia Anda bayarkan untuk armada. Untuk informasi selengkapnya, lihat Opsi konfigurasi untuk Armada EC2 atau Armada Spot.

Armada EC2 meluncurkan Instans Sesuai Permintaan saat kapasitas tersedia, dan meluncurkan Instans Spot ketika harga maksimum Anda melebihi harga Spot dan kapasitas yang tersedia.

Jika armada Anda menyertakan Instans Spot dan jenisnya`maintain`, Amazon EC2 akan berusaha mempertahankan kapasitas target armada Anda saat Instans Spot Anda terganggu.

Batasan Armada EC2

Batasan berikut berlaku untuk Armada EC2:

- Membuat Armada EC2 hanya tersedia melalui Amazon EC2 API AWS CLI,, AWS SDKs, dan. CloudFormation
- Permintaan Armada EC2 tidak dapat menjangkau AWS Wilayah. Anda perlu membuat Armada EC2 terpisah untuk setiap Wilayah.

- Permintaan Armada EC2 tidak dapat menjangkau subnet yang berbeda dari Zona Ketersediaan yang sama.

Membuat Armada EC2

Untuk meluncurkan armada instans menggunakan Armada EC2, Anda hanya perlu menentukan parameter berikut dalam permintaan armada Anda, dan armada akan menggunakan nilai default untuk parameter lainnya:

- `LaunchTemplateId`atau `LaunchTemplateName` — Menentukan template peluncuran yang akan digunakan (yang berisi parameter untuk instance yang akan diluncurkan, seperti jenis instance dan Availability Zone)
- `TotalTargetCapacity` – Menentukan total kapasitas target untuk armada
- `DefaultTargetCapacityType` – Menentukan apakah opsi pembelian default adalah Sesuai Permintaan atau Spot

Untuk mengganti parameter yang ditentukan dalam template peluncuran, Anda dapat menentukan satu atau beberapa penggantian. Setiap override dapat bervariasi menurut jenis instans, Availability Zone, subnet, dan harga maksimum, dan dapat mencakup kapasitas tertimbang yang berbeda. Sebagai alternatif untuk menentukan jenis instans, Anda dapat menentukan atribut yang harus dimiliki instance, dan Amazon EC2 akan mengidentifikasi semua jenis instance dengan atribut tersebut. Untuk informasi selengkapnya, lihat Tentukan atribut untuk pemilihan tipe contoh untuk Armada EC2 atau Armada Spot.

Untuk jenis Armada EC2`instant`, Anda dapat menentukan parameter Systems Manager, bukan ID AMI. Anda dapat menentukan parameter Systems Manager di override atau di template peluncuran. Untuk informasi selengkapnya, lihat Gunakan parameter Systems Manager alih-alih ID AMI.

Anda dapat menentukan parameter armada dalam file JSON. Untuk informasi tentang semua parameter yang mungkin dapat Anda tentukan, lihatLihat semua opsi konfigurasi Armada EC2.

Untuk contoh konfigurasi armada, lihatContoh konfigurasi CLI untuk Armada EC2.

Saat ini tidak ada dukungan konsol untuk membuat Armada EC2.

Untuk membuat Armada EC2

Gunakan perintah create-fleet untuk membuat armada dan tentukan file JSON yang berisi parameter konfigurasi armada.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Berikut adalah contoh output untuk armada tipe `request` atau `maintain`.

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Berikut adalah contoh output untuk tipe armada `instant` yang meluncurkan kapasitas target.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
```

```
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

Berikut adalah contoh output untuk armada tipe `instant` yang meluncurkan sebagian kapasitas target dengan kesalahan untuk instans yang tidak diluncurkan.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
```

```
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

Berikut adalah contoh output untuk armada tipe `instant` yang tidak meluncurkan instans.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
```

```
    },
  ],
  "Instances": []
}
```

Buat Armada EC2 yang menggantikan Instans Spot yang tidak sehat

Armada EC2 memeriksa status kondisi instans di armada setiap dua menit. Status kondisi instans adalah `healthy` atau `unhealthy`.

Armada EC2 menentukan status kondisi instans dengan menggunakan pemeriksaan status yang disediakan oleh Amazon EC2. Sebuah instans ditentukan sebagai `unhealthy` jika status pemeriksaan status instans atau pemeriksaan status sistemnya `impaired` dalam tiga kali pemeriksaan kondisi secara berturut-turut. Untuk informasi selengkapnya, lihat Pemeriksaan status untuk instans Amazon EC2.

Anda dapat mengonfigurasi armada untuk mengganti Instans Spot yang tidak sehat. Setelah mengatur `ReplaceUnhealthyInstances` ke `true`, Instans Spot diganti ketika dilaporkan sebagai `unhealthy`. Armada tersebut dapat berada di bawah kapasitas targetnya selama beberapa menit saat Instans Spot yang tidak sehat sedang diganti.

Persyaratan

- Penggantian pemeriksaan kondisi hanya didukung untuk Armada EC2 yang mempertahankan kapasitas target (armada tipe `maintain`), dan bukan untuk armada tipe `request` atau `instant`.
- Penggantian pemeriksaan kondisi hanya didukung untuk Instans Spot. Fitur ini tidak didukung untuk Instans Sesuai Permintaan.
- Anda dapat mengonfigurasi Armada EC2 untuk mengganti instans yang tidak sehat hanya saat Anda membuatnya.
- Pengguna dapat menggunakan penggantian pemeriksaan kondisi hanya jika memiliki izin untuk memanggil tindakan `ec2:DescribeInstanceStatus`.

Untuk mengonfigurasi Armada EC2 guna mengganti Instans Spot yang tidak sehat

1. Gunakan informasi untuk membuat Armada EC2 diMembuat Armada EC2.
2. Untuk mengonfigurasi armada untuk mengganti Instans Spot yang tidak sehat, dalam file JSON, untuk`ReplaceUnhealthyInstances`, tentukan. `true`

Lihat semua opsi konfigurasi Armada EC2

Untuk melihat daftar lengkap parameter konfigurasi Armada EC2, Anda dapat membuat file JSON. Untuk deskripsi setiap parameter, lihat create-fleet.

Untuk menghasilkan file JSON dengan semua kemungkinan parameter Armada EC2

Gunakan perintah create-fleet (AWS CLI) dan parameter `--generate-cli-skeleton` untuk membuat file JSON Armada EC2, dan arahkan output ke file untuk menyimpannya.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

Berikut ini adalah output contoh.

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
```

```
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "MemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        },
                        "CpuManufacturers": [
                            "amd"
                        ],
                        "MemoryGiBPerVCpu": {
                            "Min": 0.0,
                            "Max": 0.0
                        },
                        "ExcludedInstanceTypes": [
                            ""
                        ],
```

```
                    "InstanceGenerations": [
                        "previous"
                    ],
                    "SpotMaxPricePercentageOverLowestPrice": 0,
                    "OnDemandMaxPricePercentageOverLowestPrice": 0,
                    "BareMetal": "included",
                    "BurstablePerformance": "required",
                    "RequireHibernateSupport": true,
                    "NetworkInterfaceCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "LocalStorage": "excluded",
                    "LocalStorageTypes": [
                        "ssd"
                    ],
                    "TotalLocalStorageGB": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "BaselineEbsBandwidthMbps": {
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorTypes": [
                        "inference"
                    ],
                    "AcceleratorCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorManufacturers": [
                        "amd"
                    ],
                    "AcceleratorNames": [
                        "a100"
                    ],
                    "AcceleratorTotalMemoryMiB": {
                        "Min": 0,
                        "Max": 0
                    }
                }
            }
        ]
```

```
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 0,
        "DefaultTargetCapacityType": "on-demand",
        "TargetCapacityUnitType": "memory-mib"
    },
    "TerminateInstancesWithExpiration": true,
    "Type": "instant",
    "ValidFrom": "1970-01-01T00:00:00",
    "ValidUntil": "1970-01-01T00:00:00",
    "ReplaceUnhealthyInstances": true,
    "TagSpecifications": [
        {
            "ResourceType": "fleet",
            "Tags": [
                {
                    "Key": "",
                    "Value": ""
                }
            ]
        }
    ],
    "Context": ""
}
```

Tandai permintaan Armada EC2 baru atau yang sudah ada serta instans serta volume yang diluncurkan

Untuk membantu mengkategorikan dan mengelola permintaan Armada EC2 serta instans serta volume yang diluncurkan, Anda dapat menandainya dengan metadata khusus. Anda dapat menetapkan tanda untuk permintaan Armada EC2 saat membuatnya, atau sesudahnya. Demikian pula, Anda dapat menetapkan tag ke instance dan volume saat diluncurkan oleh armada, atau sesudahnya.

Saat Anda menandai permintaan armada, instans dan volume yang diluncurkan oleh armada tidak ditandai secara otomatis. Anda perlu menandai instans dan volume yang diluncurkan oleh armada secara eksplisit. Anda dapat memilih untuk menetapkan tag hanya untuk permintaan armada, atau

hanya instans yang diluncurkan oleh armada, atau hanya volume yang dilampirkan pada instans yang diluncurkan oleh armada, atau semuanya.

> **Note**
>
> Untuk tipe armada `instant`, Anda dapat menandai volume yang dilampirkan ke Instans Sesuai Permintaan dan Instans Spot. Untuk tipe armada `request` atau `maintain`, Anda hanya dapat menandai volume yang dilampirkan ke Instans Sesuai Permintaan.

Untuk informasi selengkapnya tentang cara kerja tag, lihat Tandai sumber daya Amazon EC2 Anda.

Prasyarat

Berikan izin kepada pengguna untuk menandai sumber daya. Untuk informasi selengkapnya, lihat Contoh: Memberi tanda pada sumber daya.

Berikan izin kepada pengguna untuk menandai sumber daya

Buat kebijakan IAM yang mencakup hal-hal berikut:

- Tindakan `ec2:CreateTags`. Tindakan ini memberikan izin kepada pengguna untuk membuat tanda.
- Tindakan `ec2:CreateFleet`. Tindakan ini memberikan izin kepada pengguna untuk membuat permintaan Armada EC2.
- Untuk `Resource`, kami sarankan Anda menentukan `"*"`. Tindakan ini memungkinkan pengguna untuk menandai semua tipe sumber daya.

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.
- Pengguna IAM:

- Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
- (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Untuk menandai permintaan Armada EC2 baru

Untuk menandai permintaan Armada EC2 saat Anda membuatnya, tentukan pasangan kunci-nilai di file JSON yang digunakan untuk membuat armada. Nilai untuk `ResourceType` harus `fleet`. Jika Anda menentukan nilai lain, permintaan armada akan gagal.

Untuk menandai instans dan volume yang diluncurkan oleh Armada EC2

Untuk menandai instans dan volume saat diluncurkan oleh armada tersebut, tentukan tanda di luncurkan templat yang direferensikan dalam permintaan Armada EC2.

> **Note**
>
> Anda tidak dapat menandai volume yang dilampirkan ke Instans Spot yang diluncurkan oleh tipe armada `request` atau `maintain`.

Untuk menandai permintaan, instans, dan volume Armada EC2 yang ada

Gunakan perintah create-tags untuk menandai sumber daya yang ada.

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Jelaskan Armada EC2, instance-nya, dan kejadiannya

Anda dapat menjelaskan konfigurasi Armada EC2, instans di Armada EC2, dan riwayat peristiwa Armada EC2.

Tugas

- Jelaskan Armada EC2 Anda

- Jelaskan semua instans di Armada EC2 Anda
- Jelaskan riwayat acara untuk Armada EC2 Anda

Jelaskan Armada EC2 Anda

AWS CLI

Untuk menggambarkan Armada EC2 Anda

Gunakan perintah deskripsi-armada.

```
aws ec2 describe-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Berikut ini adalah output contoh.

```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
```

```
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

PowerShell

Untuk menggambarkan Armada EC2 Anda

Gunakan Get-EC2FleetListcmdlet.

```
Get-EC2FleetList `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Jelaskan semua instans di Armada EC2 Anda

Daftar instans yang sedang berjalan yang dikembalikan diperbarui secara berkala dan mungkin sudah lawas.

AWS CLI

Untuk menjelaskan instance untuk Armada EC2 yang ditentukan

Gunakan perintah describe-fleet-instances.

```
aws ec2 describe-fleet-instances \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Berikut ini adalah output contoh.

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
```

```
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

PowerShell

Untuk menjelaskan instance untuk Armada EC2 yang ditentukan

Gunakan Get-EC2FleetInstanceListcmdlet.

```
Get-EC2FleetInstanceList `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Jelaskan riwayat acara untuk Armada EC2 Anda

Untuk informasi lebih lanjut tentang peristiwa dalam sejarah acara, lihatJenis acara Armada EC2.

AWS CLI

Untuk menggambarkan peristiwa untuk Armada EC2 yang ditentukan

Gunakan perintah describe-fleet-history.

```
aws ec2 describe-fleet-history \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2020-06-01T00:00:00Z
```

Berikut ini adalah output contoh.

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
```

```
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2020-06-01T00:00:00.000Z"
}
```

PowerShell

Untuk menggambarkan peristiwa untuk Armada EC2 yang ditentukan

Gunakan Get-EC2FleetHistorycmdlet.

```
Get-EC2FleetHistory `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE `
    -UtcStartTime 2020-06-01T00:00:00Z
```

Memodifikasi Armada EC2

Anda dapat memodifikasi total kapasitas target, kapasitas Spot, dan kapasitas On-Demand dari Armada EC2. Anda juga dapat mengubah apakah instans yang sedang berjalan harus dihentikan jika total kapasitas target baru dikurangi di bawah ukuran armada saat ini.

Pertimbangan-pertimbangan

Pertimbangkan hal berikut saat memodifikasi Armada EC2:

- Jenis armada — Anda hanya dapat memodifikasi tipe `maintain` Armada EC2. Anda tidak dapat memodifikasi jenis Armada EC2 `request` atau`instant`.
- Parameter armada — Anda dapat memodifikasi parameter Armada EC2 berikut:
  - `target-capacity-specification`Meningkatkan atau mengurangi kapasitas target untuk:
    - `TotalTargetCapacity`
    - `OnDemandTargetCapacity`
    - `SpotTargetCapacity`
  - `excess-capacity-termination-policy` – Apakah instans yang sedang berjalan harus diakhiri jika total kapasitas target Armada EC2 turun di bawah ukuran armada saat ini. Nilai yang valid adalah:
    - `no-termination`
    - `termination`
- Perilaku armada saat meningkatkan kapasitas target total — Saat Anda meningkatkan kapasitas target total, Armada EC2 meluncurkan instans tambahan sesuai dengan opsi pembelian instans yang ditentukan`DefaultTargetCapacityType`, yaitu Instans Sesuai Permintaan atau Instans Spot, dan sesuai dengan strategi alokasi yang ditentukan.

- Perilaku armada saat mengurangi kapasitas target Spot — Saat Anda mengurangi kapasitas target Spot, Armada EC2 menghapus permintaan terbuka yang melebihi kapasitas target baru. Anda dapat meminta agar armada menghentikan Instans Spot hingga ukuran armada mencapai kapasitas target baru. Saat Armada EC2 mengakhiri Instans Spot karena kapasitas target berkurang, instans tersebut akan menerima pemberitahuan gangguan Instans Spot.

  Instans dipilih untuk penghentian berdasarkan strategi alokasi:

  - `capacity-optimized`— Mengakhiri instance dari kumpulan dengan kapasitas paling sedikit yang tersedia.
  - `price-capacity-optimized`— Menggunakan kombinasi harga dan kapasitas yang tersedia: menghentikan instance dari kolam dengan kapasitas paling sedikit yang tersedia dan yang merupakan harga tertinggi di antara kumpulan ini.
  - `diversified`— Mengakhiri instance di semua kumpulan.
  - `lowest-price`— Mengakhiri instance dari pool dengan harga tertinggi.

  Atau, Anda dapat meminta Armada EC2 menjaga armada pada ukuran saat ini, tetapi tidak mengganti Instans Spot yang terputus atau yang Anda hentikan secara manual.
- Status armada - Anda dapat memodifikasi Armada EC2 yang ada di `active` negara bagian `submitted` atau. Saat Anda memodifikasi armada, maka armada tersebut memasuki status `modifying`.

Perintah untuk memodifikasi Armada EC2

AWS CLI

Untuk memodifikasi total kapasitas target Armada EC2

Gunakan perintah modify-fleet.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Jika Anda mengurangi kapasitas target tetapi ingin menjaga armada pada ukuran saat ini, Anda dapat memodifikasi contoh sebelumnya sebagai berikut.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
```

```
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

PowerShell

Untuk memodifikasi total kapasitas target Armada EC2

Gunakan Edit-EC2Fleetcmdlet.

```
Edit-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacitySpecification_TotalTargetCapacity 20
```

Jika Anda mengurangi kapasitas target tetapi ingin menjaga armada pada ukuran saat ini, Anda dapat memodifikasi contoh sebelumnya sebagai berikut.

```
Edit-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacitySpecification_TotalTargetCapacity 20 `
    -ExcessCapacityTerminationPolicy "NoTermination"
```

Menghapus permintaan Armada EC2 dan instans di armada

Jika Anda tidak lagi memerlukan permintaan Armada EC2, Anda dapat menghapusnya. Setelah Anda menghapus permintaan armada, semua permintaan Spot yang terkait dengan armada dibatalkan, sehingga tidak ada Instans Spot baru yang diluncurkan.

Ketika Anda menghapus permintaan Armada EC2, Anda juga harus menentukan apakah Anda ingin menghentikan semua instance-nya. Instans tersebut mencakup Instans Sesuai Permintaan dan Instans Spot. Untuk `instant` armada, Armada EC2 harus menghentikan instans saat armada dihapus. Armada `instant` yang dihapus dengan instans yang sedang berjalan tidak didukung.

> **Warning**
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan.

Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Jika Anda menentukan bahwa instans harus dihentikan saat permintaan armada dihapus, permintaan armada memasuki negara bagian`deleted_terminating`. Jika tidak, armada masuk ke status `deleted_running` dan instans terus berjalan hingga diinterupsi atau Anda mengakhirinya secara manual.

Pembatasan

- Anda dapat menghapus hingga 25 armada tipe `instant` dalam satu operasi.
- Anda dapat menghapus hingga 100 armada tipe `maintain` atau `request` dalam satu operasi.
- Anda dapat menghapus hingga 125 armada dalam satu operasi, asalkan Anda tidak melebihi kuota untuk setiap jenis armada, seperti yang ditentukan di atas.
- Jika Anda melebihi jumlah armada yang ditentukan untuk dihapus, tidak ada armada yang dihapus.
- Armada `instant` yang dihapus dengan instans yang sedang berjalan tidak didukung. Saat Anda menghapus `instant` armada, Amazon EC2 secara otomatis menghentikan semua instansnya. Untuk `instant` armada dengan lebih dari 1000 instance, permintaan penghapusan mungkin gagal. Jika armada Anda memiliki lebih dari 1000 instans, pertama-tama hentikan sebagian besar instance secara manual, sisakan 1000 atau kurang. Kemudian hapus armada, dan instance yang tersisa akan dihentikan secara otomatis.

AWS CLI

Untuk menghapus permintaan Armada EC2 dan menghentikan instance-nya

Gunakan perintah hapus-armada dengan opsi. `--terminate-instances`

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Berikut ini adalah output contoh.

```
{
```

```
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Untuk menghapus permintaan Armada EC2 tanpa menghentikan instance-nya

Ubah contoh sebelumnya dengan menggunakan `--no-terminate-instances` opsi sebagai gantinya. Perhatikan bahwa `--no-terminate-instances` tidak didukung untuk `instant` armada.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Berikut ini adalah output contoh.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

PowerShell

Untuk menghapus permintaan Armada EC2 dan menghentikan instance-nya

Gunakan Remove-EC2Fleetcmdlet dengan parameter. `-TerminateInstance`

```
Remove-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $true
```

Untuk menghapus permintaan Armada EC2 tanpa menghentikan instance-nya

Ubah contoh sebelumnya dengan mengubah nilai `-TerminateInstance` parameter.

```
Remove-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $false
```

Memecahkan masalah saat armada gagal dihapus

Jika permintaan Armada EC2 gagal dihapus, `UnsuccessfulFleetDeletions` dalam output mengembalikan ID permintaan Armada EC2, kode kesalahan, dan pesan kesalahan.

Kode kesalahannya adalah:

- `ExceededInstantFleetNumForDeletion`
- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Pecahkan masalah **`ExceededInstantFleetNumForDeletion`**

Jika Anda mencoba menghapus lebih dari 25 armada `instant` dalam satu permintaan, kesalahan `ExceededInstantFleetNumForDeletion` akan dikembalikan. Berikut adalah contoh output untuk kesalahan ini.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                  "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                  "Code": "ExceededInstantFleetNumForDeletion"
           }
```

```
    },
    {
          "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
          "Error": {
                "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                "Code": "ExceededInstantFleetNumForDeletion"
           }
    }
    .
    .
    .
    ],
    "SuccessfulFleetDeletions": []
}
```

Pecahkan masalah **NoTerminateInstancesNotSupported**

Jika Anda menentukan bahwa instans dalam armada `instant` tidak boleh diakhiri saat menghapus armada, kesalahan `NoTerminateInstancesNotSupported` akan dikembalikan. `--no-terminate-instances` tidak didukung untuk armada `instant`. Berikut adalah contoh output untuk kesalahan ini.

```
{
      "UnsuccessfulFleetDeletions": [
            {
                "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                "Error": {
                      "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                      "Code": "NoTerminateInstancesNotSupported"
                 }
            }
       ],
       "SuccessfulFleetDeletions": []
}
```

Pecahkan masalah **UnauthorizedOperation**

Jika Anda tidak memiliki izin untuk mengakhiri instans, Anda akan mendapatkan kesalahan `UnauthorizedOperation` saat menghapus armada yang harus mengakhiri instansnya. Berikut ini adalah respons kesalahannya.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Untuk mengatasi kesalahan tersebut, Anda harus menambahkan tindakan `ec2:TerminateInstances` ke kebijakan IAM, seperti yang ditunjukkan pada contoh berikut.

Bekerja dengan Armada Spot

Untuk mulai menggunakan Armada Spot, buat permintaan yang mencakup total kapasitas target untuk Instans Spot, bagian Sesuai Permintaan opsional, dan tentukan AMI dan key pair secara manual, atau tentukan templat peluncuran yang menyertakan konfigurasi untuk instance di armada. Anda dapat menentukan parameter tambahan secara opsional, atau membiarkan armada menggunakan nilai default. Anda juga dapat menandai permintaan armada, serta instance dan volumenya, saat Anda membuat armada.

Armada meluncurkan Instans Sesuai Permintaan ketika ada kapasitas yang tersedia, dan meluncurkan Instans Spot ketika harga maksimum Anda melebihi harga Spot dan kapasitas yang tersedia.

Setelah armada Anda diluncurkan, Anda dapat menjelaskan permintaan armada, instance dalam armada, dan peristiwa armada apa pun. Anda juga dapat menetapkan tag tambahan sesuai kebutuhan.

Jika Anda perlu mengubah parameter armada apa pun, seperti total kapasitas target, Anda dapat memodifikasi armada, asalkan dikonfigurasi untuk mempertahankan kapasitas. Anda tidak dapat mengubah kapasitas permintaan satu kali setelah dikirimkan.

Permintaan armada tetap aktif sampai habis masa berlakunya atau Anda membatalkan (menghapusnya). Saat membatalkan permintaan armada, Anda dapat menghentikan instans

atau membiarkannya berjalan. Jika Anda memilih untuk membiarkannya berjalan, Instans Sesuai Permintaan berjalan hingga Anda menghentikannya, dan Instans Spot berjalan hingga terputus atau Anda menghentikannya.

Topik

- Status permintaan Armada Spot
- Izin Armada Spot
- Membuat Armada Spot
- Menandai permintaan Armada Spot baru atau yang sudah ada serta instance serta volume yang diluncurkan
- Jelaskan permintaan Armada Spot, instansinya, dan riwayat acara
- Memodifikasi permintaan Armada Spot
- Membatalkan (menghapus) permintaan Armada Spot
- Memahami penskalaan otomatis untuk Armada Spot

Status permintaan Armada Spot

Permintaan Armada Spot dapat berupa salah satu dari berbagai status, dengan setiap status menunjukkan tahapan siklus hidup permintaan yang berbeda dan pengelolaan instansnya.

Permintaan Armada Spot dapat berada dalam salah satu kondisi berikut:

`submitted`

Permintaan Armada Spot sedang dievaluasi dan Amazon EC2 sedang bersiap untuk meluncurkan jumlah target instans. Jika permintaan melebihi kuota Armada Spot Anda, permintaan tersebut akan segera dibatalkan.

`active`

Armada Spot telah divalidasi dan Amazon EC2 berusaha mempertahankan jumlah target Instans Spot yang sedang berjalan. Permintaan tetap dalam keadaan ini sampai dimodifikasi atau dibatalkan.

`modifying`

Permintaan Armada Spot sedang dimodifikasi. Permintaan tetap dalam keadaan ini sampai modifikasi diproses sepenuhnya atau permintaan dibatalkan. Hanya tipe armada `maintain` yang dapat dimodifikasi. Keadaan ini tidak berlaku untuk jenis `request` armada satu kali.

`cancelled_running`

Armada Spot dibatalkan (dihapus) dan tidak meluncurkan Instans Spot tambahan. Instans yang ada terus berjalan sampai diinterupsi atau diakhiri secara manual. Permintaan tetap berada dalam status ini sampai semua instans diinterupsi atau diakhiri.

`cancelled_terminating`

Armada Spot dibatalkan (dihapus) dan instance-instancenya dihentikan. Permintaan tetap berada dalam status ini sampai semua instans diakhiri.

`cancelled`

Armada Spot dibatalkan (dihapus) dan tidak memiliki instance yang berjalan. Permintaan tersebut dihapus dua hari setelah instansnya diakhiri.

Izin Armada Spot

Jika pengguna Anda akan membuat atau mengelola Armada Spot, Anda perlu memberinya izin yang diperlukan.

Jika Anda menggunakan konsol Amazon EC2 untuk membuat Armada Spot, konsol ini akan membuat dua peran tertaut layanan bernama `AWSServiceRoleForEC2SpotFleet` dan `AWSServiceRoleForEC2Spot`, serta peran bernama `aws-ec2-spot-fleet-tagging-role` yang memberikan izin kepada Armada Spot untuk meminta, meluncurkan, mengakhiri, dan menandai sumber daya atas nama Anda. Jika Anda menggunakan AWS CLI atau API, Anda harus memastikan bahwa peran ini ada.

Gunakan petunjuk berikut untuk memberikan izin yang diperlukan dan membuat peran.

Izin dan peran

- Memberikan izin kepada pengguna untuk Armada Spot
- Peran tertaut layanan untuk Armada Spot
- Peran terkait layanan untuk Instans Spot
- Peran IAM untuk menandai Armada Spot

Memberikan izin kepada pengguna untuk Armada Spot

Jika pengguna Anda akan membuat atau mengelola Armada Spot, pastikan untuk memberinya izin yang diperlukan.

Untuk membuat kebijakan Armada Spot

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan, Buat kebijakan.
3. Di halaman Buat kebijakan, pilih JSON, dan ganti teks dengan yang berikut ini.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh kebijakan sebelumnya memberikan izin yang diperlukan kepada pengguna untuk sebagian besar kasus penggunaan Armada Spot. Untuk membatasi pengguna ke tindakan API tertentu, tentukan hanya tindakan API tersebut saja.

Diperlukan EC2 dan IAM APIs

Berikut ini APIs harus dimasukkan dalam kebijakan:

- `ec2:RunInstances` – Diperlukan untuk meluncurkan instans di Armada Spot
- `ec2:CreateTags` – Diperlukan untuk menandai permintaan, instans, atau volume Armada Spot
- `iam:PassRole` – Diperlukan untuk menentukan peran Armada Spot
- `iam:CreateServiceLinkedRole` – Diperlukan untuk membuat peran tertaut-layanan
- `iam:ListRoles` – Diperlukan untuk melakukan enumerasi peran IAM yang ada
- `iam:ListInstanceProfiles` – Diperlukan untuk melakukan enumerasi profil instans yang sudah ada

> **Important**
>
> Jika Anda menentukan peran untuk profil instans IAM dalam spesifikasi peluncuran atau templat peluncuran, Anda harus memberikan izin kepada pengguna untuk meneruskan peran tersebut ke layanan. Untuk melakukan ini, dalam kebijakan IAM sertakan `"arn:aws:iam::*:role/IamInstanceProfile-role"` sebagai sumber daya untuk tindakan `iam:PassRole`. Untuk informasi selengkapnya, lihat Memberikan izin pengguna untuk meneruskan peran ke AWS layanan di Panduan Pengguna IAM.

Armada Spot APIs

Tambahkan tindakan Spot Fleet API berikut ke kebijakan Anda, jika diperlukan:

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`

- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

IAM opsional APIs

(Opsional) Untuk memungkinkan pengguna membuat peran atau profil instans menggunakan konsol IAM, Anda juga harus menambahkan tindakan berikut ke kebijakan:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Pilih Tinjau kebijakan.
5. Pada halaman Tinjau kebijakan, masukkan nama dan deskripsi kebijakan, dan pilih Buat kebijakan.
6. Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:
   - Pengguna dan grup di AWS IAM Identity Center:

     Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
   - Pengguna yang dikelola di IAM melalui penyedia identitas:

     Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.
   - Pengguna IAM:
     - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
     - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Peran tertaut layanan untuk Armada Spot

Amazon EC2 menggunakan peran tertaut layanan untuk izin yang diperlukan untuk memanggil layanan AWS lain atas nama Anda. Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke layanan. AWS Peran terkait layanan menyediakan cara aman untuk mendelegasikan izin ke AWS layanan karena hanya layanan tertaut yang dapat mengambil peran terkait layanan. Untuk informasi selengkapnya, lihat Peran terkait layanan di Panduan Pengguna IAM.

Amazon EC2 menggunakan peran terkait layanan bernamaAWSServiceRoleForEC2SpotFleet untuk meluncurkan dan mengelola instance atas nama Anda.

> **Important**
>
> Jika Anda menentukan AMI terenkripsi atau snapshot Amazon EBS terenkripsi di Armada Spot, Anda harus memberikan AWSServiceRoleForEC2SpotFleetizin peran untuk menggunakan CMK sehingga Amazon EC2 dapat meluncurkan instans atas nama Anda. Untuk informasi selengkapnya, lihat Berikan akses CMKs untuk digunakan dengan snapshot terenkripsi AMIs dan EBS.

Izin yang diberikan oleh AWSService RoleFor EC2 SpotFleet

AWSServiceRoleForEC2SpotFleetPeran tersebut memberikan izin kepada Armada Spot untuk meminta, meluncurkan, menghentikan, dan menandai instans atas nama Anda. Amazon EC2 menggunakan peran tertaut layanan ini untuk menyelesaikan tindakan berikut:

- `ec2:RequestSpotInstances` - Meminta Instans Spot
- `ec2:RunInstances` - Meluncurkan instans
- `ec2:TerminateInstances` - Mengakhiri instans
- `ec2:DescribeImages`- Jelaskan Amazon Machine Images (AMIs) untuk instance
- `ec2:DescribeInstanceStatus` - Mendeskripsikan status instans
- `ec2:DescribeSubnets` - Mendeskripsikan subnet untuk instans
- `ec2:CreateTags` - Menambahkan tanda ke permintaan, instans, dan volume Armada Spot
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - Menambahkan instans yang ditentukan ke penyeimbang beban yang ditentukan
- `elasticloadbalancing:RegisterTargets` - Mendaftarkan target yang ditentukan dengan grup target yang ditentukan

Membuat peran tertaut layanan

Dalam sebagian besar situasi, Anda tidak perlu membuat peran tertaut layanan secara manual. Amazon EC2 membuatAWSServiceRoleForEC2SpotFleet peran terkait layanan saat pertama kali Anda membuat Spot Fleet menggunakan konsol.

Jika Anda memiliki permintaan Armada Spot aktif sebelum Oktober 2017, saat Amazon EC2 mulai mendukung peran terkait layanan ini, Amazon EC2 membuat peran tersebut di akun Anda. AWSServiceRoleForEC2SpotFleet AWS Untuk informasi selengkapnya, lihat Peran baru muncul di AWS akun saya di Panduan Pengguna IAM.

Jika Anda menggunakan AWS CLI atau API untuk membuat Armada Spot, Anda harus terlebih dahulu memastikan bahwa peran ini ada.

Untuk membuat AWSService RoleFor EC2 SpotFleet peran untuk Armada Spot menggunakan konsol

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran.
3. Pilih Buat peran.
4. Pada halaman Pilih entitas tepercaya, lakukan hal berikut:
   a. Untuk jenis entitas Tepercaya, pilih AWS layanan.
   b. Di bawah Kasus penggunaan, untuk Layanan atau kasus penggunaan, pilih EC2.
   c. Untuk kasus Penggunaan, pilih EC2 - Armada Spot.

      > **Note**
      >
      > Kasus penggunaan EC2 - Spot Fleet akan secara otomatis membuat kebijakan dengan izin IAM yang diperlukan dan akan menyarankan AWSEC2SpotFleetServiceRolePolicysebagai nama peran.

   d. Pilih Berikutnya.
5. Pada halaman Tambahkan izin, pilih Berikutnya.
6. Pada halaman Nama, tinjau, dan buat, pilih Buat peran.

Untuk membuat AWSService RoleFor EC2 SpotFleet peran Armada Spot menggunakan AWS CLI

Gunakan perintah create-service-linked-role sebagai berikut.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Jika Anda tidak lagi perlu menggunakan Spot Fleet, kami sarankan Anda menghapus fileAWSServiceRoleForEC2SpotFleet wewenang. Setelah peran ini dihapus dari akun Anda, Amazon EC2 akan membuat peran lagi jika Anda meminta Armada Spot dengan menggunakan konsol. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Berikan akses CMKs untuk digunakan dengan snapshot terenkripsi AMIs dan EBS

Jika Anda menentukan AMI terenkripsi atau snapshot Amazon EBS terenkripsi dalam permintaan Armada Spot dan Anda menggunakan kunci terkelola pelanggan untuk enkripsi, Anda harus memberikan AWSServiceRoleForEC2SpotFleetizin peran untuk menggunakan CMK sehingga Amazon EC2 dapat meluncurkan instans atas nama Anda. Untuk melakukannya, Anda harus menambahkan pemberian izin ke CMK, seperti yang ditunjukkan dalam prosedur berikut.

Ketika memberikan izin, pemberian izin merupakan alternatif dari kebijakan kunci. Untuk informasi selengkapnya, lihat Menggunakan Pemberian Izin dan Menggunakan Kebijakan Kunci di AWS KMS dalam Panduan Developer AWS Key Management Service .

Untuk memberikan izin AWSService RoleFor EC2 SpotFleet peran untuk menggunakan CMK

- Gunakan perintah create-grant untuk menambahkan hibah ke CMK dan untuk menentukan kepala sekolah (peran terkait layanan AWSServiceRoleForEC2SpotFleet) yang diberi izin untuk melakukan operasi yang diizinkan oleh pemberian tersebut. CMK ditentukan oleh parameter `key-id` dan ARN CMK. Kepala sekolah ditentukan oleh`grantee-principal` parameter dan ARN dariAWSServiceRoleForEC2SpotFleet peran terkait layanan.

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
      --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
  spotfleet.amazonaws.com/AWSServiceRoleForEC2SpotFleet \
      --operations "Decrypt" "Encrypt" "GenerateDataKey"
   "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
   "ReEncryptTo"
  ```

Peran terkait layanan untuk Instans Spot

Amazon EC2 menggunakan peran terkait layanan bernama AWSServiceRoleForEC2Spot untuk meluncurkan dan mengelola Instans Spot atas nama Anda. Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk permintaan Instans Spot.

Peran IAM untuk menandai Armada Spot

Peran IAM `aws-ec2-spot-fleet-tagging-role` memberikan izin ke Armada Spot untuk menandai permintaan, instans, dan volume Armada Spot. Untuk informasi selengkapnya, lihat Menandai permintaan Armada Spot baru atau yang sudah ada serta instance serta volume yang diluncurkan.

> **Important**
>
> Jika Anda memilih untuk menandai instans di armada dan Anda juga memilih untuk mempertahankan kapasitas target (permintaan Armada Spot bertipe `maintain`), perbedaan izin yang ditetapkan untuk pengguna dan `IamFleetRole` dapat menyebabkan perilaku penandaan instans yang tidak konsisten di armada. Jika `IamFleetRole` tidak menyertakan izin `CreateTags`, beberapa instans yang diluncurkan oleh armada mungkin tidak akan ditandai. Sementara kami berusaha memperbaiki inkonsistensi ini, untuk memastikan bahwa semua instans yang diluncurkan oleh armada telah ditandai, kami menyarankan Anda menggunakan peran `aws-ec2-spot-fleet-tagging-role` untuk `IamFleetRole`. Atau, untuk menggunakan peran yang ada, lampirkan Kebijakan `AmazonEC2SpotFleetTaggingRole` AWS Terkelola ke peran yang ada. Jika tidak, Anda perlu menambahkan izin `CreateTags` secara manual untuk kebijakan yang ada.

Guna membuat peran IAM untuk menandai Armada Spot

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran.
3. Pilih Buat peran.
4. Pada halaman Pilih entitas tepercaya, di bawah Tipe entitas tepercaya, pilih Layanan AWS .
5. Di bawah Kasus penggunaan, dari Kasus penggunaan untuk layanan AWS lain, pilih EC2, lalu pilih EC2 - Penandaan Armada Spot.
6. Pilih Berikutnya.

7. Pada halaman Tambahkan izin, pilih Berikutnya.
8. Pada Nama, tinjau, dan buat, untuk Nama peran, masukkan nama untuk peran (misalnya, **`aws-ec2-spot-fleet-tagging-role`**).
9. Tinjau informasi di halaman tersebut, lalu pilih Buat peran.

Pencegahan confused deputy lintas layanan

Masalah confused deputy adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang lebih berhak untuk melakukan tindakan tersebut. Sebaiknya gunakan kunci konteks kondisi global `aws:SourceArn` dan `aws:SourceAccount` dalam kebijakan kepercayaan `aws-ec2-spot-fleet-tagging-role` untuk membatasi izin yang diberikan Armada Spot pada layanan lain ke sumber daya.

Untuk menambahkan kunci SourceAccount kondisi aws: SourceArn dan aws: ke kebijakan **`aws-ec2-spot-fleet-tagging-role`** kepercayaan

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran.
3. Temukan `aws-ec2-spot-fleet-tagging-role` yang Anda buat sebelumnya dan pilih tautan (bukan kotak centang).
4. Di bawah Ringkasan, pilih tab Hubungan kepercayaan, lalu pilih Edit kebijakan kepercayaan.
5. Dalam pernyataan JSON, tambahkan elemen `Condition` yang berisi kunci konteks kondisi global `aws:SourceAccount` dan `aws:SourceArn` untuk mencegah masalah confused deputy, sebagai berikut:

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/
sfr-*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
```

> **Note**
>
> Jika nilai `aws:SourceArn` berisi ID akun Anda dan Anda menggunakan kedua kunci konteks kondisi global tersebut, nilai `aws:SourceAccount` dan akun di nilai `aws:SourceArn` harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Kebijakan kepercayaan terakhir adalah sebagai berikut:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-
request/sfr-*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  }
}
```

6. Pilih Perbarui kebijakan.

Tabel berikut memberikan nilai potensial untuk `aws:SourceArn` guna membatasi ruang lingkup `aws-ec2-spot-fleet-tagging-role` Anda dalam berbagai tingkat kekhususan.

Operasi API	Layanan yang dipanggil	Lingkup	**aws:SourceArn**
RequestSpotFleet	AWS STS (AssumeRole)	Batasi AssumeRole aws-ec2-spot-fleet-tagging-role kemampuan spot-fleet-requests di akun yang ditentukan.	arn:aws:ec2:*: *123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Batasi AssumeRole aws-ec2-spot-fleet-tagging-role kemampuan spot-fleet-requests di akun yang ditentukan dan Wilayah yang ditentukan. Perhatikan bahwa peran ini tidak akan dapat digunakan di Wilayah lain.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Batasi kemampuan AssumeRole di aws-ec2-spot-fleet-tagging-role hanya pada tindakan yang memengaruhi armada sfr-11111111-1111-1111-1111-111111111111. Perhatikan bahwa peran ini mungkin tidak dapat digunakan untuk Armada Spot lainnya. Selain itu, peran ini	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*11111111-1111-1111-1111-111111111111*

Operasi API	Layanan yang dipanggil	Lingkup	**aws:SourceArn**
		tidak dapat digunakan untuk meluncurkan Armada Spot baru. request-spot-fleet	

Membuat Armada Spot

Dengan menggunakan Konsol Manajemen AWS, Anda dapat dengan cepat membuat permintaan Armada Spot dengan memilih hanya AMI dan total kapasitas target yang Anda inginkan. Amazon EC2 akan mengonfigurasi armada yang paling sesuai dengan kebutuhan Anda dan mengikuti praktik terbaik Spot. Atau, Anda dapat memodifikasi salah satu pengaturan default.

Jika ingin menyertakan Instans Sesuai Permintaan di armada, Anda harus menentukan templat peluncuran dalam permintaan dan menentukan kapasitas Sesuai Permintaan yang Anda inginkan.

Armada meluncurkan Instans Sesuai Permintaan saat kapasitas tersedia, dan meluncurkan Instans Spot ketika harga maksimum Anda melebihi harga Spot dan kapasitas yang tersedia.

Jika armada Anda menyertakan Instans Spot dan jenisnya`maintain`, Amazon EC2 akan berusaha mempertahankan kapasitas target armada Anda saat Instans Spot Anda terganggu.

Izin yang diperlukan

Untuk informasi selengkapnya, lihat the section called “Izin Armada Spot”.

Tugas

- Buat permintaan Armada Spot dengan cepat
- Membuat permintaan Armada Spot menggunakan parameter yang ditentukan
- Buat Armada Spot yang menggantikan Instans Spot yang tidak sehat

Buat permintaan Armada Spot dengan cepat

Ikuti langkah-langkah berikut untuk membuat permintaan Armada Spot dengan cepat menggunakan konsol Amazon EC2.

Untuk membuat permintaan Armada Spot menggunakan pengaturan yang disarankan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Jika Anda baru mengenal Spot, Anda akan melihat halaman sambutan; pilih Mulai. Jika tidak, pilih Buat Permintaan Armada Spot.
4. Di bawah Parameter peluncuran, pilih Konfigurasikan parameter peluncuran secara manual.
5. Untuk AMI, pilih AMI.
6. Di bawah Kapasitas target, untuk Total kapasitas target, tentukan jumlah unit yang akan diminta. Untuk jenis unit, Anda dapat memilih Instances, v CPUs, atau Memory (GiB).
7. Sekilas tentang permintaan armada Anda, tinjau konfigurasi armada Anda, dan pilih Luncurkan.

Membuat permintaan Armada Spot menggunakan parameter yang ditentukan

Anda dapat membuat Armada Spot menggunakan parameter yang Anda tentukan.

Console

Untuk membuat permintaan Armada Spot menggunakan parameter yang ditentukan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Jika Anda baru mengenal Spot, Anda akan melihat halaman sambutan; pilih Mulai. Jika tidak, pilih Buat Permintaan Armada Spot.
4. Untuk parameter Peluncuran, Anda dapat mengonfigurasi parameter peluncuran secara manual atau Anda dapat menggunakan templat peluncuran, sebagai berikut:

    a. [Konfigurasi secara manual] Untuk menentukan parameter peluncuran di konsol Amazon EC2, pilih Konfigurasi parameter peluncuran secara manual, lalu lakukan hal berikut:

        i. Untuk AMI, pilih salah satu dasar yang AMIs disediakan oleh AWS, atau pilih Cari AMI untuk menggunakan AMI dari komunitas pengguna kami, komunitas AWS Marketplace, atau salah satu komunitas Anda sendiri.

> **Note**
>
> Jika AMI yang ditentukan dalam parameter peluncuran dideregistrasi atau dinonaktifkan, tidak ada instance baru yang dapat diluncurkan dari AMI. Untuk armada yang diatur untuk mempertahankan kapasitas target, kapasitas target tidak akan dipertahankan.

ii. (Opsional) Untuk Nama pasangan kunci, pilih pasangan kunci yang ada atau buat yang baru.

[Pasangan kunci yang ada] Pilih pasangan kunci.

[New key pair] Pilih Create new key pair untuk membuka halaman Key pair. Setelah selesai, kembali ke halaman Permintaan Spot dan segarkan daftar.

iii. (Opsional) Perluas Parameter peluncuran tambahan, dan lakukan hal berikut:

A. (Opsional) Untuk mengaktifkan optimisasi Amazon EBS, untuk Dioptimalkan dengan EBS, pilih Luncurkan instans yang dioptimalkan EBS.

B. (Opsional) Guna menambahkan penyimpanan tingkat blok sementara untuk instans Anda, untuk Penyimpanan instans, pilih Lampirkan saat peluncuran.

C. (Opsional) Untuk menambahkan penyimpanan, pilih Tambahkan volume baru, dan tentukan volume penyimpanan instans tambahan atau volume Amazon EBS, tergantung pada tipe instans.

D. (Opsional) Secara default, pemantauan dasar diaktifkan untuk instans Anda. Untuk mengaktifkan pemantauan terperinci, untuk Pemantauan, pilih Aktifkan pemantauan CloudWatch terperinci.

E. (Opsional) Guna menjalankan Instans Spot Khusus, untuk Penghunian, pilih Khusus - jalankan instans khusus.

F. (Opsional) Untuk Grup keamanan, pilih satu atau beberapa grup keamanan atau buat yang baru.

[Grup keamanan yang ada] Pilih satu atau beberapa grup keamanan.

[Grup keamanan baru] Pilih Buat grup keamanan baru untuk membuka halaman Grup Keamanan. Setelah selesai, kembali ke Permintaan Spot dan segarkan daftar.

G. (Opsional) Agar instance Anda dapat dijangkau dari internet, untuk Penetapan otomatis IPv4 IP Publik , pilih Aktifkan .

H. (Opsional) Guna meluncurkan Instans Spot Anda dengan peran IAM, untuk Profil instans IAM, pilih peran tersebut.

I. (Opsional) Untuk menjalankan skrip start-up, salin skrip tersebut ke Data pengguna.

J. (Opsional) Untuk menambahkan tanda, pilih Buat tanda dan masukkan kunci serta nilai untuk tanda tersebut, lalu pilih Buat. Ulangi hal itu untuk setiap tanda.

Untuk setiap tanda, guna menandai instans dan permintaan Armada Spot dengan tanda yang sama, pastikan bahwa Instans serta Armada telah dipilih. Untuk menandai instans yang diluncurkan oleh armada saja, hapus Armada. Untuk menandai permintaan Armada Spot saja, hapus Instans.

b. [Template peluncuran] Untuk menggunakan konfigurasi yang Anda buat di template peluncuran, pilih Gunakan templat peluncuran, dan untuk Template peluncuran, pilih templat peluncuran.

> **Note**
>
> Jika Anda menginginkan kapasitas On-Demand di Armada Spot Anda, Anda harus menentukan template peluncuran.

5. Untuk detail permintaan tambahan, lakukan hal berikut:

a. Tinjau detail permintaan tambahan. Untuk membuat perubahan, hapus Terapkan default.

b. (Opsional) Untuk Peran armada IAM, Anda dapat menggunakan peran default atau memilih peran yang berbeda. Untuk menggunakan peran default setelah mengubah peran, pilih Gunakan peran default.

c. (Opsional) Untuk membuat permintaan yang hanya berlaku selama jangka waktu tertentu, edit Permintaan berlaku mulai dan Permintaan berlaku sampai.

d. (Opsional) Secara default, Amazon EC2 menghentikan Instans Spot Anda saat permintaan Armada Spot kedaluwarsa. Agar Instans Spot tetap berjalan setelah permintaan Anda berakhir, hapus Akhiri instans saat permintaan kedaluwarsa.

e. (Opsional) Untuk mendaftarkan Instans Spot Anda dengan penyeimbang beban, pilih Terima lalu lintas dari satu atau beberapa penyeimbang beban dan pilih satu atau beberapa Penyeimbang Beban Klasik atau grup target.

6. Untuk Kapasitas target, lakukan hal berikut:

   a. Di bawah Total kapasitas target, tentukan jumlah unit yang akan diminta. Untuk jenis unit, Anda dapat memilih Instances, v CPUs, atau Memory (MiB). Untuk menentukan kapasitas target 0 sehingga Anda dapat menambahkan kapasitas nanti, Anda harus terlebih dahulu memilih Pertahankan kapasitas target.

   b. (Opsional) Untuk Sertakan kapasitas basis Sesuai Permintaan, tentukan jumlah unit Sesuai Permintaan yang akan diminta. Jumlahnya harus kurang dari Total kapasitas target. Amazon EC2 menghitung selisihnya, dan mengalokasikan selisih tersebut ke unit Spot yang akan diminta.

      > **Important**
      >
      > Untuk menentukan kapasitas Sesuai Permintaan opsional, Anda harus terlebih dahulu memilih templat peluncuran.

   c. (Opsional) Secara default, Amazon EC2 menghentikan Instans Spot saat terputus. Untuk mempertahankan kapasitas target, pilih Pertahankan kapasitas target. Anda kemudian dapat menentukan bahwa Amazon EC2 mengakhiri, menghentikan, atau hibernasi Instans Spot saat terputus. Untuk melakukannya, pilih opsi yang sesuai dari Perilaku interupsi.

      > **Note**
      >
      > Jika AMI yang ditentukan dalam parameter peluncuran dideregistrasi atau dinonaktifkan, tidak ada instance baru yang dapat diluncurkan dari AMI. Dalam hal ini, untuk armada yang diatur untuk mempertahankan kapasitas target, kapasitas target tidak akan dipertahankan.

   d. (Opsional) Untuk mengizinkan Armada Spot meluncurkan Instans Spot pengganti saat notifikasi penyeimbangan ulang instans dikeluarkan untuk Instans Spot yang ada di armada, pilih Penyeimbangan ulang kapasitas, lalu pilih strategi penggantian instans. Jika Anda memilih Luncurkan sebelum mengakhiri, tentukan penundaan (dalam hitungan detik) sebelum Amazon EC2 menghentikan instans lama. Untuk informasi selengkapnya, lihat Gunakan Rebalancing Kapasitas di Armada EC2 dan Armada Spot untuk mengganti Instans Spot yang berisiko.

e. (Opsional) Untuk mengontrol jumlah yang Anda bayarkan per jam untuk semua Instans Spot di armada, pilih Atur biaya maksimum untuk Instans Spot, lalu masukkan jumlah total maksimum yang ingin Anda bayarkan per jam. Jika jumlah total maksimum tercapai, Armada Spot akan berhenti meluncurkan Instans Spot meskipun belum memenuhi kapasitas target. Untuk informasi selengkapnya, lihat Tetapkan batas pengeluaran untuk Armada EC2 atau Armada Spot.

7. Untuk Jaringan, lakukan hal berikut:

   a. Untuk Jaringan, pilih VPC yang ada atau buat yang baru.

      [VPC yang Ada] Pilih VPC.

      [VPC Baru] Pilih Buat VPC baru untuk membuka konsol Amazon VPC. Setelah selesai, kembali ke layar ini dan segarkan daftar.

   b. (Opsional) Untuk Availability Zone, izinkan Amazon EC2 memilih Availability Zone untuk Instans Spot Anda, atau tentukan satu atau beberapa Availability Zone.

      Jika Anda memiliki lebih dari satu subnet di Zona Ketersediaan, pilih subnet yang sesuai dari Subnet. Untuk menambahkan subnet, pilih Buat subnet baru untuk membuka konsol Amazon VPC. Setelah selesai, kembali ke layar ini dan segarkan daftar.

8. Untuk Persyaratan tipe instans, Anda dapat menentukan atribut instans dan membiarkan Amazon EC2 mengidentifikasi tipe instans optimal dengan atribut ini, atau Anda dapat menentukan daftar instans. Untuk informasi selengkapnya, lihat Tentukan atribut untuk pemilihan tipe contoh untuk Armada EC2 atau Armada Spot.

   a. Jika Anda memilih Tentukan atribut instans yang cocok dengan persyaratan komputasi Anda, tentukan atribut instans sebagai berikut:

      i. Untuk v CPUs, masukkan jumlah minimum dan maksimum yang diinginkan vCPUs. Untuk menentukan tidak ada batas, pilih Tidak ada minimum atau Tidak maksimum, atau keduanya.

      ii. Untuk Memori (GiB), masukkan jumlah memori minimum dan maksimum yang diinginkan. Untuk menentukan tidak ada batas, pilih Tidak ada minimum atau Tidak maksimum, atau keduanya.

      iii. (Opsional) Untuk atribut instance Tambahan, Anda dapat secara opsional menentukan satu atau beberapa atribut untuk mengekspresikan persyaratan komputasi Anda secara lebih rinci. Setiap atribut tambahan menambahkan batasan

lebih lanjut ke permintaan Anda. Anda dapat menghilangkan atribut tambahan; ketika dihilangkan, nilai default digunakan. Untuk deskripsi setiap atribut dan nilai defaultnya, lihat get-spot-placement-scores.

iv. (Opsional) Untuk menampilkan tipe instans dengan atribut tertentu, perluas Pratinjau tipe instans yang cocok. Untuk mengecualikan tipe instans agar tidak digunakan dalam permintaan Anda, pilih instans, lalu pilih Kecualikan tipe instans yang dipilih.

b. Jika Anda memilih Pilih tipe instans secara manual, Armada Spot menyediakan daftar default tipe instans. Untuk memilih tipe instans lainnya, pilih Tambahkan tipe instans, pilih tipe instans yang akan digunakan dalam permintaan Anda, dan pilih Pilih. Untuk menghapus tipe instans, pilih tipe instans dan pilih Hapus.

9. Untuk strategi Alokasi, pilih strategi alokasi Spot dan strategi alokasi On-Demand yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat Gunakan strategi alokasi untuk menentukan bagaimana Armada EC2 atau Armada Spot memenuhi kapasitas Spot dan Sesuai Permintaan.
10. Untuk Sekilas permintaan armada Anda, tinjau konfigurasi armada dan lakukan penyesuaian apa pun jika perlu.
11. (Opsional) Untuk mengunduh salinan konfigurasi peluncuran untuk digunakan dengan AWS CLI, pilih konfigurasi JSON.
12. Saat Anda siap meluncurkan Armada Spot, pilih Luncurkan.

    Tipe permintaan Armada Spot adalah `fleet`. Saat permintaan terpenuhi, permintaan tipe `instance` ditambahkan, di mana keadaannya `active` dan statusnya adalah `fulfilled`.

AWS CLI

Untuk membuat permintaan Armada Spot

Gunakan perintah request-spot-fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Untuk file konfigurasi contoh, lihat Contoh konfigurasi CLI Spot Fleet.

PowerShell

Untuk membuat permintaan Armada Spot

Gunakan Request-EC2SpotFleetcmdlet. Contoh berikut meluncurkan Instans Spot dalam armada yang dioptimalkan kapasitas.

```
Request-EC2SpotFleet `
    -SpotFleetRequestConfig_TargetCapacity 50 `
    -SpotFleetRequestConfig_AllocationStrategy "CapacityOptimized" `
    -SpotFleetRequestConfig_IamFleetRole "arn:aws:iam::123456789012:role/my-spot-fleet-role" `
    -SpotFleetRequestConfig_LaunchTemplateConfig @($launchConfig)
```

Tentukan konfigurasi peluncuran sebagai berikut, atur template peluncuran dan ganti properti yang Anda butuhkan. Untuk contoh konfigurasi, lihat Contoh konfigurasi CLI Spot Fleet.

```
$lcSpec = Amazon.EC2.Model.FleetLaunchTemplateSpecification
# To do - Set FleetLaunchTemplateSpecification properties
$lcOverrides = New-Object Amazon.EC2.Model.LaunchTemplateOverrides
# To do - Set LaunchTemplateOverrides properties
$launchConfig = New-Object Amazon.EC2.Model.LaunchTemplateConfig
$launchConfig.LaunchTemplateSpecification $lcSpec
$launchConfig.Overrides @($lcOverrides)
```

Buat Armada Spot yang menggantikan Instans Spot yang tidak sehat

Armada Spot memeriksa status kondisi Instans Spot di armada setiap dua menit. Status kondisi instans adalah `healthy` atau `unhealthy`.

Armada Spot menentukan status kondisi instans dengan menggunakan pemeriksaan status yang disediakan oleh Amazon EC2. Sebuah instans ditentukan sebagai `unhealthy` jika status pemeriksaan status instans atau pemeriksaan status sistemnya `impaired` dalam tiga kali pemeriksaan kondisi secara berturut–turut. Untuk informasi selengkapnya, lihat Pemeriksaan status untuk instans Amazon EC2.

Anda dapat mengonfigurasi armada untuk mengganti Instans Spot yang tidak sehat. Setelah mengaktifkan penggantian pemeriksaan kondisi, Instans Spot akan diganti jika dilaporkan sebagai `unhealthy`. Armada tersebut dapat berada di bawah kapasitas targetnya hingga beberapa menit saat Instans Spot yang tidak sehat sedang diganti.

Persyaratan

- Penggantian pemeriksaan kondisi hanya didukung untuk Armada Spot yang mempertahankan kapasitas target (armada tipe `maintain`), bukan untuk Armada Spot satu kali (armada tipe `request`).
- Penggantian pemeriksaan kondisi hanya didukung untuk Instans Spot. Fitur ini tidak didukung untuk Instans Sesuai Permintaan.
- Anda dapat mengonfigurasi Armada Spot Fleet untuk mengganti instans yang tidak sehat hanya saat Anda membuatnya.
- Pengguna dapat menggunakan penggantian pemeriksaan kondisi hanya jika memiliki izin untuk memanggil tindakan `ec2:DescribeInstanceStatus`.

Console

Mengkonfigurasi Armada Spot untuk menggantikan Instans Spot yang tidak sehat

1. Ikuti langkah-langkah untuk membuat Armada Spot diMembuat permintaan Armada Spot menggunakan parameter yang ditentukan.
2. Untuk mengonfigurasi armada untuk mengganti Instans Spot yang tidak sehat, perluas Parameter peluncuran tambahan, dan di bawah Pemeriksaan Kesehatan, pilih Ganti instans yang tidak sehat. Untuk mengaktifkan opsi ini, Anda harus memilih Pertahankan kapasitas target terlebih dahulu.

AWS CLI

Mengkonfigurasi Armada Spot untuk menggantikan Instans Spot yang tidak sehat

Gunakan request-spot-fleetperintah dengan `ReplaceUnhealthyInstances` propertiSpotFleetRequestConfig.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "TargetCapacity": 10,
        "ReplaceUnhealthyInstances": true
    }
```

```
}
```

PowerShell

Untuk mengonfigurasi permintaan Armada Spot untuk mengganti Instans Spot yang tidak sehat

Gunakan Request-EC2SpotFleetcmdlet dengan parameter. -SpotFleetRequestConfig_ReplaceUnhealthyInstance

```
-SpotFleetRequestConfig_ReplaceUnhealthyInstance $true
```

Menandai permintaan Armada Spot baru atau yang sudah ada serta instance serta volume yang diluncurkan

Untuk membantu mengkategorikan dan mengelola permintaan Armada Spot serta instans serta volume yang diluncurkan, Anda dapat menandainya dengan metadata khusus. Anda dapat menetapkan tanda untuk permintaan Armada Spot saat Anda membuatnya, atau setelahnya. Demikian pula, Anda dapat menetapkan tag ke instance dan volume saat diluncurkan oleh armada, atau sesudahnya.

Saat Anda menandai permintaan armada, instans dan volume yang diluncurkan oleh armada tidak ditandai secara otomatis. Anda perlu menandai instans dan volume yang diluncurkan oleh armada secara eksplisit. Anda dapat memilih untuk menetapkan tag hanya untuk permintaan armada, atau hanya instans yang diluncurkan oleh armada, atau hanya volume yang dilampirkan pada instans yang diluncurkan oleh armada, atau semuanya.

> **Note**
>
> Anda hanya dapat menandai volume yang dilampirkan ke Instans Sesuai Permintaan. Anda tidak dapat menandai volume yang dilampirkan ke Instans Spot.

Anda dapat menetapkan tanda menggunakan konsol Amazon EC2 atau alat baris perintah.

Untuk informasi selengkapnya tentang cara kerja tag, lihat Tandai sumber daya Amazon EC2 Anda.

Daftar Isi

- Prasyarat
- Menandai Armada Spot baru dan instans serta volume yang diluncurkannya
- Menandai Armada Spot yang ada
- Menampilkan tanda permintaan Armada Spot

Prasyarat

Berikan izin kepada pengguna untuk menandai sumber daya. Untuk informasi selengkapnya, lihat Contoh: Memberi tanda pada sumber daya.

Berikan izin kepada pengguna untuk menandai sumber daya

Buat kebijakan IAM yang mencakup berikut hal berikut:

- Tindakan `ec2:CreateTags`. Tindakan ini memberikan izin kepada pengguna untuk membuat tanda.
- Tindakan `ec2:RequestSpotFleet`. Tindakan ini memberikan izin kepada pengguna untuk membuat permintaan Armada Spot.
- Untuk `Resource`, Anda harus menentukan `"*"`. Tindakan ini memungkinkan pengguna untuk menandai semua tipe sumber daya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
}
```

Important

Saat ini kami tidak mendukung izin tingkat sumber daya untuk sumber daya `spot-fleet-request`. Jika Anda menentukan `spot-fleet-request` sebagai sumber daya, Anda akan mendapatkan pengecualian yang tidak sah saat mencoba menandai armada. Contoh berikut menggambarkan cara untuk tidak mengatur kebijakan.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Menandai Armada Spot baru dan instans serta volume yang diluncurkannya

Untuk menandai permintaan Spot Fleet baru serta instance serta volume yang diluncurkan menggunakan konsol

1. Ikuti prosedur Membuat permintaan Armada Spot menggunakan parameter yang ditentukan.
2. Cara Anda menambahkan tag tergantung pada apakah Anda mengonfigurasi armada secara manual atau menggunakan templat peluncuran.

   - Jika Anda mengonfigurasi armada secara manual, lakukan hal berikut:

     Untuk menambahkan tag, perluas Parameter peluncuran tambahan, pilih Buat tag, dan masukkan kunci dan nilai untuk tag. Ulangi hal itu untuk setiap tanda.

     Untuk setiap tanda, Anda dapat menandai permintaan Armada Spot dan instans dengan tanda yang sama. Untuk menandai keduanya, pastikan bahwa Instans dan Armada dipilih. Untuk menandai permintaan Armada Spot saja, hapus Instans. Untuk menandai instans yang diluncurkan oleh armada saja, hapus Armada.

     > **Note**
     >
     > Saat Anda mengonfigurasi armada secara manual, tidak ada opsi untuk menandai volume. Tanda volume hanya didukung untuk volume yang dilampirkan ke Instans Sesuai Permintaan. Saat mengonfigurasi armada secara manual, Anda tidak dapat menentukan Instans Sesuai Permintaan.

   - Jika Anda menggunakan template peluncuran, lakukan hal berikut:

     Untuk menambahkan tag ke permintaan armada, di bawah Tag, pilih Buat Tag, dan masukkan kunci dan nilai untuk tag. Ulangi hal itu untuk setiap tanda.

     Untuk menandai sumber daya di armada Anda, Anda harus menentukan tag di template peluncuran.

Untuk menandai permintaan Armada Spot baru dan instance serta volume yang diluncurkan menggunakan AWS CLI

Untuk menandai permintaan Armada Spot saat Anda membuatnya, dan untuk menandai instans serta volume ketika diluncurkan oleh armada, konfigurasikan konfigurasi permintaan Armada Spot sebagai berikut:

Tanda permintaan Armada Spot:

- Tentukan tanda untuk permintaan Armada Spot di `SpotFleetRequestConfig`.
- Untuk `ResourceType`, tentukan `spot-fleet-request`. Jika Anda menentukan nilai lain, permintaan armada akan gagal.
- Untuk `Tags`, tentukan pasangan nilai-kunci. Anda dapat menentukan lebih dari satu pasangan nilai-kunci.

Tanda instans:

- Tentukan tanda untuk instans di `LaunchSpecifications`.
- Untuk `ResourceType`, tentukan `instance`. Jika Anda menentukan nilai lain, permintaan armada akan gagal.
- Untuk `Tags`, tentukan pasangan nilai-kunci. Anda dapat menentukan lebih dari satu pasangan nilai-kunci.

  Atau, Anda dapat menentukan tanda untuk instans di templat peluncuran yang direferensikan dalam permintaan Armada Spot.

Tanda volume:

- Tentukan tanda untuk volume di templat peluncuran yang direferensikan dalam permintaan Armada Spot. Penandaan volume `LaunchSpecifications` tidak didukung.

Dalam contoh berikut, permintaan Armada Spot ditandai dengan dua tanda: Kunci=Lingkungan dan Nilai=Produksi, serta Kunci=Pusat-Biaya dan Nilai=123. Instans yang diluncurkan oleh armada ditandai dengan satu tanda (yang sama dengan salah satu tanda untuk permintaan Armada Spot): Kunci=Pusat-Biaya dan Nilai=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Untuk menandai instans yang diluncurkan oleh Armada Spot menggunakan AWS CLI

Untuk menandai instans ketika diluncurkan oleh armada, Anda dapat menentukan tanda di templat peluncuran yang direferensikan dalam permintaan Armada Spot, atau Anda dapat menentukan tanda dalam konfigurasi permintaan Armada Spot sebagai berikut:

- Tentukan tanda untuk instans di `LaunchSpecifications`.
- Untuk `ResourceType`, tentukan `instance`. Jika Anda menentukan nilai lain, permintaan armada akan gagal.
- Untuk `Tags`, tentukan pasangan nilai-kunci. Anda dapat menentukan lebih dari satu pasangan nilai-kunci.

Dalam contoh berikut, instans yang diluncurkan oleh armada ditandai dengan satu tanda: Kunci=Pusat-Biaya dan Nilai=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
```

```
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

Untuk menandai volume yang dilampirkan ke Instans Sesuai Permintaan yang diluncurkan oleh Armada Spot menggunakan AWS CLI

Untuk menandai volume saat dibuat oleh armada, Anda harus menentukan tanda di templat peluncuran yang direferensikan dalam permintaan Armada Spot.

> **Note**
>
> Tanda volume hanya didukung untuk volume yang dilampirkan ke Instans Sesuai Permintaan. Anda tidak dapat menandai volume yang dilampirkan ke Instans Spot. Penandaan volume `LaunchSpecifications` tidak didukung.

Menandai Armada Spot yang ada

Untuk menandai permintaan Armada Spot yang sudah ada menggunakan konsol

Setelah membuat permintaan Armada Spot, Anda dapat menambahkan tag ke permintaan armada menggunakan konsol.

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.
4. Pilih tab Tanda dan pilih Buat Tanda.

Untuk menandai permintaan Armada Spot yang ada menggunakan AWS CLI

Anda dapat menggunakan perintah create-tags untuk menandai sumber daya yang ada. Dalam contoh berikut, permintaan Armada Spot yang ada ditandai dengan Kunci=tujuan dan Nilai=uji.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
```

```
    --tags Key=purpose,Value=test
```

Menampilkan tanda permintaan Armada Spot

Untuk menampilkan tanda permintaan Armada Spot menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda dan pilih tab Tanda.

Untuk menjelaskan tanda permintaan Armada Spot

Gunakan perintah describe-tags untuk melihat tanda sumber daya yang ditentukan. Dalam contoh berikut, Anda menjelaskan tanda untuk permintaan Armada Spot yang ditentukan.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

Anda juga dapat menampilkan tanda permintaan Armada Spot dengan menjelaskan permintaan Armada Spot.

Gunakan describe-spot-fleet-requestsperintah untuk melihat konfigurasi permintaan Armada Spot yang ditentukan, yang mencakup tag apa pun yang ditentukan untuk permintaan armada.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```


```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
```

```
}
```

Jelaskan permintaan Armada Spot, instansinya, dan riwayat acara

Anda dapat menjelaskan konfigurasi Armada Spot, instans di Armada Spot, dan riwayat acara Armada Spot Anda.

Console

Untuk menggambarkan Armada Spot Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda. ID dimulai dengan sfr-. Untuk melihat detail konfigurasi, pilih Deskripsi.
4. Guna membuat daftar Instans Spot untuk Armada Spot, pilih Instans.
5. Untuk menampilkan riwayat Armada Spot, pilih Riwayat.

AWS CLI

Untuk menjelaskan permintaan Armada Spot Anda

Gunakan perintah describe-spot-fleet-requests.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Untuk menjelaskan instance yang sedang berjalan untuk permintaan Armada Spot yang ditentukan

Gunakan perintah describe-spot-fleet-instances.

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Untuk menjelaskan riwayat acara untuk permintaan Armada Spot yang ditentukan

Gunakan perintah describe-spot-fleet-request-history.

```
aws ec2 describe-spot-fleet-request-history \
```

```
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2024-05-18T00:00:00Z
```

PowerShell

Untuk menjelaskan permintaan Armada Spot Anda

Gunakan Get-EC2SpotFleetRequestcmdlet.

```
Get-EC2SpotFleetRequest
```

Untuk menjelaskan instance yang sedang berjalan untuk permintaan Armada Spot yang ditentukan

Gunakan Get-EC2SpotFleetInstancecmdlet.

```
Get-EC2SpotFleetInstance `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
```

Untuk menjelaskan riwayat acara untuk permintaan Armada Spot yang ditentukan

Gunakan Get-EC2SpotFleetRequestHistorycmdlet.

```
Get-EC2SpotFleetRequestHistory `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -UtcStartTime 2024-05-18T00:00:00Z
```

Memodifikasi permintaan Armada Spot

Anda dapat memodifikasi permintaan Armada Spot yang aktif untuk menyelesaikan tugas berikut:

- Meningkatkan total kapasitas target dan porsi On-Demand
- Mengurangi total kapasitas target dan porsi On-Demand

Saat Anda meningkatkan total kapasitas target, Armada Spot meluncurkan Instans Spot tambahan sesuai dengan strategi alokasi untuk permintaan Armada Spot. Saat Anda meningkatkan bagian Sesuai Permintaan, Armada Spot meluncurkan Instans Sesuai Permintaan tambahan.

Saat Anda mengurangi total kapasitas target, Armada Spot membatalkan permintaan terbuka yang melebihi kapasitas target baru. Anda dapat meminta agar Armada Spot mengakhiri Instans

Spot hingga ukuran armada mencapai kapasitas target yang baru. Jika strategi alokasinya adalah `diversified`, Armada Spot akan mengakhiri instans di seluruh kolam. Atau, Anda dapat meminta agar Armada Spot mempertahankan armada pada ukurannya saat ini, tetapi tidak mengganti Instans Spot apa pun yang terinterupsi atau yang Anda akhiri secara manual.

Pertimbangan-pertimbangan

- Anda tidak dapat memodifikasi permintaan Armada Spot satu kali. Anda hanya dapat memodifikasi permintaan Armada Spot jika memilih Pertahankan kapasitas target saat membuat permintaan Armada Spot.
- Ketika Armada Spot mengakhiri instans karena kapasitas target berkurang, instans tersebut akan menerima pemberitahuan interupsi Instans Spot.

Console

Untuk mengubah permintaan Armada Spot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.
4. Pilih Tindakan, Modifikasi kapasitas target.
5. Dalam Modifikasi kapasitas target, lakukan hal berikut:
   a. Masukkan kapasitas target baru dan bagian Sesuai Permintaan.
   b. (Opsional) Jika Anda menurunkan kapasitas target tetapi ingin mempertahankan armada pada ukurannya saat ini, hapus Akhiri instans.
   c. Pilih Kirim.

AWS CLI

Untuk mengubah permintaan Armada Spot

Gunakan modify-spot-fleet-requestperintah untuk memperbarui kapasitas target permintaan Armada Spot yang ditentukan.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
```

```
    --target-capacity 20
```

Anda dapat mengubah perintah sebelumnya sebagai berikut untuk mengurangi kapasitas target Armada Spot yang ditentukan tanpa mengakhiri Instans Spot sebagai akibatnya.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

PowerShell

Untuk mengubah permintaan Armada Spot

Gunakan Edit-EC2SpotFleetRequestcmdlet untuk memperbarui kapasitas target permintaan Armada Spot yang ditentukan.

```
Edit-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacity 20
```

Anda dapat mengubah perintah sebelumnya sebagai berikut untuk mengurangi kapasitas target Armada Spot yang ditentukan tanpa mengakhiri Instans Spot sebagai akibatnya.

```
Edit-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacity 20 `
    -ExcessCapacityTerminationPolicy "NoTermination"
```

Membatalkan (menghapus) permintaan Armada Spot

Jika Anda tidak lagi memerlukan Armada Spot, Anda dapat membatalkan permintaan Armada Spot, yang menghapus permintaan tersebut. Setelah Anda membatalkan permintaan armada, semua permintaan Spot yang terkait dengan armada juga dibatalkan, sehingga tidak ada Instans Spot baru yang diluncurkan.

Saat membatalkan permintaan Armada Spot, Anda juga harus menentukan apakah ingin mengakhiri semua instans. Instans tersebut mencakup Instans Sesuai Permintaan dan Instans Spot.

> **Warning**
>
> Mengakhiri sebuah instance bersifat permanen dan ireversibel.
> Setelah Anda menghentikan sebuah instance, Anda tidak dapat lagi terhubung dengannya, dan itu tidak dapat dipulihkan. Semua volume Amazon EBS terlampir yang dikonfigurasi untuk dihapus saat penghentian juga dihapus secara permanen dan tidak dapat dipulihkan. Semua data yang disimpan pada volume penyimpanan instance hilang secara permanen. Untuk informasi selengkapnya, lihat Cara kerja penghentian instance.
> Sebelum menghentikan instans, pastikan bahwa Anda telah mencadangkan semua data yang perlu disimpan setelah penghentian penyimpanan persisten.

Jika Anda menentukan bahwa instans harus diakhiri saat permintaan armada dibatalkan, permintaan armada akan memasuki status `cancelled_terminating`. Jika tidak, armada masuk ke status `cancelled_running` dan instans terus berjalan hingga diinterupsi atau Anda mengakhirinya secara manual.

Pembatasan

- Anda dapat membatalkan hingga 100 armada dalam satu permintaan. Jika Anda melebihi jumlah yang ditentukan, tidak ada armada yang dibatalkan.

Console

Untuk membatalkan (menghapus) permintaan Armada Spot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.
4. Pilih Tindakan, Batalkan permintaan.
5. Di kotak dialog Batalkan permintaan Spot, lakukan hal berikut:
   a. Untuk mengakhiri instans terkait pada saat yang sama dengan membatalkan permintaan Armada Spot, biarkan kotak centang Hentikan instans dipilih. Untuk membatalkan permintaan Armada Spot tanpa menghentikan instance terkait, kosongkan kotak centang Hentikan instans.
   b. Pilih Konfirmasi.

AWS CLI

Untuk membatalkan (menghapus) permintaan Armada Spot dan menghentikan instance-nya

Gunakan perintah cancel-spot-fleet-requests dengan opsi `--terminate-instances`.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Berikut ini adalah output contoh.

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Untuk membatalkan (menghapus) permintaan Armada Spot tanpa menghentikan instance-nya

Ubah contoh sebelumnya dengan menggunakan `--no-terminate-instances` opsi sebagai gantinya.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Berikut ini adalah output contoh.

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
```

```
    "UnsuccessfulFleetRequests": []
}
```

PowerShell

Untuk membatalkan (menghapus) permintaan Armada Spot dan menghentikan instance-nya

Gunakan Stop-EC2SpotFleetRequestcmdlet dengan parameter. `-TerminateInstance`

```
Stop-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $true
```

Untuk membatalkan (menghapus) permintaan Armada Spot tanpa menghentikan instance-nya

Ubah contoh sebelumnya dengan mengubah nilai `-TerminateInstance` parameter.

```
Stop-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $false
```

Memahami penskalaan otomatis untuk Armada Spot

Penskalaan otomatis memungkinkan Armada Spot Anda menambah atau mengurangi kapasitas targetnya berdasarkan permintaan. Dengan penskalaan otomatis, Armada Spot dapat meluncurkan instans (skala keluar) atau menghentikan instance (skala masuk) dalam rentang tertentu, sebagai respons terhadap satu atau beberapa kebijakan penskalaan.

Penskalaan otomatis untuk Armada Spot dimungkinkan oleh kombinasi API Amazon EC2, CloudWatch Amazon, dan Application Auto Scaling. Permintaan Armada Spot dibuat dengan Amazon EC2, alarm dibuat dengan CloudWatch, dan kebijakan penskalaan dibuat dengan Application Auto Scaling.

Jenis penskalaan otomatis

Armada Spot mendukung tipe penskalaan otomatis berikut:

- Penskalaan pelacakan target - Menambah atau mengurangi kapasitas armada saat ini dengan menargetkan nilai untuk metrik tertentu. Ini mirip dengan cara termostat Anda mempertahankan suhu rumah Anda—Anda memilih suhu yang diinginkan dan termostat melakukan sisanya.

- Penskalaan bertahap – Meningkatkan atau menurunkan kapasitas armada saat ini berdasarkan set penyesuaian penskalaan, yang disebut dengan penyesuaian langkah, yang bervariasi berdasarkan ukuran pelanggaran alarm.
- Penskalaan Terjadwal – Meningkatkan atau mengurangi kapasitas armada saat ini berdasarkan tanggal dan waktu.

Pertimbangan-pertimbangan

Saat menggunakan penskalaan otomatis untuk Armada Spot Anda, pertimbangkan hal berikut:

- Pembobotan instans — Jika Anda menggunakan pembobotan instans, ingatlah bahwa Armada Spot dapat melebihi kapasitas target sesuai kebutuhan. Kapasitas yang terpenuhi dapat berupa angka titik mengambang, tetapi kapasitas target harus berupa bilangan bulat, sehingga Armada Spot membulatkan ke bilangan bulat berikutnya. Anda harus mempertimbangkan perilaku ini jika Anda melihat hasil dari kebijakan penskalaan saat alarm dipicu. Sebagai contoh, misalkan kapasitas target adalah 30, kapasitas yang terpenuhi adalah 30,1, dan kebijakan penskalaan dikurangi 1. Apabila alarm dipicu, proses penskalaan otomatis akan mengurangi 1 dari 30,1 untuk mendapatkan 29,1, kemudian membulatkannya menjadi 30, sehingga tidak ada tindakan penskalaan yang dilakukan. Sebagai contoh lain, misalkan Anda memilih bobot instans 2, 4, dan 8, serta kapasitas target 10, tetapi tidak ada instans bobot 2 yang tersedia sehingga Armada Spot akan menyediakan instans bobot 4 dan 8 untuk kapasitas terpenuhi sebesar 12. Jika kebijakan penskalaan mengurangi kapasitas target sebesar 20% dan alarm dipicu, proses penskalaan otomatis akan mengurangi 12*0,2 dari 12 untuk mendapatkan 9,6, kemudian membulatkannya menjadi 10, sehingga tidak ada tindakan penskalaan yang dilakukan.
- Periode Cooldown — Kebijakan penskalaan yang Anda buat untuk Armada Spot mendukung periode cooldown. Periode ini adalah jumlah detik setelah aktivitas penskalaan selesai saat aktivitas penskalaan terkait pemicu sebelumnya dapat memengaruhi peristiwa penskalaan di masa mendatang. Untuk kebijakan penskalaan ke luar, selama periode pendinginan berlaku, kapasitas yang telah ditambahkan oleh peristiwa penskalaan ke luar sebelumnya yang memulai pendinginan dihitung sebagai bagian dari kapasitas yang diinginkan untuk penskalaan ke luar berikutnya. Tujuannya adalah untuk terus (tetapi tidak berlebihan) menskalakan ke luar. Untuk kebijakan penskalaan ke dalam, periode pendinginan digunakan untuk memblokir permintaan penskalaan ke dalam berikutnya hingga kedaluwarsa. Tujuannya adalah untuk menskalakan ke dalam secara konservatif guna melindungi ketersediaan aplikasi Anda. Namun, jika alarm lain memicu kebijakan penskalaan ke luar selama periode pendinginan setelah penskalaan ke dalam, penskalaan otomatis akan segera mengurangi target yang dapat diskalakan.

- Gunakan pemantauan terperinci — Kami menyarankan Anda menskalakan berdasarkan metrik instans dengan frekuensi 1 menit karena hal itu memastikan respons yang lebih cepat terhadap perubahan pemanfaatan. Penskalaan pada metrik dengan frekuensi 5 menit dapat menyebabkan waktu respons yang lebih lambat dan penskalaan pada data metrik yang sudah usang. Untuk mengirim data metrik untuk instance Anda CloudWatch dalam periode 1 menit, Anda harus secara khusus mengaktifkan pemantauan mendetail. Untuk informasi selengkapnya, lihat Mengelola pemantauan terperinci untuk instans EC2 Anda dan Membuat permintaan Armada Spot menggunakan parameter yang ditentukan.
- AWS CLI— Jika Anda menggunakan AWS CLI untuk mengonfigurasi penskalaan untuk Spot Fleet, Anda akan menggunakan perintah application-autoscaling.

Izin IAM diperlukan untuk penskalaan otomatis Armada Spot

Penskalaan otomatis untuk Armada Spot dimungkinkan oleh kombinasi API Amazon EC2, CloudWatch Amazon, dan Application Auto Scaling. Permintaan Armada Spot dibuat dengan Amazon EC2, alarm dibuat dengan CloudWatch, dan kebijakan penskalaan dibuat dengan Application Auto Scaling. Selain izin IAM yang diperlukan untuk menggunakan Spot Fleet dan Amazon EC2, pengguna yang mengakses pengaturan penskalaan armada harus memiliki izin yang sesuai untuk layanan yang mendukung penskalaan otomatis.

Untuk menggunakan penskalaan otomatis untuk Armada Spot, pengguna harus memiliki izin untuk menggunakan tindakan yang ditampilkan dalam kebijakan contoh berikut.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
```

```
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Anda juga dapat membuat kebijakan IAM Anda sendiri yang memungkinkan izin yang lebih mendetail untuk panggilan ke API Penskalaan Otomatis Aplikasi. Untuk informasi selengkapnya, lihat Identity and Access Management untuk Application Auto Scaling di Panduan Pengguna Application Auto Scaling.

Layanan Application Auto Scaling juga memerlukan izin untuk menjelaskan Armada Spot dan CloudWatch alarm Anda, dan izin untuk mengubah kapasitas target Armada Spot Anda atas nama Anda. Jika Anda mengaktifkan penskalaan otomatis untuk Armada Spot, fitur ini akan menciptakan peran tertaut layanan bernama `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Peran tertaut layanan ini memberikan izin Penskalaan Otomatis Aplikasi untuk mendeskripsikan alarm bagi kebijakan Anda, memantau kapasitas armada saat ini, dan memodifikasi kapasitas armada. Peran Armada Spot terkelola asli untuk Penskalaan Otomatis Aplikasi adalah`aws-ec2-spot-fleet-autoscale-role`, tetapi tidak lagi diperlukan. Peran tertaut layanan adalah peran default untuk Penskalaan Otomatis Aplikasi. Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk Application Auto Scaling dalam Panduan Pengguna Application Auto Scaling.

Penskalaan pelacakan target: Skala Armada Spot dengan menargetkan nilai untuk metrik tertentu

Dengan penskalaan pelacakan target, Anda membuat kebijakan penskalaan pelacakan target dengan memilih metrik dan menetapkan nilai target. Spot Fleet kemudian membuat dan mengelola CloudWatch alarm yang memicu kebijakan penskalaan, dan menghitung penyesuaian penskalaan berdasarkan metrik dan nilai target yang dipilih. Kebijakan penskalaan menyesuaikan kapasitas

dengan menambahkan atau menghapus instance sesuai kebutuhan untuk menjaga metrik pada, atau mendekati, nilai target yang ditentukan. Kebijakan pelacakan target tidak hanya menjaga metrik mendekati nilai target, tetapi juga menyesuaikan dengan fluktuasi metrik karena pola beban yang berfluktuasi dan meminimalkan fluktuasi kapasitas yang cepat.

Anda dapat membuat beberapa kebijakan penskalaan pelacakan target untuk Armada Spot, asalkan setiap kebijakan menggunakan metrik yang berbeda. Skala armada berdasarkan kebijakan yang menentukan kapasitas armada terbesar. Ini memungkinkan Anda untuk mencakup beberapa skenario untuk memastikan kapasitas yang cukup untuk beban kerja aplikasi Anda.

Untuk memastikan ketersediaan aplikasi, armada menskalakan ke luar secara proporsional dengan metrik secepat mungkin, tetapi menskalakan ke dalam secara lebih bertahap.

Ketika Armada Spot menghentikan Instans Spot karena kapasitas target berkurang, instans menerima pemberitahuan interupsi Instans Spot.

> **Note**
>
> Jangan mengedit atau menghapus CloudWatch alarm yang dikelola Spot Fleet untuk kebijakan penskalaan pelacakan target. Armada Spot menghapus alarm secara otomatis saat Anda menghapus kebijakan penskalaan pelacakan target.

Prasyarat

- Permintaan Armada Spot harus memiliki permintaan tipe `maintain`. Penskalaan otomatis tidak didukung untuk permintaan tipe `request`.
- KonfigurasikanIzin IAM diperlukan untuk penskalaan otomatis Armada Spot.
- TinjauPertimbangan-pertimbangan.

Untuk mengonfigurasi kebijakan pelacakan target

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.
4. Pilih tab Auto Scaling di dekat bagian bawah layar. Jika Anda memilih tautan untuk Armada Spot Anda, tidak ada tab; sebagai gantinya, gulir ke bawah ke bagian Auto Scaling.

5. Jika penskalaan otomatis tidak dikonfigurasi, pilih Konfigurasikan.
6. Gunakan Skalakan kapasitas antara guna mengatur kapasitas minimum dan maksimum untuk armada Anda. Penskalaan otomatis tidak menskalakan armada Anda di bawah kapasitas minimum atau di atas kapasitas maksimum.
7. Untuk Nama kebijakan, masukkan nama untuk kebijakan tersebut.
8. Pilih Metrik target.
9. Masukkan Nilai target untuk metrik.
10. Untuk Periode pendinginan, tentukan nilai baru (dalam detik) atau simpan default.
11. (Opsional) Untuk menghilangkan pembuatan kebijakan penskalaan berdasarkan konfigurasi saat ini, pilih Nonaktifkan penskalaan. Anda dapat membuat kebijakan penskalaan ke dalam menggunakan konfigurasi yang berbeda.
12. Pilih Simpan.

Untuk mengonfigurasi kebijakan pelacakan target menggunakan AWS CLI

1. Daftarkan permintaan Spot Fleet sebagai target yang dapat diskalakan menggunakan register-scalable-targetperintah.
2. Buat kebijakan penskalaan menggunakan put-scaling-policyperintah.

Penskalaan langkah: Scale Spot Fleet menggunakan kebijakan penskalaan langkah

Dengan kebijakan penskalaan langkah, Anda menentukan CloudWatch alarm untuk memicu proses penskalaan. Misalnya, jika Anda ingin melakukan penskalaan ke luar saat pemanfaatan CPU mencapai tingkat tertentu, buat alarm menggunakan metrik `CPUUtilization` yang disediakan oleh Amazon EC2.

Saat membuat kebijakan penskalaan bertahap, Anda harus menentukan salah satu dari tipe penyesuaian penskalaan berikut:

- Tambah – Meningkatkan kapasitas target armada dengan jumlah unit kapasitas tertentu atau persentase tertentu dari kapasitas saat ini.
- Hapus – Mengurangi kapasitas target armada dengan jumlah unit kapasitas tertentu atau persentase tertentu dari kapasitas saat ini.
- Atur ke – Mengatur kapasitas target armada ke jumlah unit kapasitas yang ditentukan.

Saat alarm dipicu, proses penskalaan otomatis akan menghitung kapasitas target baru menggunakan kapasitas yang terpenuhi dan kebijakan penskalaan, lalu memperbarui kapasitas target yang sesuai. Sebagai contoh, misalkan kapasitas target dan kapasitas yang terpenuhi adalah 10 serta kebijakan penskalaan menambahkan 1. Saat alarm dipicu, proses penskalaan otomatis akan menambahkan 1 hingga 10 untuk mendapatkan 11, jadi Armada Spot meluncurkan 1 instans.

Ketika Armada Spot menghentikan Instans Spot karena kapasitas target berkurang, instans menerima pemberitahuan interupsi Instans Spot.

Prasyarat

- Permintaan Armada Spot harus memiliki permintaan tipe `maintain`. Penskalaan otomatis tidak didukung untuk permintaan tipe `request`.
- KonfigurasikanIzin IAM diperlukan untuk penskalaan otomatis Armada Spot.
- Pertimbangkan CloudWatch metrik mana yang penting untuk aplikasi Anda. Anda dapat membuat CloudWatch alarm berdasarkan metrik yang disediakan oleh AWS atau metrik kustom Anda sendiri.
- Untuk AWS metrik yang akan Anda gunakan dalam kebijakan penskalaan, aktifkan pengumpulan CloudWatch metrik jika layanan yang menyediakan metrik tidak mengaktifkannya secara default.
- TinjauPertimbangan-pertimbangan.

Untuk membuat CloudWatch alarm

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, perluas Alarm dan pilih Semua alarm.
3. Pilih Buat alarm.
4. Di halaman Tentukan metrik dan kondisi, pilih Pilih metrik.
5. Pilih EC2 Spot, lalu Metrik Permintaan Armada, lalu pilih metrik (misalnya, TargetCapacity), lalu pilih Pilih metrik.

   Halaman Tentukan metrik dan kondisi ditampilkan, yang menunjukkan grafik dan informasi lain tentang metrik yang Anda pilih.
6. Untuk Periode, pilih periode evaluasi untuk alarm, misalnya, 1 menit. Saat Anda mengevaluasi alarm, tiap periode akan digabungkan menjadi satu titik data.

> **Note**
>
> Periode yang lebih pendek menghasilkan alarm yang lebih sensitif.

7. Untuk Kondisi, tentukan alarm dengan menentukan kondisi ambang batas. Misalnya, Anda dapat menentukan ambang batas untuk memicu alarm setiap kali nilai metrik lebih besar dari atau sama dengan 80 persen.
8. Di Konfigurasi tambahan, untuk Titik data ke alarm, tentukan banyaknya titik data (periode evaluasi) yang harus berada dalam status ALARM untuk memicu alarm, misalnya, 1 periode evaluasi atau 2 dari 3 periode evaluasi. Hal tersebut membuat alarm yang masuk ke status ALARM jika terjadi pelanggaran sebanyak itu secara berturut-turut. Untuk informasi selengkapnya, lihat Mengevaluasi alarm di Panduan CloudWatch Pengguna Amazon.
9. Untuk Penanganan data hilang, pilih salah satu opsi (atau biarkan default Perlakukan data yang hilang sebagai hilang). Untuk informasi selengkapnya, lihat Mengonfigurasi cara CloudWatch alarm menangani data yang hilang di CloudWatch Panduan Pengguna Amazon.
10. Pilih Berikutnya.
11. (Opsional) Agar menerima notifikasi peristiwa penskalaan, untuk Notifikasi, Anda dapat memilih atau membuat topik Amazon SNS yang ingin Anda gunakan untuk menerima notifikasi. Jika tidak, Anda dapat menghapus notifikasi sekarang dan menambahkannya nanti sesuai kebutuhan.
12. Pilih Berikutnya.
13. Di bawah Tambahkan nama dan deskripsi, masukkan nama dan deskripsi untuk alarm dan pilih Berikutnya.
14. Pilih Buat alarm.

Untuk mengonfigurasi kebijakan penskalaan langkah untuk Armada Spot Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.
4. Pilih tab Auto Scaling di dekat bagian bawah layar. Jika Anda memilih tautan untuk Armada Spot Anda, tidak ada tab; sebagai gantinya, gulir ke bawah ke bagian Auto Scaling.
5. Jika penskalaan otomatis tidak dikonfigurasi, pilih Konfigurasikan.

6. Gunakan Skalakan kapasitas antara guna mengatur kapasitas minimum dan maksimum untuk armada Anda. Kebijakan penskalaan tidak menskalakan armada Anda di bawah atau di atas kapasitas maksimum.
7. Di bawah Kebijakan penskalaan, untuk jenis kebijakan, pilih Kebijakan penskalaan langkah.
8. Awalnya, Kebijakan penskalaan berisi kebijakan penskalaan langkah yang bernama ScaleUp dan ScaleDown. Anda dapat melengkapi kebijakan ini, atau memilih Hapus kebijakan untuk menghapusnya. Anda juga dapat memilih Tambahkan kebijakan.
9. Untuk menentukan kebijakan, lakukan hal berikut:

    a. Untuk Nama kebijakan, masukkan nama untuk kebijakan tersebut.

    b. Untuk pemicu Kebijakan, pilih alarm yang ada, atau pilih Buat alarm untuk membuka CloudWatch konsol Amazon dan membuat alarm.

    c. Untuk Modifikasi kapasitas, tentukan jumlah yang akan diskalakan serta batas bawah dan atas dari penyesuaian langkah. Anda dapat menambahkan atau menghapus sejumlah instans tertentu atau persentase ukuran armada yang ada, atau mengatur armada ke ukuran yang tepat.

    Misalnya, untuk membuat kebijakan penskalaan langkah yang meningkatkan kapasitas armada sebesar 30 persen, pilih Tambah, masukkan 30 di bidang berikutnya, lalu pilih persen. Secara default, batas bawah untuk kebijakan penambahan adalah ambang batas alarm, sedangkan batas atas adalah positif (+) tak terbatas. Secara default, batas atas untuk kebijakan penghapusan adalah ambang batas alarm, sedangkan batas bawah adalah negatif (-) tak terbatas.

    d. (Opsional) untuk menambahkan langkah lain, pilih Tambahkan langkah.

    e. Untuk Periode pendinginan, tentukan nilai baru (dalam detik) atau simpan default.
10. Pilih Simpan.

Untuk mengonfigurasi kebijakan penskalaan langkah untuk Armada Spot Anda menggunakan AWS CLI

1. Daftarkan permintaan Spot Fleet sebagai target yang dapat diskalakan menggunakan register-scalable-targetperintah.
2. Buat kebijakan penskalaan menggunakan put-scaling-policyperintah.
3. Buat alarm yang memicu kebijakan penskalaan menggunakan perintah. put-metric-alarm

Penskalaan terjadwal: Scale Spot Fleet sesuai jadwal

Menskalakan armada sesuai jadwal memungkinkan Anda menskalakan aplikasi sebagai respons terhadap perubahan permintaan yang dapat diprediksi. Dengan membuat tindakan terjadwal, Anda dapat menginstruksikan Armada Spot untuk melakukan aktivitas penskalaan pada waktu tertentu. Untuk membuat tindakan terjadwal, Anda harus menentukan Armada Spot yang ada, waktu kapan aktivitas penskalaan harus terjadi, dan kapasitas minimum dan maksimum yang diinginkan. Tindakan terjadwal dapat dikonfigurasi untuk skala sekali atau pada jadwal berulang. Jika perlu diubah, Anda dapat mengedit atau menghapus tindakan terjadwal.

Prasyarat

- Tindakan terjadwal hanya dapat dibuat untuk Armada Spot yang ada. Anda tidak dapat membuat tindakan terjadwal saat membuat Armada Spot.
- Permintaan Armada Spot harus memiliki permintaan tipe `maintain`. Penskalaan otomatis tidak didukung untuk permintaan tipe `request`.
- KonfigurasikanIzin IAM diperlukan untuk penskalaan otomatis Armada Spot.
- TinjauPertimbangan-pertimbangan.

Untuk membuat tindakan terjadwal satu kali

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.
4. Pilih tab Penskalaan Terjadwal di dekat bagian bawah layar. Jika Anda memilih tautan untuk Armada Spot Anda, tidak ada tab; sebagai gantinya, gulir ke bawah ke bagian Penskalaan Terjadwal.
5. Pilih Buat tindakan terjadwal.
6. Untuk Nama, tentukan nama untuk tindakan terjadwal.
7. Masukkan nilai untuk Kapasitas minimum, Kapasitas maksimum, atau keduanya.
8. Untuk Perulangan, pilih Sekali.
9. (Opsional) Pilih tanggal dan waktu untuk Waktu mulai, Waktu berakhir, atau keduanya.
10. Pilih Buat.

Untuk membuat tindakan terjadwal berulang

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.
4. Pilih tab Penskalaan Terjadwal di dekat bagian bawah layar. Jika Anda memilih tautan untuk Armada Spot Anda, tidak ada tab; sebagai gantinya, gulir ke bawah ke bagian Penskalaan Terjadwal.
5. Untuk Nama, tentukan nama untuk tindakan terjadwal.
6. Masukkan nilai untuk Kapasitas minimum, Kapasitas maksimum, atau keduanya.
7. Untuk Perulangan, pilih salah satu jadwal yang telah ditentukan sebelumnya (misalnya, Setiap hari), atau pilih Kustom dan masukkan ekspresi cron. Untuk informasi selengkapnya tentang ekspresi cron yang didukung oleh penskalaan terjadwal, lihat Ekspresi cron di Panduan Pengguna Amazon EventBridge .
8. (Opsional) Pilih tanggal dan waktu untuk Waktu mulai, Waktu berakhir, atau keduanya.
9. Pilih Kirim.

Untuk mengedit tindakan terjadwal

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.
4. Pilih tab Penskalaan Terjadwal di dekat bagian bawah layar. Jika Anda memilih tautan untuk Armada Spot Anda, tidak ada tab; sebagai gantinya, gulir ke bawah ke bagian Penskalaan Terjadwal.
5. Pilih tindakan terjadwal dan pilih Tindakan, Edit.
6. Lakukan perubahan yang diperlukan dan pilih Kirim.

Untuk menghapus tindakan terjadwal

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Permintaan Spot.
3. Pilih permintaan Armada Spot Anda.

4. Pilih tab Penskalaan Terjadwal di dekat bagian bawah layar. Jika Anda memilih tautan untuk Armada Spot Anda, tidak ada tab; sebagai gantinya, gulir ke bawah ke bagian Penskalaan Terjadwal.
5. Pilih tindakan terjadwal dan pilih Tindakan, Hapus.
6. Saat diminta konfirmasi, pilih Hapus.

Untuk mengelola penskalaan terjadwal menggunakan AWS CLI

Gunakan salah satu perintah berikut ini:

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Pantau Armada EC2 atau Armada Spot

Pemantauan yang efektif terhadap Armada EC2 atau Armada Spot Anda sangat penting untuk menjaga kinerja optimal dan memastikan keandalan. Ada berbagai alat untuk membantu Anda mencapai ini, termasuk Amazon CloudWatch dan Amazon EventBridge, yang dibahas dalam topik ini.

Dengan CloudWatch, Anda dapat mengumpulkan dan melacak metrik, mengatur alarm, dan secara otomatis bereaksi terhadap perubahan status armada Anda.

Dengan EventBridge, Anda dapat memantau dan merespons secara terprogram peristiwa yang dipancarkan oleh armada Anda. Dengan menetapkan aturan di EventBridge, Anda dapat mengotomatiskan respons terhadap peristiwa armada tertentu, seperti penghentian instans atau perubahan status armada, meningkatkan efisiensi operasional Anda.

Topik

- Pantau Armada EC2 atau Armada Spot Anda menggunakan CloudWatch
- Memantau dan merespons secara terprogram peristiwa yang dipancarkan oleh Armada EC2 atau Armada Spot Anda menggunakan Amazon EventBridge

Pantau Armada EC2 atau Armada Spot Anda menggunakan CloudWatch

Anda dapat memantau Armada EC2 atau Armada Spot menggunakan CloudWatch metrik Amazon yang dijelaskan di bagian ini.

> **Important**
>
> Untuk memastikan keakuratannya, sebaiknya Anda mengaktifkan pemantauan mendetail saat menggunakan metrik ini. Untuk informasi selengkapnya, lihat Mengelola pemantauan terperinci untuk instans EC2 Anda.

Untuk informasi selengkapnya tentang penggunaan CloudWatch, lihatPantau instans Anda menggunakan CloudWatch.

Metrik Armada EC2 dan Armada Spot

`AWS/EC2Spot`Namespace mencakup metrik berikut untuk armada Anda, ditambah metrik untuk Instans Spot di armada Anda. CloudWatch Untuk informasi selengkapnya, lihat Metrik instans.

Metrik	Deskripsi
`AvailableInstancePoolsCount`	Kumpulan kapasitas Spot yang ditentukan dalam permintaan armada. Unit: Hitungan
`BidsSubmittedForCapacity`	Kapasitas Amazon EC2 telah mengajukan permintaan armada. Unit: Hitungan
`EligibleInstancePoolCount`	Kumpulan kapasitas Spot yang ditentukan dalam permintaan armada tempat Amazon EC2 dapat memenuhi permintaan. Amazon EC2 tidak memenuhi permintaan di kolam tempat harga maksimum yang bersedia Anda bayarkan untuk Instans Spot kurang dari harga Spot atau harga Spot lebih tinggi dari harga Instans Sesuai Permintaan.

Metrik	Deskripsi
	Unit: Jumlah
FulfilledCapacity	Kapasitas yang telah dipenuhi oleh Amazon EC2. Unit: Hitungan
MaxPercentCapacityAllocation	Nilai maksimum PercentCapacityAllocation di semua kumpulan armada yang ditentukan dalam permintaan armada. Unit: Persen
PendingCapacity	Perbedaan antara TargetCapacity dan FulfilledCapacity . Unit: Jumlah
PercentCapacityAllocation	Kapasitas yang dialokasikan untuk kolam kapasitas Spot untuk dimensi tertentu. Agar nilai maksimum dapat tercatat di semua kolam kapasitas Spot, gunakan MaxPercentCapacityAllocation . Unit: Persen
TargetCapacity	Kapasitas target permintaan armada. Unit: Hitungan
TerminatingCapacity	Kapasitas yang sedang diakhiri karena kapasitas yang disediakan lebih besar dari kapasitas target. Unit: Jumlah

Jika unit ukuran untuk metrik adalah Count, statistik yang paling berguna adalah Average.

Dimensi Armada EC2 dan Armada Spot

Untuk memfilter data armada Anda, gunakan dimensi berikut.

Dimensi	Deskripsi
`AvailabilityZone`	Filter data berdasarkan Zona Ketersediaan.
`FleetRequestId`	Filter data berdasarkan permintaan armada.
`InstanceType`	Filter data menurut tipe instans.

Lihat CloudWatch metrik untuk Armada EC2 atau Armada Spot

Anda dapat melihat CloudWatch metrik untuk armada Anda menggunakan CloudWatch konsol Amazon. Metrik ini ditampilkan sebagai grafik pemantauan. Grafik ini menunjukkan titik data jika armada aktif.

Metrik dikelompokkan terlebih dahulu berdasarkan namespace, kemudian berdasarkan berbagai kombinasi dimensi di dalam setiap namespace. Misalnya, Anda dapat melihat semua metrik armada atau grup metrik armada berdasarkan ID permintaan armada, jenis instans, atau Availability Zone.

Untuk melihat metrik armada

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, perluas Metrik, dan pilih Semua metrik.
3. Pilih namespace Spot EC2.

> **Note**
>
> Jika namespace Spot EC2 tidak ditampilkan, ada dua alasan untuk ini. Entah Anda belum pernah menggunakan Armada EC2 atau Armada Spot di Region—hanya AWS layanan yang Anda gunakan mengirim metrik ke Amazon. CloudWatch Atau, jika Anda telah menggunakan Armada EC2 atau Armada Spot di Wilayah, tetapi tidak selama dua minggu terakhir, namespace tidak muncul.

4. Untuk memfilter metrik berdasarkan dimensi, pilih salah satu dari berikut ini:
   - Metrik Permintaan Armada — Kelompokkan berdasarkan permintaan armada
   - Berdasarkan Availability Zone — Kelompokkan berdasarkan permintaan armada dan Availability Zone

- Berdasarkan Jenis Instance - Kelompokkan berdasarkan permintaan armada dan jenis instans
- Berdasarkan Zone/Instance Jenis Ketersediaan — Kelompokkan berdasarkan permintaan armada, Availability Zone, dan tipe instans

5. Untuk melihat data untuk metrik, pilih kotak centang di sebelah metrik.

Memantau dan merespons secara terprogram peristiwa yang dipancarkan oleh Armada EC2 atau Armada Spot Anda menggunakan Amazon EventBridge

Ketika status Armada EC2 atau Armada Spot berubah, ia mengeluarkan pemberitahuan. Pemberitahuan dibuat tersedia sebagai acara yang dikirim ke Amazon EventBridge (sebelumnya dikenal sebagai Amazon CloudWatch Events). Peristiwa dipancarkan atas dasar upaya terbaik.

Anda dapat menggunakan Amazon EventBridge untuk membuat aturan yang memicu tindakan terprogram sebagai respons terhadap suatu peristiwa. Misalnya, Anda dapat membuat dua EventBridge aturan: satu dipicu saat status armada berubah, dan yang lain dipicu saat instance dalam armada dihentikan. Dalam contoh ini, Anda dapat mengonfigurasi aturan pertama sehingga, jika status armada berubah, aturan akan memanggil topik SNS, mengirimkan pemberitahuan email kepada Anda. Anda dapat mengonfigurasi aturan kedua sehingga, jika instance dalam armada dihentikan, aturan akan memanggil fungsi Lambda untuk meluncurkan instance baru.

> **Note**
>
> Hanya armada tipe `maintain` dan `request` yang memancarkan peristiwa. Armada tipe `instant` tidak memancarkan peristiwa karena armada tipe tersebut mengirimkan permintaan satu kali sinkron, dan status armada segera diketahui dalam respons. Untuk menggunakan Amazon EventBridge untuk memantau peristiwa armada, jenis permintaan harus `maintain` atau`request`.

Untuk petunjuk tentang cara mendeskripsikan sejarah peristiwa armada, lihatJelaskan riwayat acara untuk Armada EC2 Anda.

Topik

- Membuat EventBridge aturan Amazon untuk memantau peristiwa Armada EC2 atau Armada Spot
- Jenis acara Armada EC2

- Tipe peristiwa Armada Spot

Membuat EventBridge aturan Amazon untuk memantau peristiwa Armada EC2 atau Armada Spot

Ketika pemberitahuan perubahan status dipancarkan untuk Armada EC2 atau Armada Spot, pemberitahuan tersebut dikirim sebagai peristiwa ke Amazon EventBridge sebagai file JSON. Jika EventBridge mendeteksi pola peristiwa yang cocok dengan pola yang ditentukan dalam aturan, EventBridge memanggil target (atau target) yang ditentukan dalam aturan.

Anda dapat menulis EventBridge aturan untuk mengotomatiskan tindakan berdasarkan pola peristiwa yang cocok.

Bidang berikut dalam acara membentuk pola acara yang didefinisikan dalam aturan:

`"source": "aws.ec2fleet"`

Mengidentifikasi bahwa peristiwa tersebut berasal dari Armada EC2.

`"detail-type": "EC2 Fleet State Change"`

Mengidentifikasi tipe peristiwa.

`"detail": { "sub-type": "submitted" }`

Mengidentifikasi subtipe peristiwa.

Untuk daftar peristiwa Armada EC2 dan Spot Fleet dan contoh data peristiwa, lihat Jenis acara Armada EC2 danTipe peristiwa Armada Spot.

Contoh

- Buat EventBridge aturan untuk mengirim pemberitahuan
- Buat EventBridge aturan untuk memicu fungsi Lambda

Buat EventBridge aturan untuk mengirim pemberitahuan

Contoh berikut membuat EventBridge aturan untuk mengirim email, pesan teks, atau pemberitahuan push seluler setiap kali Amazon EC2 memancarkan pemberitahuan perubahan status Armada EC2. Sinyal dalam contoh ini dipancarkan sebagai peristiwa `EC2 Fleet State Change`, yang memicu tindakan yang ditentukan oleh aturan.

Prasyarat

Sebelum membuat EventBridge aturan, Anda harus membuat topik Amazon SNS untuk email, pesan teks, atau pemberitahuan push seluler.

Untuk membuat EventBridge aturan untuk mengirim pemberitahuan saat status Armada EC2 berubah

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Pilih Buat aturan.
3. Untuk Tentukan detail aturan, lakukan hal berikut:
   a. Masukkan Nama untuk aturan tersebut dan, secara opsional, deskripsi.

      Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus peristiwa yang sama.
   b. Untuk Bus peristiwa, pilih default. Ketika AWS layanan di akun Anda menghasilkan acara, itu selalu masuk ke bus acara default akun Anda.
   c. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
   d. Pilih Selanjutnya.
4. Untuk Pola peristiwa build, lakukan hal berikut ini:
   a. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.
   b. Untuk Pola peristiwa, untuk contoh ini Anda akan menentukan pola peristiwa berikut agar sesuai dengan peristiwa `EC2 Fleet Instance Change`.

      ```
      {
       "source": ["aws.ec2fleet"],
       "detail-type": ["EC2 Fleet Instance Change"]
      }
      ```

      Untuk menambahkan pola peristiwa, Anda dapat menggunakan templat dengan memilih Bentuk pola peristiwa, atau menentukan pola Anda sendiri dengan memilih Pola kustom (editor JSON), sebagai berikut:

      i. Untuk menggunakan templat untuk membuat pola peristiwa, lakukan hal berikut:

         A. Pilih Formulir pola peristiwa.

         B. Untuk Sumber peristiwa, pilih Layanan AWS .

C. Untuk Layanan AWS , pilih Armada EC2.

D. Untuk Tipe peristiwa, pilih Perubahan Instans Armada EC2.

E. Untuk menyesuaikan templat, pilih Edit pola dan buat perubahan Anda agar sesuai dengan contoh pola peristiwa.

ii. (Alternatif) Untuk menentukan pola peristiwa khusus, lakukan hal berikut:

A. Pilih Pola kustom (editor JSON).

B. Dalam kotak Pola peristiwa, tambahkan pola peristiwa untuk contoh ini.

c. Pilih Selanjutnya.

5. Untuk Pilih target, lakukan hal berikut:

a. Untuk Tipe Target, pilih Layanan AWS .

b. Untuk Memilih target, pilih topik SNS untuk mengirim email, pesan teks, atau notifikasi push seluler saat peristiwa tersebut terjadi.

c. Untuk Topik, pilih topik yang ada. Anda harus terlebih dahulu membuat topik Amazon SNS menggunakan konsol Amazon SNS. Untuk informasi selengkapnya, lihat Menggunakan Amazon SNS untuk pesan application-to-person (A2P) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

d. (Opsional) Pada Pengaturan tambahan, Anda dapat mengonfigurasi pengaturan tambahan secara opsional. Untuk informasi selengkapnya, lihat Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa (langkah 16) di Panduan EventBridge Pengguna Amazon.

e. Pilih Selanjutnya.

6. (Opsional) Untuk Tanda, Anda dapat secara opsional menetapkan satu atau beberapa tanda ke aturan, lalu pilih Berikutnya.

7. Untuk Tinjau dan buat, lakukan hal berikut:

a. Tinjau detail aturan dan modifikasi seperlunya.

b. Pilih Buat aturan.

Untuk informasi selengkapnya, lihat EventBridge aturan Amazon dan pola EventBridge peristiwa Amazon di Panduan EventBridge Pengguna Amazon

Buat EventBridge aturan untuk memicu fungsi Lambda

Contoh berikut membuat EventBridge aturan untuk memicu fungsi Lambda setiap kali Amazon EC2 memancarkan pemberitahuan perubahan instans Armada EC2 saat instance diluncurkan. Sinyal dalam contoh ini dipancarkan sebagai peristiwa `EC2 Fleet Instance Change`, subtipe `launched`, yang memicu tindakan yang ditentukan oleh aturan.

Sebelum membuat EventBridge aturan, Anda harus membuat fungsi Lambda.

Untuk membuat fungsi Lambda untuk digunakan dalam aturan EventBridge

1. Buka AWS Lambda konsol di https://console.aws.amazon.com/lambda/.
2. Pilih Buat fungsi.
3. Masukkan nama untuk fungsi Anda, konfigurasikan kodenya, lalu pilih Buat fungsi.

   Untuk informasi selengkapnya, lihat Membuat fungsi Lambda pertama Anda di Panduan AWS Lambda Pengembang.

Untuk membuat EventBridge aturan untuk memicu fungsi Lambda saat instance di Armada EC2 mengubah status

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Pilih Buat aturan.
3. Untuk Tentukan detail aturan, lakukan hal berikut:

   a. Masukkan Nama untuk aturan tersebut dan, secara opsional, deskripsi.

      Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus peristiwa yang sama.

   b. Untuk Bus peristiwa, pilih default. Ketika AWS layanan di akun Anda menghasilkan acara, itu selalu masuk ke bus acara default akun Anda.

   c. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.

   d. Pilih Selanjutnya.
4. Untuk Pola peristiwa build, lakukan hal berikut ini:

   a. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.

   b. Untuk Pola peristiwa, untuk contoh ini Anda akan menentukan pola peristiwa berikut agar sesuai dengan peristiwa `EC2 Fleet Instance Change` dan subtipe `launched`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

Untuk menambahkan pola peristiwa, Anda dapat menggunakan templat dengan memilih Bentuk pola peristiwa, atau menentukan pola Anda sendiri dengan memilih Pola kustom (editor JSON), sebagai berikut:

i. Untuk menggunakan templat untuk membuat pola peristiwa, lakukan hal berikut:

A. Pilih Formulir pola peristiwa.

B. Untuk Sumber peristiwa, pilih Layanan AWS .

C. Untuk Layanan AWS , pilih Armada EC2.

D. Untuk Tipe peristiwa, pilih Perubahan Instans Armada EC2.

E. Pilih Edit pola, dan tambahkan `"detail": {"sub-type": ["launched"]` agar sesuai dengan contoh pola peristiwa. Untuk format JSON yang tepat, masukkan koma (`,`) setelah tanda kurung siku sebelumnya (`]`).

ii. (Alternatif) Untuk menentukan pola peristiwa kustom, lakukan hal berikut:

A. Pilih Pola kustom (editor JSON).

B. Dalam kotak Pola peristiwa, tambahkan pola peristiwa untuk contoh ini.

c. Pilih Selanjutnya.

5. Untuk Pilih target, lakukan hal berikut:

a. Untuk Tipe Target, pilih Layanan AWS .

b. Untuk Memilih target, pilih topik SNS untuk mengirim email, pesan teks, atau notifikasi push seluler saat peristiwa tersebut terjadi.

c. Untuk Topik, pilih fungsi Lambda, dan untuk Fungsi, pilih fungsi yang Anda buat untuk merespons saat peristiwa terjadi.

d. (Opsional) Di bawah Pengaturan tambahan, Anda dapat mengonfigurasi pengaturan tambahan secara opsional. Untuk informasi selengkapnya, lihat Membuat EventBridge

aturan Amazon yang bereaksi terhadap peristiwa (langkah 16) di Panduan EventBridge Pengguna Amazon.

e. Pilih Selanjutnya.

6. (Opsional) Untuk Tanda, Anda dapat secara opsional menetapkan satu atau beberapa tanda ke aturan, lalu pilih Berikutnya.
7. Untuk Tinjau dan buat, lakukan hal berikut:

a. Tinjau detail aturan dan modifikasi seperlunya.

b. Pilih Buat aturan.

Untuk tutorial tentang cara membuat fungsi Lambda dan EventBridge aturan yang menjalankan fungsi Lambda, lihat Tutorial: Log Status Instans Amazon EC2 Menggunakan dalam Panduan Pengembang. EventBridge AWS Lambda

Jenis acara Armada EC2

Ada lima jenis acara Armada EC2. Untuk setiap jenis acara, ada beberapa sub-jenis.

Tipe peristiwa

- Perubahan Status Armada EC2
- Perubahan Permintaan Instans Spot Armada EC2
- Perubahan Instans Armada EC2
- Informasi Armada EC2
- Kesalahan Armada EC2

Perubahan Status Armada EC2

Armada EC2 mengirimkan `EC2 Fleet State Change` acara ke Amazon EventBridge saat Armada EC2 mengubah status.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
```

```
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

Nilai yang mungkin untuk `sub-type` adalah:

`active`

Armada EC2 telah divalidasi dan Amazon EC2 berupaya untuk mempertahankan jumlah target dari instans yang sedang berjalan.

`deleted`

Permintaan Armada EC2 dihapus dan tidak ada instans yang berjalan. Armada EC2 akan dihapus dua hari setelah instansnya diakhiri.

`deleted_running`

Permintaan Armada EC2 dihapus dan tidak meluncurkan instans tambahan. Instans yang ada terus berjalan hingga diinterupsi atau diakhiri. Permintaan tetap berada dalam status ini sampai semua instans diinterupsi atau diakhiri.

`deleted_terminating`

Permintaan Armada EC2 dihapus dan instansnya diakhiri. Permintaan tetap berada dalam status ini sampai semua instans diakhiri.

`expired`

Permintaan Armada EC2 telah kedaluwarsa. Jika permintaan itu dibuat dengan set `TerminateInstancesWithExpiration`, peristiwa `terminated` berikutnya menunjukkan bahwa instans diakhiri.

`modify_in_progress`

Permintaan Armada EC2 sedang dimodifikasi. Permintaan tetap berada dalam status ini sampai modifikasi diproses sepenuhnya.

`modify_succeeded`

Permintaan Armada EC2 telah dimodifikasi.

`submitted`

Permintaan Armada EC2 sedang dievaluasi dan Amazon EC2 sedang bersiap untuk meluncurkan jumlah target instans.

`progress`

Permintaan Armada EC2 sedang dalam proses dipenuhi.

Perubahan Permintaan Instans Spot Armada EC2

Armada EC2 mengirimkan `EC2 Fleet Spot Instance Request Change` peristiwa ke Amazon EventBridge saat permintaan Instans Spot di armada berubah status.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Nilai yang mungkin untuk `sub-type` adalah:

`active`

Permintaan Instans Spot terpenuhi dan memiliki Instans Spot terkait.

`cancelled`

Anda membatalkan permintaan Instans Spot atau permintaan Instans Spot kedaluwarsa.

`disabled`

Anda menghentikan Instans Spot.

`submitted`

Permintaan Instans Spot dikirim.

Perubahan Instans Armada EC2

EC2 Fleet mengirimkan`EC2 Fleet Instance Change` acara ke Amazon EventBridge ketika sebuah instance dalam armada berubah status.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "instance-id": "i-0c594155dd5ff1829",
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

Nilai yang mungkin untuk`sub-type` adalah:

`launched`

Instans baru sudah diluncurkan.

`terminated`

Instans diakhiri.

`termination_notified`

Notifikasi pengakhiran instans dikirim ketika Instans Spot diakhiri oleh Amazon EC2 selama penurunan skala, ketika kapasitas target armada diturunkan, misalnya, dari kapasitas target 4 ke kapasitas target 3.

Informasi Armada EC2

Armada EC2 mengirimkan `EC2 Fleet Information` acara ke Amazon EventBridge ketika ada kesalahan selama pemenuhan. Peristiwa informasi tidak memblokir armada untuk mencoba memenuhi kapasitas targetnya.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

Nilai yang mungkin untuk `sub-type` adalah:

`fleetProgressHalted`

Harga di setiap spesifikasi peluncuran tidak berlaku karena berada di bawah harga Spot (semua spesifikasi peluncuran telah menghasilkan peristiwa `launchSpecUnusable`). Spesifikasi peluncuran mungkin menjadi valid jika harga Spot berubah.

`launchSpecTemporarilyBlacklisted`

Konfigurasi tidak valid dan beberapa upaya untuk meluncurkan instans gagal. Untuk informasi selengkapnya, lihat deskripsi peristiwa.

`launchSpecUnusable`

Harga dalam spesifikasi peluncuran tidak berlaku karena berada di bawah harga Spot.

`registerWithLoadBalancersFailed`

Upaya untuk mendaftarkan instans dengan penyeimbang beban gagal. Untuk informasi selengkapnya, lihat deskripsi peristiwa.

Kesalahan Armada EC2

Armada EC2 mengirimkan `EC2 Fleet Error` acara ke Amazon EventBridge ketika ada kesalahan selama pemenuhan. Peristiwa kesalahan memblokir armada untuk mencoba memenuhi kapasitas targetnya.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
```

```
    }
}
```

Nilai yang mungkin untuk `sub-type` adalah:

`iamFleetRoleInvalid`

Armada EC2 tidak memiliki izin yang diperlukan untuk meluncurkan atau mengakhiri instans.

`allLaunchSpecsTemporarilyBlacklisted`

Tidak ada konfigurasi yang valid, dan beberapa upaya untuk meluncurkan instans gagal. Untuk informasi selengkapnya, lihat deskripsi peristiwa.

`spotInstanceCountLimitExceeded`

Anda telah mencapai batas jumlah Instans Spot yang dapat diluncurkan.

`spotFleetRequestConfigurationInvalid`

Konfigurasi tidak valid. Untuk informasi selengkapnya, lihat deskripsi peristiwa.

Tipe peristiwa Armada Spot

Ada lima tipe peristiwa Armada Spot. Untuk setiap tipe peristiwa, ada beberapa subtipe.

Tipe peristiwa

- Perubahan Status Armada Spot EC2
- Perubahan Permintaan Instans Spot Armada Spot EC2
- Perubahan Instans Armada Spot EC2
- Informasi Armada Spot EC2
- Kesalahan Armada Spot EC2

Perubahan Status Armada Spot EC2

Spot Fleet mengirimkan file`EC2 Spot Fleet State Change` acara ke Amazon EventBridge saat Fleet Spot berubah status.

Berikut adalah data contoh untuk peristiwa ini.

```
{
```

```
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
        "sub-type": "submitted"
    }
}
```

Nilai yang mungkin untuk `sub-type` adalah:

`active`

Permintaan Armada Spot telah divalidasi dan Amazon EC2 berupaya untuk mempertahankan jumlah target instans yang sedang berjalan.

`cancelled`

Permintaan Armada Spot dibatalkan dan tidak ada instans yang berjalan. Armada Spot akan dihapus dua hari setelah instansnya diakhiri.

`cancelled_running`

Permintaan Armada Spot dibatalkan dan tidak meluncurkan instans tambahan. Instans yang ada terus berjalan hingga diinterupsi atau diakhiri. Permintaan tetap berada dalam status ini sampai semua instans diinterupsi atau diakhiri.

`cancelled_terminating`

Permintaan Armada Spot dibatalkan dan instansnya diakhiri. Permintaan tetap berada dalam status ini sampai semua instans diakhiri.

`expired`

Permintaan Armada Spot telah kedaluwarsa. Jika permintaan itu dibuat dengan set `TerminateInstancesWithExpiration`, peristiwa `terminated` berikutnya menunjukkan bahwa instans diakhiri.

`modify_in_progress`

Permintaan Armada Spot sedang dimodifikasi. Permintaan tetap berada dalam status ini sampai modifikasi diproses sepenuhnya.

`modify_succeeded`

Permintaan Armada Spot telah dimodifikasi.

`submitted`

Permintaan Armada Spot sedang dievaluasi dan Amazon EC2 sedang bersiap untuk meluncurkan jumlah target instans.

`progress`

Permintaan Armada Spot sedang dalam proses dipenuhi.

Perubahan Permintaan Instans Spot Armada Spot EC2

Armada Spot mengirimkan `EC2 Spot Fleet Spot Instance Request Change` peristiwa ke Amazon EventBridge saat permintaan Instans Spot di armada berubah status.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Nilai yang mungkin untuk `sub-type` adalah:

`active`

Permintaan Instans Spot terpenuhi dan memiliki Instans Spot terkait.

`cancelled`

Anda membatalkan permintaan Instans Spot atau permintaan Instans Spot kedaluwarsa.

`disabled`

Anda menghentikan Instans Spot.

`submitted`

Permintaan Instans Spot dikirim.

Perubahan Instans Armada Spot EC2

Armada Spot mengirimkan `EC2 Spot Fleet Instance Change` acara ke Amazon EventBridge saat instance di armada berubah status.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```

Nilai yang mungkin untuk`sub-type` adalah:

`launched`

Instans baru sudah diluncurkan.

`terminated`

Instans diakhiri.

`termination_notified`

Notifikasi pengakhiran instans dikirim ketika Instans Spot diakhiri oleh Amazon EC2 selama penurunan skala, ketika kapasitas target armada diturunkan, misalnya, dari kapasitas target 4 ke kapasitas target 3.

Informasi Armada Spot EC2

Spot Fleet mengirimkan file`EC2 Spot Fleet Information` acara ke Amazon EventBridge ketika ada kesalahan selama pemenuhan. Peristiwa informasi tidak memblokir armada untuk mencoba memenuhi kapasitas targetnya.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

Nilai yang mungkin untuk `sub-type` adalah:

`fleetProgressHalted`

Harga di setiap spesifikasi peluncuran tidak berlaku karena berada di bawah harga Spot (semua spesifikasi peluncuran telah menghasilkan peristiwa `launchSpecUnusable`). Spesifikasi peluncuran mungkin menjadi valid jika harga Spot berubah.

`launchSpecTemporarilyBlacklisted`

Konfigurasi tidak valid dan beberapa upaya untuk meluncurkan instans gagal. Untuk informasi selengkapnya, lihat deskripsi peristiwa.

`launchSpecUnusable`

Harga dalam spesifikasi peluncuran tidak berlaku karena berada di bawah harga Spot.

`registerWithLoadBalancersFailed`

Upaya untuk mendaftarkan instans dengan penyeimbang beban gagal. Untuk informasi selengkapnya, lihat deskripsi peristiwa.

Kesalahan Armada Spot EC2

Armada Spot mengirimkan `EC2 Spot Fleet Error` acara ke Amazon EventBridge ketika ada kesalahan selama pemenuhan. Peristiwa kesalahan memblokir armada untuk mencoba memenuhi kapasitas targetnya.

Berikut adalah data contoh untuk peristiwa ini.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
```

```
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Nilai yang mungkin untuk `sub-type` adalah:

`iamFleetRoleInvalid`

Armada Spot tidak memiliki izin yang diperlukan untuk meluncurkan atau mengakhiri sebuah instans.

`allLaunchSpecsTemporarilyBlacklisted`

Tidak ada konfigurasi yang valid, dan beberapa upaya untuk meluncurkan instans gagal. Untuk informasi selengkapnya, lihat deskripsi peristiwa.

`spotInstanceCountLimitExceeded`

Anda telah mencapai batas jumlah Instans Spot yang dapat diluncurkan.

`spotFleetRequestConfigurationInvalid`

Konfigurasi tidak valid. Untuk informasi selengkapnya, lihat deskripsi peristiwa.

Tutorial untuk Armada EC2

Ada berbagai cara untuk mengkonfigurasi Armada EC2. Konfigurasi yang Anda pilih tergantung pada kasus penggunaan spesifik Anda.

Tutorial berikut mencakup beberapa kasus penggunaan yang mungkin dan menyediakan tugas yang diperlukan untuk mengimplementasikannya.

Kasus penggunaan	Tautan ke tutorial
Gunakan pembobotan instans untuk mengelola ketersediaan dan kinerja Armada EC2 Anda. Dengan pembobotan instans, Anda menetapkan bobot untuk setiap jenis instans di Armada	Tutorial: Konfigurasikan Armada EC2 untuk menggunakan pembobotan instance

Kasus penggunaan	Tautan ke tutorial
EC2 Anda untuk mewakili kapasitas komputasi dan kinerjanya relatif satu sama lain. Berdasarkan bobot, armada dapat menggunakan kombinasi jenis instans yang ditentukan, asalkan dapat memenuhi kapasitas target yang diinginkan.	
Gunakan kapasitas Sesuai Permintaan untuk memastikan ketersediaan selama periode puncak, tetapi manfaatkan kapasitas Spot tambahan dengan biaya lebih rendah. Konfigurasikan Armada EC2 Anda untuk menggunakan Instans Sesuai Permintaan sebagai kapasitas utama untuk memastikan kapasitas yang tersedia selama periode puncak. Selain itu, alokasikan beberapa kapasitas ke Instans Spot untuk mendapatkan keuntungan dari harga diskon, sambil mengingat bahwa Instans Spot dapat terganggu jika Amazon EC2 membutuhkan kapasitasnya kembali.	Tutorial: Konfigurasikan Armada EC2 untuk menggunakan Instans Sesuai Permintaan sebagai kapasitas utama

Kasus penggunaan	Tautan ke tutorial
Gunakan Reservasi Kapasitas untuk memesan kapasitas komputasi untuk Instans Sesuai Permintaan Anda. Konfigurasikan Armada EC2 Anda untuk menggunakan Reservasi `targeted` Kapasitas terlebih dahulu saat meluncurkan Instans Sesuai Permintaan. Jika Anda memiliki persyaratan kapasitas yang ketat, dan menjalankan beban kerja penting bisnis yang memerlukan jaminan kapasitas pada tingkat jangka panjang atau jangka pendek tertentu, kami sarankan Anda membuat Reservasi Kapasitas untuk memastikan bahwa Anda selalu memiliki akses ke kapasitas Amazon EC2 saat Anda membutuhkannya, selama Anda membutuhkannya.	Tutorial: Konfigurasikan Armada EC2 untuk meluncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas yang ditargetkan
Gunakan Blok Kapasitas untuk menyimpan instans GPU yang sangat dicari untuk beban kerja ML Anda. Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Blok Kapasitas.	Tutorial: Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Blok Kapasitas

Kasus penggunaan	Tautan ke tutorial
Gunakan Reservasi Kapasitas Interruptible untuk menggunakan kembali kapasitas idle sementara di seluruh Organisasi Anda AWS dan menghemat biaya. Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Reservasi Kapasitas yang Dapat Diinterupsi, yang mewakili kapasitas cadangan dalam organisasi Anda. AWS Pemilik kapasitas dapat merebut kembali kapasitas kapan saja. Setelah direklamasi, EC2 menghentikan instans setelah pemberitahuan 2 menit.	Tutorial: Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Reservasi Kapasitas yang Dapat Diinterupsi

Tutorial: Konfigurasikan Armada EC2 untuk menggunakan pembobotan instance

Tutorial ini menggunakan perusahaan fiktif bernama Example Corp untuk mengilustrasikan proses permintaan Armada EC2 menggunakan pembobotan instans.

Tujuan

Example Corp, sebuah perusahaan farmasi, ingin menggunakan kekuatan komputasi Amazon EC2 untuk melakukan skrining senyawa kimia yang dapat digunakan untuk melawan kanker.

Perencanaan

Pertama-tama, Example Corp meninjau Praktik Terbaik Spot. Selanjutnya, Example Corp menentukan kebutuhan untuk Armada EC2 mereka.

Jenis instance

Example Corp memiliki aplikasi intensif komputasi dan intensif memori yang memiliki performa terbaik dengan setidaknya 60 GB memori dan delapan virtual CPU (vCPU). Mereka ingin memaksimalkan sumber daya ini untuk aplikasi dengan harga serendah mungkin. Example Corp memutuskan bahwa tipe instans EC2 berikut akan memenuhi kebutuhan mereka:

Jenis instans	Memori (GiB)	v CPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Kapasitas target dalam unit

Dengan pembobotan instance, kapasitas target dapat sama dengan sejumlah instance (default) atau kombinasi faktor seperti inti (vCPU), memori (), dan penyimpanan (GBGiBs). Dengan mempertimbangkan dasar untuk aplikasi mereka (60 GB RAM dan delapan vCPU) sebagai satu unit, Example Corp memutuskan bahwa 20 kali jumlah ini akan memenuhi kebutuhan mereka. Jadi perusahaan menetapkan kapasitas target permintaan Armada EC2 mereka menjadi 20 unit.

Bobot instans

Setelah menentukan kapasitas target, Example Corp menghitung bobot instans. Guna menghitung bobot instans untuk setiap tipe instans, mereka menentukan unit dari setiap tipe instans yang diperlukan untuk mencapai kapasitas target sebagai berikut:

- r3.2xlarge (61.0 GB, 8 vCPUs) = 1 unit 20
- r3.4xlarge (122.0 GB, 16 vCPUs) = 2 unit 20
- r3.8xlarge (244.0 GB, 32 vCPUs) = 4 unit 20

Oleh karena itu, Example Corp menetapkan bobot instans 1, 2, dan 4 ke konfigurasi peluncuran masing-masing dalam permintaan Armada EC2.

Harga per unit jam

Example Corp menggunakan harga Sesuai Permintaan per jam instans sebagai titik awal untuk harga mereka. Mereka juga dapat menggunakan harga Spot baru-baru ini, atau kombinasi keduanya. Untuk menghitung harga per unit jam, mereka membagi harga awal per jam instans berdasarkan bobot. Misalnya:

Jenis instans	Harga Sesuai Permintaan	Bobot instans	Harga per unit jam
r3.2xLarge	$0,7	1	$0,7
r3.4xLarge	$1,4	2	$0,7
r3.8xlarge	$2,8	4	$0,7

Example Corp dapat menggunakan harga global per unit jam sebesar 0,7 USD dan kompetitif untuk ketiga tipe instans. Mereka juga dapat menggunakan harga global per unit jam 0,7 USD dan harga spesifik per unit jam 0,9 USD di spesifikasi peluncuran `r3.8xlarge`.

Memverifikasi izin

Sebelum membuat Armada EC2, Example Corp memverifikasi bahwa mereka memiliki peran IAM dengan izin yang diperlukan. Untuk informasi selengkapnya, lihat Prasyarat Armada EC2.

Membuat templat peluncuran

Selanjutnya, Example Corp membuat templat peluncuran. ID templat peluncuran digunakan di langkah berikut. Untuk informasi selengkapnya, lihat Buat template peluncuran Amazon EC2.

Membuat Armada EC2

Example Corp membuat file, `config.json`, dengan konfigurasi sebagai berikut untuk Armada EC2 file tersebut. Dalam contoh berikut, ganti pengidentifikasi sumber daya dengan pengidentifikasi sumber daya Anda sendiri.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
            "Overrides": [
```

```
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Example Corp membuat Armada EC2 menggunakan perintah create-fleet berikut.

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Untuk informasi selengkapnya, lihat Membuat Armada EC2.

Pemenuhan

Strategi alokasi menentukan asal dari kolam kapasitas Spot yang menjadi sumber Instans Spot Anda.

Dengan strategi `lowest-price` (yang merupakan strategi default), Instans Spot berasal dari kolam dengan harga terendah per unit pada saat pemenuhan. Untuk menyediakan kapasitas 20 unit, Armada EC2 meluncurkan 20 instans `r3.2xlarge` (20 dibagi 1), 10 instans `r3.4xlarge` (20 dibagi 2), atau 5 instans `r3.8xlarge` (20 dibagi 4).

Jika Example Corp menggunakan strategi `diversified`, Instans Spot akan berasal dari ketiga kolam. Armada EC2 akan meluncurkan 6 instans `r3.2xlarge` (yang menyediakan 6 unit), 3 instans

`r3.4xlarge` (yang menyediakan 6 unit), dan 2 instans `r3.8xlarge` (yang menyediakan 8 unit), dengan total 20 unit.

Tutorial: Konfigurasikan Armada EC2 untuk menggunakan Instans Sesuai Permintaan sebagai kapasitas utama

Tutorial ini menggunakan perusahaan fiktif bernama ABC Online untuk menggambarkan proses permintaan Armada EC2 dengan Sesuai Permintaan sebagai kapasitas primer, dan kapasitas Spot jika tersedia.

Tujuan

ABC Online, perusahaan pengiriman restoran, bertujuan untuk menyediakan kapasitas Amazon EC2 di seluruh jenis instans EC2 dan opsi pembelian untuk mencapai skala, kinerja, dan biaya yang diinginkan.

Rencana

ABC Online membutuhkan kapasitas tetap untuk menangani periode puncak, tetapi ingin mendapatkan keuntungan dari kapasitas tambahan dengan biaya lebih rendah. Perusahaan menentukan persyaratan berikut untuk Armada EC2 mereka:

- Kapasitas Instans Sesuai Permintaan – ABC Online memerlukan 15 Instans Sesuai Permintaan untuk memastikan bahwa mereka dapat mengakomodasi lalu lintas pada periode puncak.
- Kapasitas Instans Spot — Untuk meningkatkan kinerja, tetapi dengan harga lebih murah, ABC Online berencana untuk menyediakan 5 Instans Spot.

Memverifikasi izin

Sebelum membuat Armada EC2, ABC Online memverifikasi bahwa mereka memiliki peran IAM dengan izin yang diperlukan. Untuk informasi selengkapnya, lihat Prasyarat Armada EC2.

Membuat templat peluncuran

Selanjutnya, ABC Online membuat templat peluncuran. ID templat peluncuran digunakan di langkah berikut. Untuk informasi selengkapnya, lihat Buat template peluncuran Amazon EC2.

Membuat Armada EC2

ABC Online membuat file, `config.json`, dengan konfigurasi sebagai berikut untuk Armada EC2-nya. Dalam contoh berikut, ganti pengidentifikasi sumber daya dengan pengidentifikasi sumber daya Anda sendiri.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

ABC Online membuat Armada EC2 menggunakan perintah create-fleet berikut.

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Untuk informasi selengkapnya, lihat Membuat Armada EC2.

Pemenuhan

Strategi alokasi menentukan bahwa kapasitas On-Demand selalu terpenuhi, sedangkan keseimbangan kapasitas target terpenuhi sebagai Spot jika ada kapasitas yang tersedia.

Tutorial: Konfigurasikan Armada EC2 untuk meluncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas yang ditargetkan

Tutorial ini memandu Anda melalui semua langkah yang harus Anda lakukan agar Armada EC2 Anda meluncurkan Instans Sesuai Permintaan ke Reservasi Kapasitas `targeted`.

Anda akan mempelajari cara mengonfigurasi armada untuk menggunakan Reservasi Kapasitas Sesuai Permintaan `targeted` terlebih dahulu saat meluncurkan Instans Sesuai Permintaan. Anda juga akan mempelajari cara mengonfigurasi armada sehingga saat total kapasitas target Sesuai Permintaan melebihi jumlah Reservasi Kapasitas yang tidak terpakai yang tersedia, armada tersebut akan menggunakan strategi alokasi yang ditentukan untuk memilih kolam instans untuk meluncurkan kapasitas target yang tersisa.

Konfigurasi Armada EC2

Dalam tutorial ini, armada dikonfigurasi sebagai berikut:

- Kapasitas target: 10 Instans Sesuai Permintaan
- Total Reservasi Kapasitas `targeted` yang tidak terpakai: 6 (kurang dari kapasitas target Sesuai Permintaan armada sebesar 10 Instans Sesuai Permintaan)
- Jumlah kolam Reservasi Kapasitas: 2 (`us-east-1a` dan `us-east-1b`)
- Jumlah Reservasi Kapasitas per kolam: 3
- Strategi alokasi Sesuai Permintaan: `lowest-price` (Jika jumlah Reservasi Kapasitas yang tidak terpakai kurang dari kapasitas target Sesuai Permintaan, armada akan menentukan kolam tempat meluncurkan kapasitas Sesuai Permintaan yang tersisa berdasarkan strategi alokasi Sesuai Permintaan.)

  Perhatikan bahwa Anda juga dapat menggunakan strategi alokasi `prioritized` alih-alih strategi alokasi `lowest-price`.

Untuk meluncurkan Instans Sesuai Permintaan ke Reservasi Kapasitas targeted, Anda harus menjalankan sejumlah langkah, sebagai berikut:

- Langkah 1: Membuat Reservasi Kapasitas
- Langkah 2: Membuat grup sumber daya Reservasi Kapasitas
- Langkah 3: Menambahkan Reservasi Kapasitas ke grup sumber daya Reservasi Kapasitas
- (Opsional) Langkah 4: Melihat Reservasi Kapasitas di grup sumber daya
- Langkah 5: Membuat templat peluncuran yang menentukan bahwa Reservasi Kapasitas menargetkan grup sumber daya tertentu
- (Opsional) Langkah 6: Mendeskripsikan templat peluncuran
- Langkah 7: Membuat Armada EC2
- (Opsional) Langkah 8: Melihat jumlah Reservasi Kapasitas yang tidak terpakai yang tersisa

Langkah 1: Membuat Reservasi Kapasitas

Gunakan create-capacity-reservationperintah untuk membuat Reservasi Kapasitas, tiga untuk `us-east-1a` dan tiga lainnya untuk`us-east-1b`. Kecuali untuk Zona Ketersediaan, atribut lain dari Reservasi Kapasitas bersifat identik.

3 Reservasi Kapasitas di **`us-east-1a`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Contoh ID Reservasi Kapasitas yang dihasilkan

```
cr-1234567890abcdef1
```

3 Reservasi Kapasitas di **`us-east-1b`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Contoh ID Reservasi Kapasitas yang dihasilkan

```
cr-54321abcdef567890
```

Langkah 2: Membuat grup sumber daya Reservasi Kapasitas

Gunakan layanan `resource-groups` dan perintah create-group untuk membuat grup sumber daya Reservasi Kapasitas. Dalam contoh ini, grup sumber daya diberi nama `my-cr-group`. Untuk informasi tentang alasan Anda harus membuat grup sumber daya, lihat Gunakan Reservasi Kapasitas untuk memesan kapasitas Sesuai Permintaan di Armada EC2.

```
aws resource-groups create-group \
    --name my-cr-group \
```

```
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Langkah 3: Menambahkan Reservasi Kapasitas ke grup sumber daya Reservasi Kapasitas

Gunakan layanan `resource-groups` dan perintah group-resources untuk menambahkan Reservasi Kapasitas yang Anda buat di Langkah 1 ke grup sumber daya Reservasi Kapasitas. Perhatikan bahwa Anda harus mereferensikan Reservasi Kapasitas Sesuai Permintaan berdasarkan Reservasi tersebut. ARNs

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Contoh Output

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Opsional) Langkah 4: Melihat Reservasi Kapasitas di grup sumber daya

Gunakan `resource-groups` layanan dan list-group-resourcesperintah untuk mendeskripsikan grup sumber daya secara opsional untuk melihat Reservasi Kapasitasnya.

```
aws resource-groups list-group-resources --group my-cr-group
```

Contoh Output

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
```

```
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

Langkah 5: Membuat templat peluncuran yang menentukan bahwa Reservasi Kapasitas menargetkan grup sumber daya tertentu

Gunakan create-launch-templateperintah untuk membuat template peluncuran untuk menentukan Reservasi Kapasitas yang akan digunakan. Dalam contoh ini, armada akan menggunakan Reservasi Kapasitas `targeted`, yang telah ditambahkan ke grup sumber daya. Oleh karena itu, data templat peluncuran menentukan bahwa Reservasi Kapasitas menargetkan grup sumber daya tertentu. Dalam contoh ini, templat peluncuran diberi nama `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

(Opsional) Langkah 6: Mendeskripsikan templat peluncuran

Gunakan describe-launch-template-versionsperintah untuk mendeskripsikan template peluncuran secara opsional untuk melihat konfigurasinya.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Contoh Output

```
{
```

```
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

Langkah 7: Membuat Armada EC2

Buat Armada EC2 yang menentukan informasi konfigurasi untuk instans yang akan diluncurkan. Konfigurasi Armada EC2 berikut hanya menampilkan konfigurasi terkait untuk contoh ini. Templat peluncuran `my-launch-template` adalah templat peluncuran yang Anda buat di Langkah 5. Terdapat dua kolam instans, masing-masing dengan tipe instans yang sama (`c5.xlarge`), tetapi dengan Zona Ketersediaan (`us-east-1a` dan `us-east-1b`) yang berbeda. Harga kolam instans sama karena harga ditentukan untuk Wilayah, bukan per Zona Ketersediaan. Total kapasitas target adalah 10, dan tipe kapasitas target default adalah `on-demand`. Strategi alokasi Sesuai Permintaan adalah `lowest-price`. Strategi penggunaan untuk Reservasi Kapasitas adalah `use-capacity-reservations-first`.

> **Note**
>
> Tipe armada harus `instant`. Tipe armada lainnya tidak mendukung `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
```

```
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Setelah Anda membuat armada `instant` menggunakan konfigurasi sebelumnya, 10 instans berikut diluncurkan untuk memenuhi kapasitas target:

- Reservasi Kapasitas digunakan terlebih dahulu untuk meluncurkan 6 Instans Sesuai Permintaan sebagai berikut:
  - 3 Instans Sesuai Permintaan diluncurkan ke dalam 3 Reservasi Kapasitas `c5.xlarge targeted` di `us-east-1a`
  - 3 Instans Sesuai Permintaan diluncurkan ke dalam 3 Reservasi Kapasitas `c5.xlarge targeted` di `us-east-1b`
- Untuk memenuhi kapasitas target, 4 Instans Sesuai Permintaan tambahan diluncurkan ke kapasitas Sesuai Permintaan reguler sesuai dengan strategi alokasi Sesuai Permintaan, yaitu

`lowest-price` dalam contoh ini. Namun, karena kolam memiliki harga yang sama (karena harganya adalah per Wilayah dan bukan per Zona Ketersediaan), armada meluncurkan 4 Instans Sesuai Permintaan yang tersisa ke salah satu kolam.

(Opsional) Langkah 8: Melihat jumlah Reservasi Kapasitas yang tidak terpakai yang tersisa

Setelah armada diluncurkan, Anda dapat menjalankan secara opsional describe-capacity-reservationsuntuk melihat berapa banyak Reservasi Kapasitas yang tidak terpakai yang tersisa. Dalam contoh ini, Anda akan melihat respons berikut, yang menunjukkan bahwa semua Reservasi Kapasitas di semua kolam telah digunakan.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutorial: Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Blok Kapasitas

Tutorial ini memandu Anda melalui langkah-langkah yang harus Anda lakukan sehingga Armada EC2 Anda meluncurkan instans ke Blok Kapasitas.

Dalam kebanyakan kasus, kapasitas target permintaan Armada EC2 harus kurang dari atau sama dengan kapasitas yang tersedia dari reservasi Blok Kapasitas yang Anda targetkan. Permintaan kapasitas target yang melebihi batas reservasi Blok Kapasitas tidak akan dipenuhi. Jika permintaan kapasitas target melebihi batas reservasi Blok Kapasitas Anda, Anda akan menerima kapasitas yang melebihi batas reservasi Blok Kapasitas Anda. `Insufficient Capacity Exception`

> **Note**
>
> Untuk Blok Kapasitas, Armada EC2 tidak akan melakukan fallback guna meluncurkan Instans Sesuai Permintaan untuk sisa kapasitas target yang diinginkan.

Jika Armada EC2 tidak dapat memenuhi kapasitas target yang diminta dalam reservasi Blok Kapasitas yang tersedia, Armada EC2 akan memenuhi kapasitas sebanyak mungkin dan mengembalikan instans yang dapat diluncurkan. Anda dapat mengulangi panggilan ke Armada EC2 lagi hingga semua instans disediakan.

Setelah mengonfigurasi permintaan Armada EC2, Anda harus menunggu hingga tanggal mulai reservasi Blok Kapasitas Anda. Jika Anda mengajukan permintaan ke Armada EC2 untuk diluncurkan ke Blok Kapasitas yang belum dimulai, Anda akan menerima file`Insufficient Capacity Error`.

Setelah reservasi Blok Kapasitas aktif, Anda dapat membuat panggilan API Armada EC2 dan menyediakan instans ke dalam Blok Kapasitas berdasarkan parameter yang Anda pilih. Instans yang berjalan di Blok Kapasitas terus berjalan hingga Anda menghentikan atau menghentikannya secara manual atau hingga Amazon EC2 menghentikan instans saat reservasi Blok Kapasitas berakhir.

Untuk informasi selengkapnya tentang Blok Kapasitas, lihatBlok Kapasitas untuk ML.

Pertimbangan-pertimbangan

- Hanya jenis permintaan Armada EC2 `instant` yang didukung untuk meluncurkan instans ke Blok Kapasitas. Untuk informasi selengkapnya, lihat Konfigurasikan jenis Armada EC2 instant.
- Beberapa Blok Kapasitas dalam permintaan Armada EC2 yang sama tidak didukung.
- Menggunakan `OnDemandTargetCapacity` atau `SpotTargetCapacity` sekaligus juga mengatur `capacity-block` sebagai `DefaultTargetCapacity` tidak didukung.
- Jika `DefaultTargetCapacityType` diatur ke `capacity-block`, Anda tidak dapat menyediakan `OnDemandOptions::CapacityReservationOptions`. Pengecualian akan terjadi.

Untuk mengonfigurasi Armada EC2 untuk meluncurkan instans ke Blok Kapasitas

1. Buat template peluncuran.

   Dalam template peluncuran, lakukan hal berikut:

   - Untuk`InstanceMarketOptionsRequest`, atur `MarketType` ke`capacity-block`.
   - Untuk menargetkan reservasi Blok Kapasitas, untuk`CapacityReservationID`, tentukan ID reservasi Blok Kapasitas.

Catat nama dan versi template peluncuran. Anda akan menggunakan informasi ini di langkah berikutnya.

Untuk informasi selengkapnya tentang membuat template peluncuran, lihatBuat template peluncuran Amazon EC2.

2. Konfigurasikan Armada EC2.

   Buat file,`config.json`, dengan konfigurasi berikut untuk Armada EC2 Anda. Dalam contoh berikut, ganti pengidentifikasi sumber daya dengan pengidentifikasi sumber daya Anda sendiri.

   Untuk informasi selengkapnya tentang mengonfigurasi Armada EC2, lihat. Membuat Armada EC2

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
}
```

3. Luncurkan armada.

   Gunakan perintah create-fleet berikut.

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Untuk informasi selengkapnya, lihat Membuat Armada EC2.

Tutorial: Konfigurasikan Armada EC2 Anda untuk meluncurkan instans ke Reservasi Kapasitas yang Dapat Diinterupsi

Tutorial ini memandu Anda melalui langkah-langkah yang harus Anda lakukan sehingga Armada EC2 Anda meluncurkan instans ke Reservasi Kapasitas Interruptible.

Reservasi Kapasitas Interruptible mewakili kapasitas cadangan yang dipinjamkan kepada Anda oleh pemilik Reservasi Kapasitas Sesuai Permintaan dalam organisasi Anda. AWS Reservasi ini cocok untuk beban kerja yang dapat terputus karena pemilik kapasitas dapat merebut kembali kapasitas kapan saja dengan pemberitahuan interupsi 2 menit, setelah itu EC2 menghentikan instans. Untuk informasi selengkapnya tentang Reservasi Kapasitas yang Dapat Diinterupsi, lihat. Reservasi Kapasitas yang Dapat Diputus

Kapasitas target permintaan Armada EC2 harus kurang dari atau sama dengan kapasitas yang tersedia dari Reservasi Kapasitas Interruptible yang Anda targetkan. Jika permintaan kapasitas target melebihi kapasitas yang tersedia dari Reservasi Kapasitas Interruptible Anda, Armada EC2 meluncurkan sebanyak mungkin instans dan melaporkan instans yang diluncurkan dalam respons API.

Instans yang berjalan dalam Reservasi Kapasitas yang Dapat Diinterupsi terus berjalan hingga Anda menghentikan atau menghentikannya secara manual, atau hingga pemilik kapasitas merebut kembali kapasitas tersebut. Saat pemilik kapasitas mengklaim kembali kapasitasnya, Amazon EC2 mengirimkan pemberitahuan EventBridge Amazon 2 menit sebelum menghentikan instans.

Pertimbangan-pertimbangan

- Hanya jenis `instant` permintaan Armada EC2 yang didukung untuk meluncurkan instans ke Reservasi Kapasitas yang Dapat Diinterupsi.
- Menggunakan `OnDemandTargetCapacity` atau `SpotTargetCapacity` sementara juga mengatur `reserved-capacity` sebagai `DefaultTargetCapacityType` tidak didukung.
- Saat Anda menentukan beberapa templat peluncuran, masing-masing menargetkan Reservasi Kapasitas Interruptible yang berbeda, Armada EC2 menyediakan instans di semua reservasi yang cocok.
- Untuk Reservasi Kapasitas Interruptible, Armada EC2 tidak mundur untuk meluncurkan Instans Sesuai Permintaan atau Instans Spot untuk sisa kapasitas target yang diinginkan.

Memverifikasi izin

Sebelum membuat Armada EC2, verifikasi bahwa Anda memiliki peran IAM dengan izin yang diperlukan. Untuk informasi selengkapnya, lihat Prasyarat Armada EC2.

Untuk meluncurkan instans ke Reservasi Kapasitas Interruptible, Anda harus melakukan langkah-langkah berikut:

Langkah 1: Buat templat peluncuran

Gunakan create-launch-templateperintah untuk membuat template peluncuran yang menentukan Reservasi Kapasitas Interruptible untuk ditargetkan. Dalam template peluncuran, atur `MarketType` ke `interruptible-capacity-reservation` dan tentukan `CapacityReservationId` Reservasi Kapasitas Interruptible Anda.

Contoh konfigurasi template peluncuran:

```
{
    "LaunchTemplateName": "interruptible-cr-launch-template",
    "LaunchTemplateData": {
        "InstanceType": "m5.large",
        "ImageId": "ami-0abcdef1234567890",
        "CapacityReservationSpecification": {
            "CapacityReservationTarget": {
                "CapacityReservationId": "cr-0123456789abcdef0"
            }
        },
        "InstanceMarketOptions": {
            "MarketType": "interruptible-capacity-reservation"
        }
    }
}
```

Contoh Output

```
{
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-0123456789example",
        "LaunchTemplateName": "interruptible-cr-launch-template",
        "CreateTime": "2026-03-12T10:00:00.000Z",
        "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
```

```
        "DefaultVersionNumber": 1,
        "LatestVersionNumber": 1
    }
}
```

Untuk informasi selengkapnya, lihat Buat template peluncuran Amazon EC2.

Langkah 2: Konfigurasikan Armada EC2

Buat file konfigurasi untuk Armada EC2 yang menentukan template peluncuran dan kapasitas target. Konfigurasi berikut menggunakan template peluncuran `interruptible-cr-launch-template` yang Anda buat di Langkah 1.

Anda harus menentukan `ReservedCapacityOptions` dengan `ReservationType` set ke `interruptible-capacity-reservation` saat menggunakan `reserved-capacity` sebagai`DefaultTargetCapacityType`.

Buat file bernama `config.json` dengan konten berikut:

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "interruptible-cr-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "m5.large",
                    "AvailabilityZone": "us-east-1a"
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "reserved-capacity"
    },
    "ReservedCapacityOptions": {
        "ReservationType": ["interruptible-capacity-reservation"]
    },
    "Type": "instant"
```

```
}
```

Parameter konfigurasi kunci:

Parameter	Deskripsi
`DefaultTargetCapacityType`	Setel `reserved-capacity` untuk menunjukkan bahwa instance harus diluncurkan ke kapasitas cadangan.
`ReservedCapacityOptions`	Menentukan jenis kapasitas cadangan. Untuk Reservasi Kapasitas yang Dapat Diinterupsi, atur ke. `ReservationType` `["interruptible-capacity-reservation"]`
`Type`	Harus diatur ke `instant`. Hanya armada instan yang didukung untuk Reservasi Kapasitas Interruptible.

Langkah 3: Luncurkan armada dan lihat hasilnya

Gunakan perintah create-fleet untuk membuat armada:

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Setelah Anda membuat `instant` armada menggunakan konfigurasi sebelumnya, Armada EC2 meluncurkan 10 instans ke Reservasi Kapasitas Interruptible untuk memenuhi kapasitas target.

> **Note**
>
> Jika armada tidak dapat memenuhi kapasitas target penuh, respons mencakup contoh yang diluncurkan dan kesalahan untuk kapasitas yang tidak terpenuhi.

Contoh Output

```
{
    "FleetId": "fleet-12345678-1234-1234-1234-123456789012",
    "Instances": [
        {
```

```
            "LaunchTemplateAndOverrides": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": {
                    "InstanceType": "m5.large",
                    "AvailabilityZone": "us-east-1a"
                }
            },
            "Lifecycle": "interruptible-capacity-reservation",
            "InstanceIds": [
                "i-0123456789example1",
                "i-0123456789example2",
                "i-0123456789example3",
                "i-0123456789example4",
                "i-0123456789example5",
                "i-0123456789example6",
                "i-0123456789example7",
                "i-0123456789example8",
                "i-0123456789example9",
                "i-0123456789example0"
            ],
            "InstanceType": "m5.large",
            "Platform": "Linux/UNIX"
        }
    ],
    "Errors": []
}
```

Untuk informasi selengkapnya, lihat Membuat Armada EC2.

Bersihkan

Untuk menghentikan biaya, hentikan kasus ketika mereka tidak lagi diperlukan. Perhatikan bahwa EC2 juga menghentikan instans yang diluncurkan ke Reservasi Kapasitas yang Dapat Diinterupsi secara otomatis ketika pemilik kapasitas merebut kembali kapasitas.

Sumber daya terkait

- Reservasi Kapasitas yang Dapat Diputus
- Cadangan kapasitas komputasi dengan Reservasi Kapasitas Sesuai Permintaan EC2

- Bekerja dengan Armada EC2
- Membuat Armada EC2
- Simpan parameter peluncuran instans di templat peluncuran Amazon EC2

Contoh konfigurasi CLI untuk Armada EC2

Anda dapat menentukan konfigurasi Armada EC2 Anda dalam file JSON, dan kemudian mereferensikan file tersebut dengan perintah create-fleet untuk membuat armada Anda, sebagai berikut:

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Contoh berikut menggambarkan konfigurasi peluncuran untuk berbagai kasus penggunaan Armada EC2. Untuk informasi selengkapnya tentang parameter konfigurasi, lihat create-fleet.

Contoh

- Contoh 1: Meluncurkan Instans Spot sebagai opsi pembelian default
- Contoh 2: Meluncurkan Instans Sesuai Permintaan sebagai opsi pembelian default
- Contoh 3: Meluncurkan Instans Sesuai Permintaan sebagai kapasitas primer
- Contoh 4: Luncurkan Instans Sesuai Permintaan menggunakan beberapa Reservasi Kapasitas
- Contoh 5: Luncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas ketika total kapasitas target melebihi jumlah Reservasi Kapasitas yang tidak digunakan
- Contoh 6: Luncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas yang ditargetkan
- Contoh 7: Konfigurasikan Penyeimbangan Kembali Kapasitas untuk meluncurkan Instans Spot pengganti
- Contoh 8: Luncurkan Instans Spot dalam armada yang dioptimalkan kapasitas
- Contoh 9: Luncurkan Instans Spot dalam armada yang dioptimalkan kapasitas dengan prioritas
- Contoh 10: Luncurkan Instans Spot di armada price-capacity-optimized
- Contoh 11: Konfigurasikan pemilihan tipe instans berbasis atribut

Untuk contoh CLI lainnya untuk armada tipe`instant`, lihat. Konfigurasikan jenis Armada EC2 instant

Contoh 1: Meluncurkan Instans Spot sebagai opsi pembelian default

Contoh berikut menentukan parameter minimum yang diperlukan dalam Armada EC2: templat peluncuran, kapasitas target, dan opsi pembelian default. Templat peluncuran diidentifikasi dengan ID templat dan nomor versi peluncurannya. Kapasitas target untuk armada adalah 2 instans, dan opsi pembelian default adalah `spot`, yang menghasilkan armada meluncurkan 2 Instans Spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Contoh 2: Meluncurkan Instans Sesuai Permintaan sebagai opsi pembelian default

Contoh berikut menentukan parameter minimum yang diperlukan dalam Armada EC2: templat peluncuran, kapasitas target, dan opsi pembelian default. Templat peluncuran diidentifikasi dengan ID templat dan nomor versi peluncurannya. Kapasitas target untuk armada adalah 2 instans, dan opsi pembelian default adalah `on-demand`, yang menghasilkan armada meluncurkan 2 Instans Sesuai Permintaan.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
```

```
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Contoh 3: Meluncurkan Instans Sesuai Permintaan sebagai kapasitas primer

Contoh berikut menentukan total kapasitas target dari 2 instans untuk armada tersebut dan kapasitas target dari 1 Instans Sesuai Permintaan. Opsi pembelian default adalah `spot`. Armada meluncurkan 1 Instans Sesuai Permintaan sebagaimana ditentukan, tetapi perlu meluncurkan satu instans lagi untuk memenuhi total kapasitas target. Opsi pembelian untuk selisihnya dihitung sebagai `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, yang menghasilkan armada yang meluncurkan 1 Instans Spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Contoh 4: Luncurkan Instans Sesuai Permintaan menggunakan beberapa Reservasi Kapasitas

Anda dapat mengonfigurasi armada agar menggunakan Reservasi Kapasitas Sesuai Permintaan terlebih dahulu saat meluncurkan Instans Sesuai Permintaan dengan mengatur strategi penggunaan

untuk Reservasi Kapasitas ke `use-capacity-reservations-first`. Contoh ini menunjukkan cara armada memilih Reservasi Kapasitas yang akan digunakan jika terdapat lebih banyak Reservasi Kapasitas daripada yang dibutuhkan untuk memenuhi kapasitas target.

Dalam contoh ini, konfigurasi armada adalah sebagai berikut:

- Kapasitas target: 12 Instans Sesuai Permintaan
- Total Reservasi Kapasitas yang tidak terpakai: 15 (lebih dari kapasitas target armada sebesar 12 Instans Sesuai Permintaan)
- Jumlah kolam Reservasi Kapasitas: 3 (`m5.large`, `m4.xlarge`, dan `m4.2xlarge`)
- Jumlah Reservasi Kapasitas per kolam: 5
- Strategi alokasi Sesuai Permintaan: `lowest-price` (Jika terdapat lebih dari satu Reservasi Kapasitas yang tidak terpakai di lebih dari satu kolam instans, armada akan menentukan kolam tempat untuk meluncurkan Instans Sesuai Permintaan berdasarkan strategi alokasi Sesuai Permintaan.)

  Perhatikan bahwa Anda juga dapat menggunakan strategi alokasi `prioritized` alih-alih strategi alokasi `lowest-price`.

Reservasi Kapasitas

Akun tersebut memiliki 15 Reservasi Kapasitas yang tidak terpakai dalam 3 kolam yang berbeda. Jumlah Reservasi Kapasitas di setiap kolam ditunjukkan dengan `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
```

```
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Konfigurasi Armada

Konfigurasi armada berikut hanya menampilkan konfigurasi terkait untuk contoh ini. Total kapasitas target adalah 12, dan tipe kapasitas target default adalah `on-demand`. Strategi alokasi Sesuai Permintaan adalah `lowest-price`. Strategi penggunaan untuk Reservasi Kapasitas adalah `use-capacity-reservations-first`.

Dalam contoh ini, harga Instans Sesuai Permintaan adalah:

- `m5.large` – 0,096 USD per jam
- `m4.xlarge` – 0,20 USD per jam
- `m4.2xlarge` – 0,40 USD per jam

> **Note**
>
> Tipe armada harus bertipe `instant`. Tipe armada lainnya tidak mendukung `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
```

```
            },
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant"
}
```

Setelah Anda membuat armada `instant` menggunakan konfigurasi sebelumnya, 12 instans berikut diluncurkan untuk memenuhi kapasitas target:

- 5 Instans Sesuai Permintaan `m5.large` di `us-east-1a` – `m5.large` di `us-east-1a` merupakan harga terendah, dan terdapat 5 Reservasi Kapasitas `m5.large` yang tidak terpakai yang tersedia
- 5 Instans Sesuai Permintaan `m4.xlarge` di us-east-1a – `m4.xlarge` di `us-east-1a` merupakan harga terendah berikutnya, dan terdapat 5 Reservasi Kapasitas `m4.xlarge` yang tidak terpakai yang tersedia

- 2 Instans Sesuai Permintaan `m4.2xlarge` di us-east-1a – `m4.2xlarge` di `us-east-1a` merupakan harga terendah ketiga, dan terdapat 5 Reservasi Kapasitas `m4.2xlarge` yang hanya dibutuhkan 2 untuk memenuhi target kapasitas

Setelah armada diluncurkan, Anda dapat berlari describe-capacity-reservationsuntuk melihat berapa banyak Reservasi Kapasitas yang tidak terpakai yang tersisa. Dalam contoh ini, Anda akan melihat respons berikut, yang menunjukkan bahwa semua Reservasi Kapasitas `m5.large` dan `m4.xlarge` digunakan, dengan 3 Reservasi Kapasitas `m4.2xlarge` yang masih belum digunakan.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Contoh 5: Luncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas ketika total kapasitas target melebihi jumlah Reservasi Kapasitas yang tidak digunakan

Anda dapat mengonfigurasi armada agar menggunakan Reservasi Kapasitas Sesuai Permintaan terlebih dahulu saat meluncurkan Instans Sesuai Permintaan dengan mengatur strategi penggunaan untuk Reservasi Kapasitas ke `use-capacity-reservations-first`. Contoh ini juga menunjukkan cara armada memilih kolam instans tempat untuk meluncurkan Instans Sesuai Permintaan jika total kapasitas target melebihi jumlah Reservasi Kapasitas yang tidak terpakai yang tersedia.

Dalam contoh ini, konfigurasi armada adalah sebagai berikut:

- Kapasitas target: 16 Instans Sesuai Permintaan
- Total Reservasi Kapasitas yang tidak terpakai: 15 (kurang dari kapasitas target armada sebesar 16 Instans Sesuai Permintaan)
- Jumlah kolam Reservasi Kapasitas: 3 (`m5.large`, `m4.xlarge`, dan `m4.2xlarge`)
- Jumlah Reservasi Kapasitas per kolam: 5
- Strategi alokasi Sesuai Permintaan: `lowest-price` (Jika jumlah Reservasi Kapasitas yang tidak terpakai kurang dari kapasitas target Sesuai Permintaan, armada akan menentukan kolam tempat meluncurkan kapasitas Sesuai Permintaan yang tersisa berdasarkan strategi alokasi Sesuai Permintaan.)

  Perhatikan bahwa Anda juga dapat menggunakan strategi alokasi `prioritized` alih-alih strategi alokasi `lowest-price`.

Reservasi Kapasitas

Akun tersebut memiliki 15 Reservasi Kapasitas yang tidak terpakai dalam 3 kolam yang berbeda. Jumlah Reservasi Kapasitas di setiap kolam ditunjukkan dengan `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
```

```
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Konfigurasi Armada

Konfigurasi armada berikut hanya menampilkan konfigurasi terkait untuk contoh ini. Total kapasitas target adalah 16, dan tipe kapasitas target default adalah `on-demand`. Strategi alokasi Sesuai Permintaan adalah `lowest-price`. Strategi penggunaan untuk Reservasi Kapasitas adalah `use-capacity-reservations-first`.

Dalam contoh ini, harga Instans Sesuai Permintaan adalah:

- m5.large – 0,096 USD per jam
- m4.xlarge – 0,20 USD per jam
- m4.2xlarge – 0,40 USD per jam

> **Note**
>
> Tipe armada harus `instant`. Tipe armada lainnya tidak mendukung `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            },
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
```

```
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Setelah Anda membuat armada `instant` menggunakan konfigurasi sebelumnya, 16 instans berikut diluncurkan untuk memenuhi kapasitas target:

- 6 Instans Sesuai Permintaan `m5.large` di `us-east-1a` – `m5.large` di `us-east-1a` merupakan harga terendah, dan terdapat 5 Reservasi Kapasitas `m5.large` yang tidak terpakai yang tersedia. Reservasi Kapasitas digunakan terlebih dahulu untuk meluncurkan 5 Instans Sesuai Permintaan. Setelah sisa Reservasi Kapasitas `m4.xlarge` dan `m4.2xlarge` digunakan, untuk memenuhi kapasitas target, Instans Sesuai Permintaan tambahan diluncurkan sesuai dengan strategi alokasi Sesuai Permintaan, yaitu `lowest-price` dalam contoh ini.
- 5 Instans Sesuai Permintaan `m4.xlarge` di `us-east-1a` – `m4.xlarge` di `us-east-1a` merupakan harga terendah berikutnya, dan terdapat 5 Reservasi Kapasitas `m4.xlarge` yang tidak terpakai yang tersedia

- 5 Instans Sesuai Permintaan `m4.2xlarge` di `us-east-1a` – `m4.2xlarge` di `us-east-1a` merupakan harga terendah ketiga, dan terdapat 5 Reservasi Kapasitas `m4.2xlarge` yang tidak terpakai yang tersedia

Setelah armada diluncurkan, Anda dapat berlari describe-capacity-reservationsuntuk melihat berapa banyak Reservasi Kapasitas yang tidak terpakai yang tersisa. Dalam contoh ini, Anda akan melihat respons berikut, yang menunjukkan bahwa semua Reservasi Kapasitas di semua kolam telah digunakan.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Contoh 6: Luncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas yang ditargetkan

Anda dapat mengonfigurasi armada agar menggunakan Reservasi Kapasitas Sesuai Permintaan `targeted` terlebih dahulu saat meluncurkan Instans Sesuai Permintaan dengan mengatur strategi penggunaan untuk Reservasi Kapasitas ke `use-capacity-reservations-first`. Contoh ini menunjukkan cara meluncurkan Instans Sesuai Permintaan ke dalam Reservasi Kapasitas `targeted`, jika atribut Reservasi Kapasitas sama kecuali untuk Zona Ketersediaan (`us-east-1a` dan `us-east-1b`). Contoh ini juga menunjukkan cara armada memilih kolam instans tempat untuk meluncurkan Instans Sesuai Permintaan jika total kapasitas target melebihi jumlah Reservasi Kapasitas yang tidak terpakai yang tersedia.

Dalam contoh ini, konfigurasi armada adalah sebagai berikut:

- Kapasitas target: 10 Instans Sesuai Permintaan
- Total Reservasi Kapasitas `targeted` yang tidak terpakai: 6 (kurang dari kapasitas target Sesuai Permintaan armada sebesar 10 Instans Sesuai Permintaan)
- Jumlah kolam Reservasi Kapasitas: 2 (`us-east-1a` dan `us-east-1b`)
- Jumlah Reservasi Kapasitas per kolam: 3
- Strategi alokasi Sesuai Permintaan: `lowest-price` (Jika jumlah Reservasi Kapasitas yang tidak terpakai kurang dari kapasitas target Sesuai Permintaan, armada akan menentukan kolam tempat meluncurkan kapasitas Sesuai Permintaan yang tersisa berdasarkan strategi alokasi Sesuai Permintaan.)

  Perhatikan bahwa Anda juga dapat menggunakan strategi alokasi `prioritized` alih-alih strategi alokasi `lowest-price`.

Untuk panduan prosedur yang harus Anda lakukan untuk menyelesaikan contoh ini, lihat Tutorial: Konfigurasikan Armada EC2 untuk meluncurkan Instans Sesuai Permintaan menggunakan Reservasi Kapasitas yang ditargetkan.

Reservasi Kapasitas

Akun tersebut memiliki 6 Reservasi Kapasitas yang tidak terpakai dalam 2 kolam yang berbeda. Dalam contoh ini, kolam berbeda-beda menurut Zona Ketersediaannya. Jumlah Reservasi Kapasitas di setiap kolam ditunjukkan dengan `AvailableInstanceCount`.


```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
```

```
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Konfigurasi Armada

Konfigurasi armada berikut hanya menampilkan konfigurasi terkait untuk contoh ini. Total kapasitas target adalah 10, dan tipe kapasitas target default adalah `on-demand`. Strategi alokasi Sesuai Permintaan adalah `lowest-price`. Strategi penggunaan untuk Reservasi Kapasitas adalah `use-capacity-reservations-first`.

Dalam contoh ini, harga Instans Sesuai Permintaan untuk `c5.xlarge` di `us-east-1` adalah 0,17 USD per jam.

> **Note**
>
> Tipe armada harus `instant`. Tipe armada lainnya tidak mendukung `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
```

```
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Setelah Anda membuat armada `instant` menggunakan konfigurasi sebelumnya, 10 instans berikut diluncurkan untuk memenuhi kapasitas target:

- Reservasi Kapasitas digunakan terlebih dahulu untuk meluncurkan 6 Instans Sesuai Permintaan sebagai berikut:
  - 3 Instans Sesuai Permintaan diluncurkan ke dalam 3 Reservasi Kapasitas `c5.xlarge targeted` di `us-east-1a`
  - 3 Instans Sesuai Permintaan diluncurkan ke dalam 3 Reservasi Kapasitas `c5.xlarge targeted` di `us-east-1b`
- Untuk memenuhi kapasitas target, 4 Instans Sesuai Permintaan tambahan diluncurkan ke kapasitas Sesuai Permintaan reguler sesuai dengan strategi alokasi Sesuai Permintaan, yaitu `lowest-price` dalam contoh ini. Namun, karena kolam memiliki harga yang sama (karena harganya adalah per Wilayah dan bukan per Zona Ketersediaan), armada meluncurkan 4 Instans Sesuai Permintaan yang tersisa ke salah satu kolam.

Setelah armada diluncurkan, Anda dapat berlari describe-capacity-reservationsuntuk melihat berapa banyak Reservasi Kapasitas yang tidak terpakai yang tersisa. Dalam contoh ini, Anda akan melihat respons berikut, yang menunjukkan bahwa semua Reservasi Kapasitas di semua kolam telah digunakan.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}

{
```

```
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Contoh 7: Konfigurasikan Penyeimbangan Kembali Kapasitas untuk meluncurkan Instans Spot pengganti

Contoh berikut mengonfigurasi Armada EC2 untuk meluncurkan Instans Spot pengganti saat Amazon EC2 memancarkan rekomendasi penyeimbangan ulang untuk Instans Spot di armada. Untuk mengonfigurasi penggantian otomatis Instans Spot, untuk`ReplacementStrategy` , tentukan`launch-before-terminate` . Untuk mengonfigurasi penundaan waktu dari saat Instans Spot pengganti baru diluncurkan hingga saat Instans Spot lama dihapus secara otomatis, untuk `termination-delay`, tentukan nilai dalam detik. Untuk informasi selengkapnya, lihat Opsi konfigurasi.

> **Note**
>
> Sebaiknya gunakan `launch-before-terminate` hanya jika Anda dapat memprediksi lamanya prosedur pematian instans akan selesai sehingga instans lama hanya dihentikan setelah prosedur ini selesai. Anda dikenai biaya untuk semua instans saat semuanya berjalan.

Efektivitas strategi Penyeimbangan Ulang Kapasitas bergantung pada jumlah kolam kapasitas Spot yang ditentukan dalam permintaan Armada EC2. Sebaiknya konfigurasikan armada dengan set tipe instans dan Zona Ketersediaan yang beragam, dan untuk `AllocationStrategy`, tentukan `capacity-optimized`. Untuk informasi selengkapnya tentang hal-hal yang harus Anda pertimbangkan saat mengonfigurasi Armada EC2 untuk Penyeimbangan Ulang Kapasitas, lihat Gunakan Rebalancing Kapasitas di Armada EC2 dan Armada Spot untuk mengganti Instans Spot yang berisiko.

```
{
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
```

```
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                   ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Contoh 8: Luncurkan Instans Spot dalam armada yang dioptimalkan kapasitas

Contoh berikut menunjukkan cara mengonfigurasi Armada EC2 dengan strategi alokasi yang mengoptimalkan kapasitas. Untuk mengoptimalkan kapasitas, Anda harus mengatur `AllocationStrategy` ke `capacity-optimized`.

Pada contoh berikut ini, tiga spesifikasi peluncuran menentukan tiga kolam kapasitas Spot. Kapasitas target adalah 50 Instans Spot. Armada EC2 berupaya meluncurkan 50 Instans Spot ke kolam kapasitas Spot dengan kapasitas optimal untuk jumlah instans yang diluncurkan.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                 ]
          }
```

```
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Contoh 9: Luncurkan Instans Spot dalam armada yang dioptimalkan kapasitas dengan prioritas

Contoh berikut menunjukkan cara mengonfigurasi Armada EC2 dengan strategi alokasi Spot yang mengoptimalkan kapasitas sambil menggunakan prioritas dengan upaya terbaik.

Jika menggunakan strategi alokasi `capacity-optimized-prioritized`, Anda dapat menggunakan parameter `Priority` untuk menentukan prioritas kolam kapasitas Spot, yaitu makin rendah angkanya, makin tinggi prioritasnya. Anda juga dapat mengatur prioritas yang sama untuk beberapa kolam kapasitas Spot jika Anda menginginkannya setara. Jika Anda tidak menetapkan prioritas, kolam akan dianggap yang terakhir dalam hal prioritas.

Untuk memprioritaskan kolam kapasitas Spot, Anda harus mengatur `AllocationStrategy` ke `capacity-optimized-prioritized`. Armada EC2 akan mengoptimalkan kapasitas terlebih dahulu, tetapi akan mempertimbangkan prioritas dengan upaya terbaik (misalnya, jika mempertimbangkan prioritas tidak akan secara signifikan memengaruhi kemampuan Armada EC2 untuk menyediakan kapasitas optimal). Ini adalah pilihan opsi yang bagus untuk beban kerja di mana kemungkinan gangguan harus diminimalkan dan preferensi untuk tipe instans tertentu menjadi penting.

Pada contoh berikut ini, tiga spesifikasi peluncuran menentukan tiga kolam kapasitas Spot. Setiap kolam diprioritaskan, yaitu makin rendah jumlahnya, makin tinggi prioritasnya. Kapasitas target adalah 50 Instans Spot. Armada EC2 berupaya meluncurkan 50 Instans Spot ke dalam kolam kapasitas Spot dengan prioritas tertinggi menggunakan upaya terbaik, tetapi mengoptimalkan kapasitas terlebih dahulu.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
        {
```

```
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "Placement": {
                                "AvailabilityZone": "us-west-2a"
                            },
                        },
                         {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            },
                         },
                         {
                            "InstanceType": "c5.2xlarge",
                            "Priority": 3,
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            }
                         }
                    ]
             }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Contoh 10: Luncurkan Instans Spot di armada price-capacity-optimized

Contoh berikut menunjukkan cara mengonfigurasi Armada EC2 dengan strategi alokasi Spot yang mengoptimalkan kapasitas dan harga terendah. Untuk mengoptimalkan kapasitas sambil mempertimbangkan harga, Anda harus mengatur Spot `AllocationStrategy` ke `price-capacity-optimized`.

Pada contoh berikut ini, tiga spesifikasi peluncuran menentukan tiga kolam kapasitas Spot. Kapasitas target adalah 50 Instans Spot. Armada EC2 berupaya meluncurkan 50 Instans Spot ke kolam

kapasitas Spot dengan kapasitas optimal untuk jumlah instans yang diluncurkan sekaligus memilih kolam yang memiliki harga terendah.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                  ]
           }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
```

```
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Contoh 11: Konfigurasikan pemilihan tipe instans berbasis atribut

Contoh berikut menunjukkan cara mengonfigurasi Armada EC2 untuk menggunakan pemilihan tipe instans berbasis atribut untuk mengidentifikasi tipe instans. Untuk menentukan atribut instans yang diperlukan, Anda menentukan atribut dalam struktur `InstanceRequirements`.

Pada contoh berikut ini, dua atribut instans ditentukan:

- `VCpuCount`— Minimal 2 v CPUs ditentukan. Karena tidak ada jumlah maksimum yang ditentukan, maka tidak ada batas maksimum.
- `MemoryMiB` – Minimum 4 MiB memori ditentukan. Karena tidak ada jumlah maksimum yang ditentukan, maka tidak ada batas maksimum.

Setiap jenis instance yang memiliki 2 atau lebih v CPUs dan 4 MiB atau lebih memori akan diidentifikasi. Namun, perlindungan harga dan strategi alokasi mungkin akan mengecualikan beberapa tipe instans jika Armada EC2 menyediakan armada.

Untuk daftar dan deskripsi semua kemungkinan atribut yang dapat Anda tentukan, lihat InstanceRequirementsdi Referensi API Amazon EC2.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
```

```
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Contoh konfigurasi CLI Spot Fleet

Anda dapat menentukan konfigurasi Spot Fleet Anda dalam file JSON, dan kemudian referensi file tersebut menggunakan request-spot-fleet AWS CLI perintah untuk membuat armada Anda, sebagai berikut:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://file_name.json
```

Contoh berikut menggambarkan konfigurasi peluncuran untuk berbagai kasus penggunaan Armada Spot. Untuk informasi selengkapnya tentang parameter konfigurasi, lihat request-spot-fleet. Untuk informasi selengkapnya tentang membuat Armada Spot, lihatMembuat Armada Spot.

> **Note**
>
> Untuk Armada Spot, Anda tidak dapat menentukan ID antarmuka jaringan di templat peluncuran atau spesifikasi peluncuran. Pastikan Anda menghilangkan parameter `NetworkInterfaceID` di templat peluncuran atau spesifikasi peluncuran.

Contoh

- Contoh 1: Luncurkan Instans Spot menggunakan Availability Zone dengan harga terendah di Region
- Contoh 2: Luncurkan Instans Spot menggunakan Availability Zone dengan harga terendah dari daftar
- Contoh 3: Luncurkan Instans Spot menggunakan jenis instans dengan harga terendah dari daftar

- Contoh 4. Menimpa harga untuk permintaan
- Contoh 5: Meluncurkan Armada Spot menggunakan strategi alokasi yang terdiversifikasi
- Contoh 6: Meluncurkan Armada Spot menggunakan pembobotan instans
- Contoh 7: Luncurkan Armada Spot menggunakan kapasitas On-Demand
- Contoh 8: Mengonfigurasikan Penyeimbangan Ulang Kapasitas untuk meluncurkan Instans Spot pengganti
- Contoh 9: Meluncurkan Instans Spot dalam armada yang dioptimalkan kapasitas
- Contoh 10: Meluncurkan Instans Spot dalam armada yang dioptimalkan kapasitas dengan prioritas
- Contoh 11: Luncurkan Instans Spot di armada priceCapacityOptimized
- Contoh 12: Mengonfigurasi pemilihan tipe instans berbasis atribut

Contoh 1: Luncurkan Instans Spot menggunakan Availability Zone dengan harga terendah di Region

Contoh berikut menentukan spesifikasi peluncuran tunggal tanpa Zona Ketersediaan atau subnet. Armada Spot meluncurkan instans di Zona Ketersediaan dengan harga terendah yang memiliki subnet default. Harga yang Anda bayarkan tidak melebihi harga Sesuai Permintaan.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Contoh 2: Luncurkan Instans Spot menggunakan Availability Zone dengan harga terendah dari daftar

Contoh berikut menentukan dua spesifikasi peluncuran dengan Zona Ketersediaan atau subnet yang berbeda, tetapi dengan tipe instans dan AMI yang sama.

Zona Ketersediaan

Armada Spot meluncurkan instans di subnet default Zona Ketersediaan dengan harga terendah yang Anda tentukan.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "Placement": {
              "AvailabilityZone": "us-west-2a, us-west-2b"
          },
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Subnet

Anda dapat menentukan subnet default atau subnet non-default, dan subnet non-default dapat berasal dari VPC default atau VPC non-default. Layanan Spot meluncurkan instans di subnet mana pun yang berada di Zona Ketersediaan dengan harga terendah.

Anda tidak dapat menentukan subnet yang berbeda dari Zona Ketersediaan yang sama dalam permintaan Armada Spot.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Jika instance diluncurkan dalam VPC default, mereka menerima alamat IPv4 publik secara default. Jika instance diluncurkan dalam VPC nondefault, mereka tidak menerima alamat publik IPv4 secara default. Gunakan antarmuka jaringan dalam spesifikasi peluncuran untuk menetapkan IPv4 alamat publik ke instance yang diluncurkan di VPC nondefault. Saat Anda menentukan antarmuka jaringan, Anda harus menyertakan ID subnet dan ID grup keamanan menggunakan antarmuka jaringan.

```
  ...
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "InstanceType": "m3.medium",
          "NetworkInterfaces": [
              {
                  "DeviceIndex": 0,
                  "SubnetId": "subnet-1a2b3c4d",
                  "Groups": [ "sg-1a2b3c4d" ],
                  "AssociatePublicIpAddress": true
              }
          ],
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
```

```
            }
        }
    ...
```

Contoh 3: Luncurkan Instans Spot menggunakan jenis instans dengan harga terendah dari daftar

Contoh berikut menentukan dua konfigurasi peluncuran dengan tipe instans yang berbeda, tetapi dengan AMI dan Zona Ketersediaan atau subnet yang sama. Armada Spot meluncurkan instans menggunakan tipe instans yang ditentukan dengan harga terendah.

Zona Ketersediaan

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "Placement": {
            "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
```

```
}
```

Subnet

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Contoh 4. Menimpa harga untuk permintaan

Sebaiknya gunakan harga maksimum default, yaitu harga Sesuai Permintaan. Jika Anda memilih, Anda dapat menentukan harga maksimum untuk permintaan armada dan harga maksimum untuk spesifikasi peluncuran individu.

Contoh berikut menentukan harga maksimum untuk permintaan armada dan harga maksimum untuk dua dari tiga spesifikasi peluncuran. Harga maksimum permintaan armada digunakan untuk spesifikasi peluncuran apa pun yang tidak menentukan harga maksimum. Armada Spot meluncurkan instans menggunakan tipe instans dengan harga terendah.

Zona Ketersediaan

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
    ]
}
```

Subnet

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
```

```
            "SubnetId": "subnet-1a2b3c4d",
            "SpotPrice": "0.10"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.4xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "SpotPrice": "0.20"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Contoh 5: Meluncurkan Armada Spot menggunakan strategi alokasi yang terdiversifikasi

Contoh berikut menggunakan strategi alokasi `diversified`. Spesifikasi peluncuran memiliki tipe instans yang berbeda, tetapi AMI dan Zona Ketersediaan atau subnet yang sama. Armada Spot mendistribusikan 30 instans di tiga spesifikasi peluncuran, sehingga terdapat 10 instans untuk setiap tipe. Untuk informasi selengkapnya, lihat Gunakan strategi alokasi untuk menentukan bagaimana Armada EC2 atau Armada Spot memenuhi kapasitas Spot dan Sesuai Permintaan.

Zona Ketersediaan

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
```

```
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

Subnet

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Praktik terbaik untuk meningkatkan peluang permintaan spot dapat dipenuhi oleh kapasitas EC2 jika terjadi pemadaman di salah satu Zona Ketersediaan adalah dengan melakukan diversifikasi di seluruh zona. Untuk skenario ini, sertakan setiap Zona Ketersediaan yang tersedia untuk Anda dalam spesifikasi peluncuran. Selain itu, alih-alih menggunakan subnet yang sama setiap kalinya, gunakan tiga subnet unik (masing-masing memetakan ke zona yang berbeda).

Zona Ketersediaan

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2a"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2c"
          }
      }
  ]
}
```

Subnet

```
{
    "SpotPrice": "0.70",
```

```
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

Contoh 6: Meluncurkan Armada Spot menggunakan pembobotan instans

Contoh berikut menggunakan pembobotan instans, yang berarti harga adalah per unit jam, bukan per jam instans. Setiap konfigurasi peluncuran mencantumkan tipe instans yang berbeda dan bobot yang berbeda. Armada Spot memilih tipe instans dengan harga terendah per unit jam. Armada Spot menghitung jumlah Instans Spot yang akan diluncurkan dengan membagi kapasitas target dengan bobot instans. Jika hasilnya bukan bilangan bulat, Armada Spot akan membulatkannya ke bilangan bulat berikutnya, sehingga ukuran armada Anda tidak berada di bawah kapasitas targetnya.

Jika permintaan `r3.2xlarge` berhasil, Spot akan menyediakan 4 instans ini. Bagilah 20 dengan 6 untuk total 3,33 instans, lalu bulatkan menjadi 4 instans.

Jika permintaan `c3.xlarge` berhasil, Spot akan menyediakan 7 instans ini. Bagilah 20 dengan 3 untuk total 6,66 instans, lalu bulatkan menjadi 7 instans.

Untuk informasi selengkapnya, lihat Gunakan pembobotan instans untuk mengelola biaya dan kinerja Armada EC2 atau Armada Spot Anda.

Zona Ketersediaan

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 3
      }
    ]
}
```

Subnet

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 3
      }
```

```
  ]
}
```

Contoh 7: Luncurkan Armada Spot menggunakan kapasitas On-Demand

Untuk memastikan bahwa Anda selalu memiliki kapasitas instans, Anda dapat menyertakan permintaan kapasitas Sesuai Permintaan dalam permintaan Armada Spot. Jika terdapat kapasitas, permintaan Sesuai Permintaan akan selalu terpenuhi. Keseimbangan kapasitas target akan terpenuhi sebagai Spot jika terdapat kapasitas dan ketersediaan.

Contoh berikut menentukan kapasitas target yang diinginkan sebagai 10, yang 5 di antaranya harus merupakan kapasitas Sesuai Permintaan. Kapasitas spot tidak ditentukan; hal tersebut tersirat dalam keseimbangan kapasitas target dikurangi kapasitas Sesuai Permintaan. Amazon EC2 meluncurkan 5 unit kapasitas sebagai Sesuai Permintaan, dan 5 unit kapasitas (10-5 = 5) sebagai Spot jika tersedia kapasitas dan ketersediaan Amazon EC2.

```
{
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
```

```
}
```

Contoh 8: Mengonfigurasikan Penyeimbangan Ulang Kapasitas untuk meluncurkan Instans Spot pengganti

Contoh berikut mengonfigurasi Armada Spot untuk meluncurkan Instans Spot pengganti saat Amazon EC2 memancarkan rekomendasi penyeimbangan ulang untuk Instans Spot di armada. Untuk mengonfigurasi penggantian otomatis Instans Spot, untuk `ReplacementStrategy`, tentukan `launch-before-terminate`. Untuk mengonfigurasi waktu tunda dari peluncuran Instans Spot pengganti baru ke penghapusan otomatis Instans Spot lama, untuk `termination-delay`, tentukan nilai dalam hitungan detik. Untuk informasi selengkapnya, lihat Opsi konfigurasi.

> **Note**
>
> Sebaiknya gunakan `launch-before-terminate` hanya jika Anda dapat memprediksi lamanya prosedur pematian instans Anda akan selesai. Hal ini memastikan bahwa instans lama diakhiri hanya setelah prosedur pematian selesai. Anda dikenai biaya untuk semua instans saat semuanya berjalan.

Efektivitas strategi Penyeimbangan Ulang Kapasitas bergantung pada jumlah kolam kapasitas Spot yang ditentukan dalam permintaan Armada Spot. Sebaiknya konfigurasikan armada dengan set tipe instans dan Zona Ketersediaan yang beragam, dan untuk `AllocationStrategy`, tentukan `capacityOptimized`. Untuk informasi selengkapnya tentang hal-hal yang harus Anda pertimbangkan saat mengonfigurasi Armada Spot untuk Penyeimbangan Ulang Kapasitas, lihat Gunakan Rebalancing Kapasitas di Armada EC2 dan Armada Spot untuk mengganti Instans Spot yang berisiko.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
```

```
                },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                ]
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Contoh 9: Meluncurkan Instans Spot dalam armada yang dioptimalkan kapasitas

Contoh berikut menunjukkan cara mengonfigurasi Armada Spot dengan strategi alokasi Spot yang mengoptimalkan kapasitas. Untuk mengoptimalkan kapasitas, Anda harus mengatur `AllocationStrategy` ke `capacityOptimized`.

Pada contoh berikut ini, tiga spesifikasi peluncuran menentukan tiga kolam kapasitas Spot. Kapasitas target adalah 50 Instans Spot. Armada Spot berupaya meluncurkan 50 Instans Spot ke kolam kapasitas Spot dengan kapasitas optimal untuk jumlah instans yang diluncurkan.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                    "AvailabilityZone": "us-west-2a"
                },
                {
                    "InstanceType": "m4.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                },
                {
                    "InstanceType": "c5.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Contoh 10: Meluncurkan Instans Spot dalam armada yang dioptimalkan kapasitas dengan prioritas

Contoh berikut menunjukkan cara mengonfigurasi Armada Spot dengan strategi alokasi Spot yang mengoptimalkan kapasitas sambil menggunakan prioritas dengan upaya terbaik.

Jika menggunakan strategi alokasi `capacityOptimizedPrioritized`, Anda dapat menggunakan parameter `Priority` untuk menentukan prioritas kolam kapasitas Spot, yaitu makin rendah

angkanya, makin tinggi prioritasnya. Anda juga dapat mengatur prioritas yang sama untuk beberapa kolam kapasitas Spot jika Anda menginginkannya setara. Jika Anda tidak menetapkan prioritas, kolam akan dianggap yang terakhir dalam hal prioritas.

Untuk memprioritaskan kolam kapasitas Spot, Anda harus mengatur `AllocationStrategy` ke `capacityOptimizedPrioritized`. Armada Spot akan mengoptimalkan kapasitas terlebih dahulu, tetapi akan mempertimbangkan prioritas dengan upaya terbaik (misalnya, jika mempertimbangkan prioritas tidak akan secara signifikan memengaruhi kemampuan Armada Spot untuk menyediakan kapasitas optimal). Ini adalah pilihan opsi yang bagus untuk beban kerja di mana kemungkinan gangguan harus diminimalkan dan preferensi untuk tipe instans tertentu menjadi penting.

Pada contoh berikut ini, tiga spesifikasi peluncuran menentukan tiga kolam kapasitas Spot. Setiap kolam diprioritaskan, yaitu makin rendah jumlahnya, makin tinggi prioritasnya. Kapasitas target adalah 50 Instans Spot. Armada Spot berupaya meluncurkan 50 Instans Spot ke dalam kolam kapasitas Spot dengan prioritas tertinggi menggunakan upaya terbaik, tetapi mengoptimalkan kapasitas terlebih dahulu.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                   "Priority": 1,
                    "AvailabilityZone": "us-west-2a"
                },
                {
                          "InstanceType": "m4.2xlarge",
                          "Priority": 2,
                          "AvailabilityZone": "us-west-2b"
                },
                {
                          "InstanceType": "c5.2xlarge",
                          "Priority": 3,
```

```
                        "AvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Contoh 11: Luncurkan Instans Spot di armada priceCapacityOptimized

Contoh berikut menunjukkan cara mengonfigurasi Armada Spot dengan strategi alokasi Spot yang mengoptimalkan kapasitas dan harga terendah. Untuk mengoptimalkan kapasitas sambil mempertimbangkan harga, Anda harus mengatur Spot `AllocationStrategy` ke `priceCapacityOptimized`.

Pada contoh berikut ini, tiga spesifikasi peluncuran menentukan tiga kolam kapasitas Spot. Kapasitas target adalah 50 Instans Spot. Armada Spot berupaya meluncurkan 50 Instans Spot ke kolam kapasitas Spot dengan kapasitas optimal untuk jumlah instans yang diluncurkan sekaligus memilih kolam yang memiliki harga terendah.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                      {
                           "InstanceType": "m4.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                      },
                      {
```

```
                        "InstanceType": "c5.2xlarge",
                        "AvailabilityZone": "us-west-2b"
                    }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Contoh 12: Mengonfigurasi pemilihan tipe instans berbasis atribut

Contoh berikut menunjukkan cara mengonfigurasi Armada Spot untuk menggunakan pemilihan tipe instans berbasis atribut untuk mengidentifikasi tipe instans. Untuk menentukan atribut instans yang diperlukan, Anda menentukan atribut dalam struktur `InstanceRequirements`.

Pada contoh berikut ini, dua atribut instans ditentukan:

- `VCpuCount`— Minimal 2 v CPUs ditentukan. Karena tidak ada jumlah maksimum yang ditentukan, maka tidak ada batas maksimum.
- `MemoryMiB` – Minimum 4 MiB memori ditentukan. Karena tidak ada jumlah maksimum yang ditentukan, maka tidak ada batas maksimum.

Setiap jenis instance yang memiliki 2 atau lebih v CPUs dan 4 MiB atau lebih memori akan diidentifikasi. Namun, perlindungan harga dan strategi alokasi mungkin akan mengecualikan beberapa tipe instans jika Armada Spot menyediakan armada.

Untuk daftar dan deskripsi semua kemungkinan atribut yang dapat Anda tentukan, lihat InstanceRequirementsdi Referensi API Amazon EC2.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
```

```
    "InstanceRequirements": {
     "VCpuCount": {
      "Min": 2
     },
     "MemoryMiB": {
      "Min": 4
     }
    }
   }]
  }]
}
```

Kuota untuk Armada EC2 dan Armada Spot

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah.

Kuota Amazon EC2 biasa berlaku untuk instans yang diluncurkan oleh Armada EC2 atau Armada Spot, seperti batas Instans Spot dan batas volume.

Selain itu, Anda Akun AWS memiliki kuota berikut yang terkait dengan Armada EC2 dan Armada Spot:

Deskripsi kuota	Kuota
Jumlah Armada EC2 dan Armada Spot per Wilayah jenis `maintain` dan `request` diactive,, `deleted_running` dan negara bagian `cancelled_running`	1,000 [1] [2] [3]
Jumlah Armada EC2 tipe `instant`	Tidak terbatas.
Jumlah kumpulan kapasitas Spot (kombinasi unik dari tipe instans dan subnet) untuk Armada EC2 dan Armada Spot jenis dan `maintain` `request`	300 [1]
Jumlah kumpulan kapasitas Spot (kombinasi unik dari tipe instans dan subnet) untuk jenis Armada EC2 `instant`	Tidak terbatas.

Deskripsi kuota	Kuota
Ukuran data pengguna dalam spesifikasi peluncuran	16 KB ²
Kapasitas target per Armada EC2 atau Armada Spot	10.000
Kapasitas target di semua Armada EC2 dan Armada Spot di suatu Wilayah	100.000 ¹
Permintaan Armada EC2 atau permintaan Armada Spot tidak dapat menjangkau Wilayah.	
Permintaan Armada EC2 atau permintaan Armada Spot tidak dapat menjangkau subnet yang berbeda dari Zona Ketersediaan yang sama.	

¹ Kuota ini berlaku untuk Armada EC2 dan Armada Spot Anda.

² Kuota ini merupakan kuota hard. Anda tidak dapat meminta kenaikan untuk kuota ini.

³ Setelah Anda menghapus Armada EC2 atau membatalkan permintaan Armada Spot, dan jika Anda menentukan bahwa armada tidak boleh mengakhiri Instans Spot-nya saat Anda menghapus atau membatalkan permintaan, permintaan armada akan memasuki status `deleted_running` (Armada EC2) atau `cancelled_running` (Armada Spot) dan instans terus berjalan hingga terinterupsi atau Anda mengakhirinya secara manual. Jika Anda menghentikan instans, permintaan armada akan memasuki status `deleted_terminating` (Armada EC2) atau `cancelled_terminating` (Armada Spot) dan tidak dihitung dalam kuota ini. Untuk informasi selengkapnya, lihat Menghapus permintaan Armada EC2 dan instans di armada dan Membatalkan (menghapus) permintaan Armada Spot.

Meminta peningkatan kuota untuk kapasitas target

Jika Anda membutuhkan lebih dari kuota default untuk kapasitas target, Anda dapat meminta peningkatan kuota.

Untuk meminta peningkatan kuota pada kapasitas target

1. Buka formulir Dukungan Center Create case.
2. Pilih Peningkatan batas layanan.
3. Untuk Tipe batas, pilih Armada EC2.
4. Untuk Wilayah, pilih AWS Wilayah tempat permintaan kenaikan kuota.
5. Untuk Batas, pilih Kapasitas Armada Target per Armada (dalam unit) atau Kapasitas Armada Target per Wilayah (dalam unit), bergantung pada kuota yang ingin Anda tingkatkan.
6. Untuk Nilai batas baru, masukkan nilai kuota baru.
7. Untuk meminta peningkatan kuota lain, pilih Tambahkan permintaan lain, dan ulangi Langkah 4–6.
8. Untuk Deskripsi kasus penggunaan, masukkan alasan Anda meminta peningkatan kuota.
9. Di Opsi kontak, tentukan bahasa kontak dan metode kontak pilihan Anda.
10. Pilih Kirim.

Jaringan di Amazon EC2

Amazon VPC memungkinkan Anda meluncurkan AWS sumber daya, seperti instans Amazon EC2, ke dalam jaringan virtual yang didedikasikan untuk akun AWS Anda, yang dikenal sebagai virtual private cloud (VPC). Saat Anda meluncurkan sebuah instans, Anda dapat memilih subnet dari VPC. Instans dikonfigurasi dengan antarmuka jaringan primer, yang merupakan kartu jaringan virtual logis. Instance menerima alamat IP pribadi utama dari IPv4 alamat subnet, dan ditugaskan ke antarmuka jaringan utama.

Anda dapat mengendalikan apakah instans menerima alamat IP publik dari kumpulan alamat IP publik Amazon. Alamat IP publik dari sebuah instans dikaitkan dengan instans Anda hanya sampai dihentikan atau diakhiri. Jika Anda memerlukan alamat IP publik persisten, Anda dapat mengalokasikan alamat IP Elastis untuk AWS akun Anda dan mengaitkannya dengan instance atau antarmuka jaringan. Alamat IP Elastis tetap terkait dengan AWS akun Anda sampai Anda melepaskannya, dan Anda dapat memindahkannya dari satu instance ke yang lain sesuai kebutuhan. Anda dapat membawa rentang alamat IP Anda sendiri ke akun AWS Anda, di mana muncul sebagai kumpulan alamat, dan kemudian mengalokasikan alamat IP elastis dari kumpulan alamat Anda.

Untuk meningkatkan performa jaringan dan mengurangi latensi, Anda dapat meluncurkan instans dalam grup penempatan. Anda bisa mendapatkan performa paket per detik (PPS) yang jauh lebih tinggi menggunakan jaringan yang ditingkatkan. Anda dapat mempercepat komputasi performa tinggi dan aplikasi machine learning menggunakan Elastic Fabric Adapter (EFA), yang merupakan perangkat jaringan yang dapat Anda pasang ke tipe instans yang didukung.

Fitur

- Wilayah dan Zona
- Pengalamatan IP instans Amazon EC2
- Nama host dan domain instans EC2
- Bawa alamat IP Anda sendiri (BYOIP) ke Amazon EC2
- Alamat Elastic IP
- Antarmuka jaringan elastis
- Bandwidth jaringan EC2 instans Amazon
- Jaringan yang disempurnakan di EC2 instans Amazon
- Adaptor Kain Elastis untuk AI/ML dan beban kerja HPC di Amazon EC2

- Topologi Amazon EC2
- Grup penempatan untuk EC2 instans Amazon Anda
- Unit transmisi maksimum jaringan (MTU) untuk instans Anda EC2
- Virtual private cloud untuk EC2 instans Anda
- Jaringan Sekunder

Wilayah dan Zona

Amazon EC2 di-host di berbagai lokasi di seluruh dunia. Lokasi ini terdiri dari Wilayah AWS, Availability Zones, Local Zones AWS Outposts, dan Wavelength Zones.

- Wilayah adalah wilayah geografis yang terpisah.
- Availability Zone adalah beberapa lokasi yang terisolasi di setiap Wilayah.
- Local Zones memberi Anda kemampuan untuk menempatkan sumber daya, seperti komputasi dan penyimpanan, di beberapa lokasi yang lebih dekat dengan pengguna akhir Anda.
- Wavelength Zones memberi Anda kemampuan untuk membangun aplikasi yang memberikan latensi ultra-rendah ke perangkat 5G dan pengguna akhir. Wavelength menyebarkan layanan komputasi dan penyimpanan AWS standar ke tepi jaringan 5G operator telekomunikasi.
- AWS Outpostsmenghadirkan AWS layanan asli, infrastruktur, dan model operasi ke hampir semua pusat data, ruang kolokasi, atau fasilitas lokal.

AWS beroperasi state-of-the-art, pusat data yang sangat tersedia. Meskipun jarang terjadi, kegagalan dapat terjadi yang memengaruhi ketersediaan instans yang berada di lokasi yang sama. Jika Anda meng-host semua instans Anda di satu lokasi yang dipengaruhi oleh kegagalan, tidak ada instans Anda yang akan tersedia.

Untuk informasi lebih lanjut, lihat AWS Infrastruktur Global.

Daftar Isi

- Wilayah
- Zona Ketersediaan
- Zona Lokal
- Wavelength Zones
- AWS Outposts

Wilayah

Setiap Wilayah dirancang untuk diisolasi dari Wilayah lainnya. Ini mencapai toleransi kesalahan dan stabilitas sebesar mungkin.

Saat meluncurkan instans, pilih Wilayah yang menempatkan instans Anda dekat dengan pelanggan tertentu, atau yang memenuhi persyaratan hukum atau persyaratan lain yang Anda miliki. Anda dapat meluncurkan instance di beberapa Wilayah.

Saat melihat sumber daya, Anda hanya melihat sumber daya yang terkait dengan Wilayah yang Anda tentukan. Hal ini karena Wilayah terisolasi dari satu sama lain dan kami tidak mereplikasi sumber daya di seluruh Wilayah secara otomatis.

Wilayah yang Tersedia

Untuk daftar Wilayah yang tersedia, lihat AWS Wilayah.

Titik akhir regional untuk Amazon EC2

Saat Anda bekerja dengan sebuah instans menggunakan antarmuka baris perintah atau tindakan API, Anda harus menentukan titik akhir Wilayah. Untuk informasi selengkapnya tentang Wilayah dan titik akhir Amazon EC2, lihat titik akhir EC2 layanan Amazon di Panduan EC2 Pengembang Amazon.

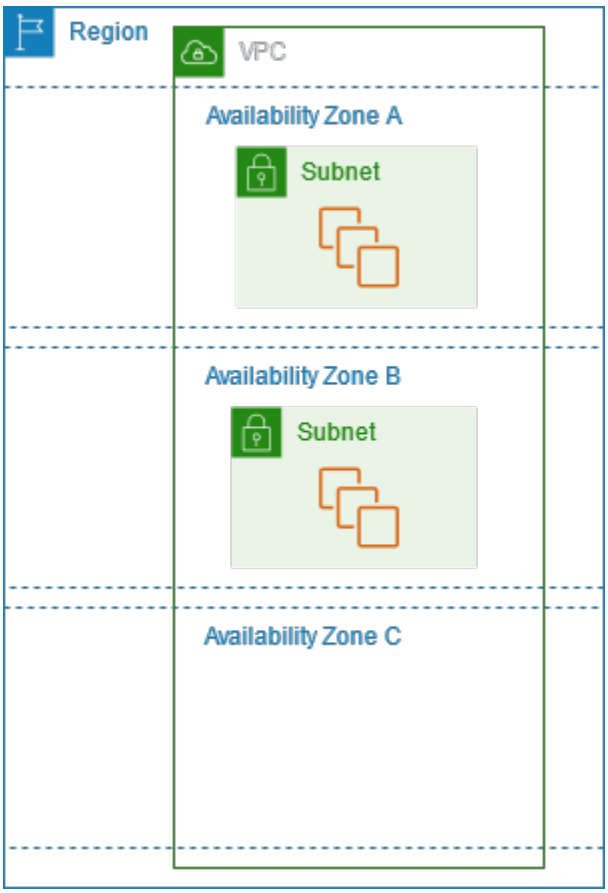
Untuk informasi selengkapnya, lihat Wilayah AWSdi Panduan Pengguna Wilayah AWS dan Availability Zones.

Zona Ketersediaan

Setiap Wilayah memiliki beberapa lokasi terisolasi yang dikenal sebagai Zona Ketersediaan. Kode untuk Availability Zone adalah kode Region diikuti oleh pengidentifikasi huruf. Misalnya, `us-east-1a`.

Dengan meluncurkan EC2 instans di beberapa Availability Zone, Anda dapat melindungi aplikasi Anda dari kegagalan satu lokasi di Wilayah.

Diagram berikut menggambarkan beberapa Availability Zone di suatu AWS Wilayah. Availability Zone A dan Availability Zone B masing-masing memiliki satu subnet, dan setiap subnet memiliki EC2 instance. Zona Ketersediaan C tidak memiliki subnet, oleh karena itu Anda tidak dapat meluncurkan instans ke Zona Ketersediaan ini.



Untuk informasi selengkapnya, lihat Virtual private cloud untuk EC2 instans Anda.

Zona Ketersediaan menurut Wilayah

Untuk daftar Availability Zone menurut Wilayah, lihat AWS Availability Zone.

Contoh di Availability Zone

Saat meluncurkan instance, Anda memilih Region dan virtual private cloud (VPC). Kemudian, Anda dapat memilih subnet dari salah satu Availability Zones atau biarkan kami memilih subnet untuk Anda. Ketika Anda meluncurkan instans awal Anda, kami sarankan Anda mengizinkan kami memilih Availability Zone untuk Anda berdasarkan kesehatan sistem dan kapasitas yang tersedia. Jika Anda meluncurkan instance tambahan, tentukan Availability Zone hanya jika instance baru Anda harus dekat, atau terpisah dari, instans yang ada.

Jika Anda mendistribusikan instance di beberapa Availability Zone dan sebuah instance gagal, Anda dapat mendesain aplikasi sehingga instance di Availability Zone lain akan menangani permintaan.

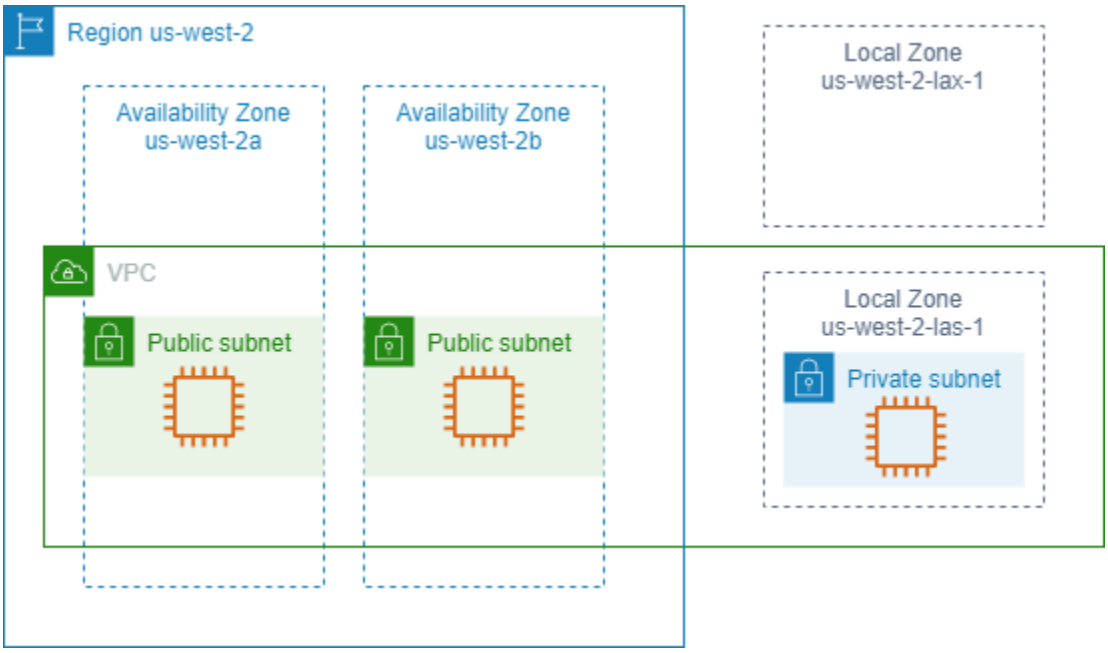
Untuk informasi selengkapnya, lihat AWS Availability Zone di Panduan Pengguna Wilayah AWS dan Availability Zones.

Zona Lokal

Zona Lokal adalah perpanjangan dari AWS Wilayah dalam kedekatan geografis dengan pengguna Anda. Local Zones memiliki koneksi sendiri ke internet dan dukungan Direct Connect, sehingga sumber daya yang dibuat di Local Zone dapat melayani pengguna lokal dengan komunikasi latensi rendah. Untuk informasi selengkapnya, lihat Apa itu AWS Local Zones? di Panduan Pengguna AWS Local Zones.

Kode untuk Local Zones adalah kode Wilayah diikuti oleh pengidentifikasi yang menunjukkan lokasi fisiknya. Misalnya, `us-west-2-lax-1` di Los Angeles.

Diagram berikut menggambarkan AWS Wilayah`us-west-2`, dua dari Availability Zone-nya, dan dua Local Zones-nya. VPC mencakup Zona Ketersediaan dan salah satu Local Zones. Setiap zona di VPC memiliki satu subnet, dan setiap subnet memiliki instans.



Local Zones yang Tersedia

Untuk daftar Local Zones yang tersedia, lihat Available Local Zones di Panduan Pengguna AWS Local Zones. Untuk daftar Local Zones yang diumumkan, lihat lokasi AWS Local Zones.

Contoh di Local Zones

Untuk menggunakan Local Zones, Anda harus mengaktifkannya terlebih dahulu. Kemudian, buat subnet di Local Zone. Anda dapat menentukan subnet Zona Lokal saat meluncurkan instance, yang menempatkannya di subnet Zona Lokal di Zona Lokal.

Saat meluncurkan instance di Local Zone, Anda juga mengalokasikan alamat IP dari grup perbatasan jaringan. Grup perbatasan jaringan adalah kumpulan unik Availability Zones, Local Zones, atau Wavelength Zones dari AWS mana mengiklankan alamat IP, misalnya,. `us-west-2-lax-1a` Anda dapat mengalokasikan alamat IP berikut dari grup batas jaringan:

- Alamat Elastis yang disediakan Amazon IPv4
- Alamat IPv6 VPC yang disediakan Amazon (hanya tersedia di zona Los Angeles)

Untuk informasi selengkapnya tentang cara meluncurkan instance di Zona Lokal, lihat Memulai AWS Local Zones di Panduan Pengguna AWS Local Zones.

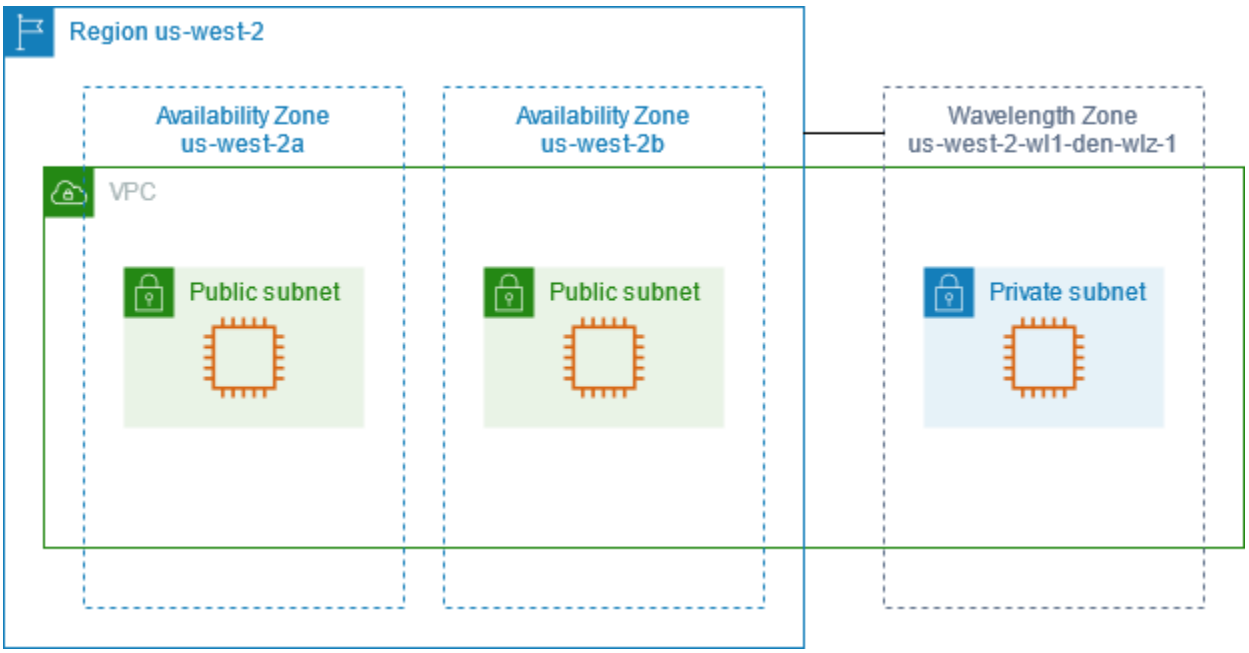
Wavelength Zones

AWS Wavelength memungkinkan pengembang untuk membangun aplikasi yang memberikan latensi ultra-rendah ke perangkat seluler dan pengguna akhir. Wavelength menyebarkan layanan komputasi dan penyimpanan AWS standar ke tepi jaringan 5G operator telekomunikasi. Pengembang dapat memperluas virtual private cloud (VPC) ke satu atau beberapa Wavelength Zone, dan kemudian menggunakan sumber daya AWS seperti EC2 instans Amazon untuk menjalankan aplikasi yang memerlukan latensi ultra-rendah dan koneksi ke layanan di Wilayah. AWS

Zona Panjang Gelombang adalah zona terisolasi di lokasi pembawa tempat infrastruktur panjang gelombang digunakan. Wavelength Zone terikat pada suatu Wilayah. Zona Panjang Gelombang adalah perpanjangan logis dari Wilayah, dan dikelola oleh bidang kontrol di Wilayah.

Kode untuk Wavelength Zone adalah kode Wilayah diikuti oleh pengidentifikasi yang menunjukkan lokasi fisik. Misalnya, `us-east-1-wl1-bos-wlz-1` di Boston.

Diagram berikut menggambarkan AWS Wilayah`us-west-2`, dua Zona Ketersediaan, dan Zona Wavelength. VPC mencakup Zona Ketersediaan dan Wavelength Zone. Setiap zona di VPC memiliki satu subnet, dan setiap subnet memiliki instans.



Wavelength Zones tidak tersedia di setiap Wilayah. Untuk informasi tentang Wilayah yang mendukung Wavelength Zones, lihat Wavelength Zones yang Tersedia di Panduan Developer AWS Wavelength .

Zona Wavelength yang Tersedia

Untuk daftar Zona Wavelength yang tersedia, lihat Zona Wavelength yang Tersedia di Panduan.AWS Wavelength

Contoh di Zona Wavelength

Untuk menggunakan Wavelength Zone, Anda harus terlebih dahulu memilih Zona. Kemudian, buat subnet di Wavelength Zone. Anda dapat menentukan subnet Wavelength saat meluncurkan instance. Anda juga mengalokasikan alamat IP operator dari grup batas jaringan, yang merupakan kumpulan unik dari Zona Ketersediaan, Local Zones, atau Wavelength Zone tempat AWS mengiklankan alamat IP, misalnya, `us-east-1-wl1-bos-wlz-1`.

Untuk step-by-step petunjuk arah untuk meluncurkan instance di Wavelength Zone, lihat AWS Wavelength Memulai di Panduan Pengembang.AWS Wavelength

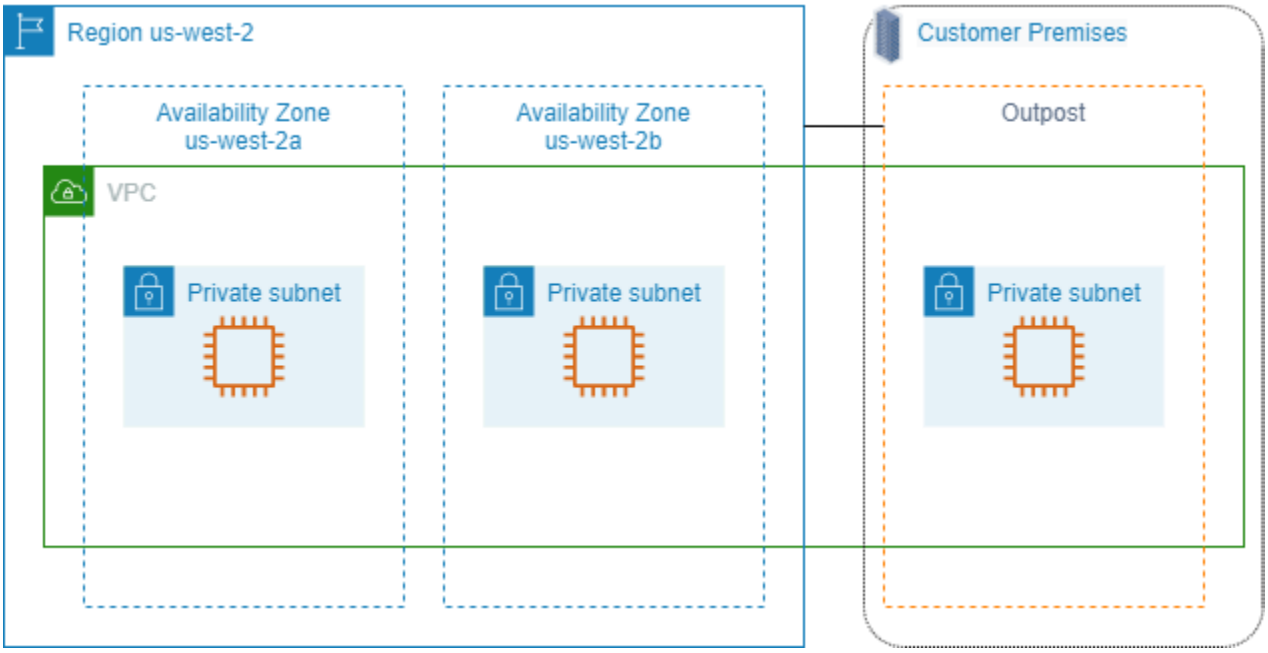
AWS Outposts

AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, layananAPIs, dan alat ke tempat pelanggan. Dengan menyediakan akses lokal ke infrastruktur AWS

terkelola, AWS Outposts memungkinkan pelanggan untuk membangun dan menjalankan aplikasi di tempat menggunakan antarmuka pemrograman yang sama seperti di AWS Wilayah, sambil menggunakan sumber daya komputasi dan penyimpanan lokal untuk latensi yang lebih rendah dan kebutuhan pemrosesan data lokal.

Outpost adalah kumpulan kapasitas AWS komputasi dan penyimpanan yang digunakan di situs pelanggan. AWS mengoperasikan, memantau, dan mengelola kapasitas ini sebagai bagian dari suatu AWS Wilayah. Anda dapat membuat subnet di Outpost Anda dan menentukannya saat Anda membuat AWS sumber daya. Instance dalam subnet Outpost berkomunikasi dengan instans lain di AWS Wilayah menggunakan alamat IP pribadi, semuanya dalam VPC yang sama.

Diagram berikut menggambarkan AWS Wilayah`us-west-2`, dua Zona Ketersediaan, dan Pos Terdepan. VPC mencakup Zona Ketersediaan dan Outpost. Outpost berada di pusat data pelanggan on-premise. Setiap zona di VPC memiliki satu subnet, dan setiap subnet memiliki instans.



Contoh di Pos Terdepan

Untuk mulai menggunakan AWS Outposts, Anda harus membuat Outpost dan memesan kapasitas Outpost. AWS Outposts menawarkan dua faktor bentuk, Outposts rack dan Outposts server. Untuk informasi selengkapnya tentang konfigurasi Outposts, lihat Keluarga.AWS Outposts Setelah peralatan Outpost Anda diinstal, kapasitas komputasi dan penyimpanan tersedia untuk Anda saat Anda meluncurkan EC2 instans di Outpost Anda.

Untuk meluncurkan EC2 instance, Anda harus membuat subnet Outpost. Grup keamanan mengontrol lalu lintas masuk dan keluar untuk instance di subnet Outpost, seperti yang mereka lakukan

untuk instance di subnet Availability Zone. Untuk menyambung ke instance di subnet Outpost menggunakan SSH, tentukan key pair saat Anda meluncurkannya, seperti yang Anda lakukan untuk instance di subnet Availability Zone.

Untuk informasi selengkapnya, lihat Memulai Rak Outposts atau Memulai server Outposts.

Volume di rak Outposts

Jika kapasitas komputasi Outposts Anda ada di rak Outpost, Anda dapat membuat volume EBS di subnet Outpost yang Anda buat. Saat Anda membuat volume, tentukan Amazon Resource Name (ARN) dari Outpost.

Perintah buat volume berikut membuat volume kosong 50 GB di Pos terdepan yang ditentukan.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Anda dapat secara dinamis mengubah ukuran volume gp2 Amazon EBS Anda tanpa melepaskan mereka. Untuk informasi selengkapnya tentang memodifikasi volume tanpa melepaskannya, lihat Meminta modifikasi pada volume EBS Anda di Panduan Pengguna Amazon EBS.

Kami menyarankan Anda membatasi volume root untuk instance pada rak Outpost hingga 30 GiB atau lebih kecil. Anda dapat menentukan volume data dalam pemetaan perangkat blok dari AMI atau instans untuk menyediakan penyimpanan tambahan. Untuk memangkas blok yang tidak terpakai dari volume boot, lihat Cara Membangun Volume EBS yang jarang di Blog Jaringan AWS Mitra.

Kami menyarankan Anda meningkatkan NVMe batas waktu untuk volume root. Untuk informasi selengkapnya, lihat batas waktu operasi I/O di Panduan Pengguna Amazon EBS.

Volume di server Outposts

Instans di server Outposts menyediakan volume penyimpanan instans tetapi tidak mendukung volume EBS. Pilih AMI yang didukung Amazon EBS-backed hanya dengan satu snapshot EBS. Pilih ukuran instans dengan penyimpanan instans yang cukup untuk memenuhi kebutuhan aplikasi Anda. Lihat informasi yang lebih lengkap di Batas volume penyimpanan instans.

Pengalamatan IP instans Amazon EC2

Amazon EC2 dan Amazon VPC mendukung protokol pengalamatan dan IPv4 pengalamatan. IPv6 Secara default, Amazon VPC menggunakan protokol IPv4 pengalamatan; Anda tidak dapat

menonaktifkan perilaku ini. Saat Anda membuat VPC, Anda harus menentukan blok IPv4 CIDR (berbagai alamat pribadi IPv4). Anda dapat secara opsional menetapkan blok IPv6 CIDR ke VPC Anda dan menetapkan IPv6 alamat dari blok itu ke instance di subnet Anda.

Saat meluncurkan instans EC2, Anda menentukan VPC dan subnet. Instance menerima alamat IPv4 pribadi dari rentang CIDR subnet. Anda dapat mengonfigurasi instans secara opsional dengan alamat IPv4 publik dan alamat IPv6. Jika instans EC2 dalam VPCs komunikasi yang berbeda menggunakan alamat IP publik, lalu lintas tetap berada di jaringan global AWS pribadi dan tidak melintasi internet publik.

Daftar Isi

- IPv4 Alamat pribadi
- IPv4 Alamat publik
- Optimalisasi IPv4 alamat publik
- IPv6 alamat
- Beberapa alamat IP
- Nama host instans EC2
- Alamat link-lokal
- Kelola alamat IPv4 untuk instans EC2 Anda
- Kelola alamat IPv6 untuk instans EC2 Anda
- Alamat IP sekunder untuk instans EC2 Anda
- Konfigurasikan IPv4 alamat pribadi sekunder untuk instance Windows

IPv4 Alamat pribadi

IPv4 Alamat pribadi adalah alamat IP yang tidak dapat dijangkau melalui Internet. Anda dapat menggunakan IPv4 alamat pribadi untuk komunikasi antar instance di VPC yang sama. Untuk informasi lebih lanjut tentang standar dan spesifikasi IPv4 alamat pribadi, lihat RFC 1918. Kami mengalokasikan IPv4 alamat pribadi untuk instance menggunakan DHCP.

> **Note**
>
> Anda dapat membuat VPC dengan blok CIDR yang dapat dirutekan secara publik yang berada di luar rentang IPv4 alamat pribadi yang ditentukan dalam RFC 1918. Namun, untuk

keperluan dokumentasi ini, kami merujuk ke IPv4 alamat pribadi (atau 'alamat IP pribadi') sebagai alamat IP yang berada dalam IPv4 kisaran CIDR VPC Anda.

Subnet VPC dapat berupa salah satu tipe dari berikut ini:

- IPv4-hanya subnet — Anda hanya dapat membuat sumber daya di subnet ini dengan IPv4 alamat yang ditetapkan untuk mereka.
- IPv6-hanya subnet — Anda hanya dapat membuat sumber daya di subnet ini dengan IPv6 alamat yang ditetapkan untuk mereka.
- IPv4 dan IPv6 subnet — Anda dapat membuat sumber daya di subnet ini dengan salah satu IPv4 atau IPv6 alamat yang ditetapkan untuk mereka.

Saat Anda meluncurkan instans EC2 ke subnet IPv4 -only atau dual stack (IPv4 dan IPv6), instance menerima alamat IP pribadi utama dari rentang IPv4 alamat subnet. Untuk informasi selengkapnya, lihat ACL Jaringan di Panduan Pengguna Amazon VPC. Jika Anda tidak menentukan alamat IP pribadi utama saat Anda meluncurkan instans, kami akan memilih alamat IP yang tersedia di rentang subnet IPv4 untuk Anda. Setiap instance memiliki antarmuka jaringan default (indeks 0) yang diberi IPv4 alamat pribadi utama. Anda juga dapat menentukan IPv4 alamat pribadi tambahan, yang dikenal sebagai IPv4 alamat pribadi sekunder. Tidak seperti alamat IP privat primer, alamat IP privat sekunder dapat ditetapkan ulang dari satu instans ke instans lainnya. Untuk informasi selengkapnya, lihat Beberapa alamat IP.

IPv4 Alamat pribadi, terlepas dari apakah itu alamat primer atau sekunder, tetap terkait dengan antarmuka jaringan ketika instance dihentikan dan dimulai, atau hibernasi dan dimulai, dan dirilis ketika instance dihentikan.

IPv4 Alamat publik

Alamat IP publik adalah IPv4 alamat yang dapat dijangkau dari Internet. Anda dapat menggunakan alamat publik untuk komunikasi antara instans Anda dan Internet.

Saat Anda meluncurkan sebuah instans di VPC default, kami menetapkannya sebagai alamat IP publik secara default. Saat Anda meluncurkan instance ke VPC nondefault, subnet memiliki atribut yang menentukan apakah instance yang diluncurkan ke subnet tersebut menerima alamat IP publik dari kumpulan alamat publik. IPv4 Secara default, kami tidak menetapkan alamat IP publik ke instans yang diluncurkan di subnet non-default.

Anda dapat mengontrol apakah instans Anda menerima alamat IP publik sebagai berikut:

- Ubah atribut pengalamatan IP publik dari subnet Anda. Untuk informasi selengkapnya, lihat Memodifikasi atribut IPv4 pengalamatan publik untuk subnet Anda di Panduan Pengguna Amazon VPC.
- Aktifkan atau nonaktifkan fitur pengalamatan IP publik selama peluncuran. Ini mengesampingkan atribut pengalamatan IP publik subnet. Untuk informasi selengkapnya, lihat Tetapkan IPv4 alamat publik saat peluncuran.
- Hapus penetapan alamat IP publik dari instans Anda setelah peluncuran. Untuk informasi selengkapnya, lihat the section called “Mengelola alamat IP”.

Alamat IP publik ditetapkan ke instans Anda dari kumpulan IPv4 alamat publik Amazon, dan tidak terkait dengan AWS akun Anda. Ketika alamat IP publik dipisahkan dari instans Anda, itu dilepaskan kembali ke kumpulan IPv4 alamat publik, dan Anda tidak dapat menggunakannya kembali.

Kami merilis alamat IP publik dari instans Anda dan menetapkan yang baru dalam kasus berikut:

- Kami merilis alamat IP publik ketika instance dihentikan, hibernasi, atau dihentikan. Kami menetapkan alamat IP publik baru ketika Anda memulai instans berhenti atau hibernasi.
- Kami merilis alamat IP publik saat Anda mengaitkan alamat IP Elastis dengan instance. Kami menetapkan alamat IP publik baru saat Anda memisahkan alamat IP Elastis dari instans Anda.
- Jika kami merilis alamat IP publik dari instans Anda dan memiliki antarmuka jaringan sekunder, kami tidak menetapkan alamat IP publik baru.
- Jika kami merilis alamat IP publik instans Anda dan memiliki alamat IP pribadi sekunder yang terkait dengan alamat IP Elastis, kami tidak menetapkan alamat IP publik baru.

Jika Anda memerlukan alamat IP publik yang persisten yang dapat dikaitkan dengan dan dari instans sesuai kebutuhan, gunakan alamat IP Elastis.

Jika Anda menggunakan DNS dinamis untuk memetakan nama DNS yang ada ke alamat IP publik instans baru, mungkin perlu waktu hingga 24 jam agar alamat IP tersebut tersebar melalui Internet. Akibatnya, instans baru mungkin tidak menerima traffic sedangkan instans yang dihentikan terus menerima permintaan. Untuk mengatasi masalah ini, gunakan alamat IP Elastis. Anda dapat mengalokasikan alamat IP Elastis Anda sendiri, dan mengaitkannya dengan instans Anda. Untuk informasi selengkapnya, lihat Alamat Elastic IP.

Jika Anda menggunakan Amazon VPC IP Address Manager (IPAM), Anda bisa mendapatkan blok alamat publik yang berdekatan AWS dan menggunakannya untuk mengalokasikan IPv4 alamat IP Elastis ke sumber daya. AWS Menggunakan blok IPv4 alamat yang berdekatan dapat secara signifikan mengurangi overhead manajemen untuk daftar kontrol akses keamanan dan menyederhanakan alokasi dan pelacakan alamat IP untuk penskalaan perusahaan. AWS Untuk informasi selengkapnya, lihat Mengalokasikan alamat IP Elastis berurutan dari kumpulan IPAM di Panduan Pengguna Amazon VPC IPAM.

Pertimbangan-pertimbangan

- AWS mengenakan biaya untuk semua IPv4 alamat publik, termasuk IPv4 alamat publik yang terkait dengan instans yang sedang berjalan dan alamat IP Elastis. Untuk informasi selengkapnya, lihat tab IPv4 Alamat Publik di halaman harga Amazon VPC.
- Instans yang mengakses instans lain melalui alamat IP NAT publiknya dikenai biaya untuk transfer data regional atau Internet, bergantung pada apakah instans tersebut berada di Wilayah yang sama.

Optimalisasi IPv4 alamat publik

AWS mengenakan biaya untuk semua IPv4 alamat publik, termasuk IPv4 alamat publik yang terkait dengan instans yang sedang berjalan dan alamat IP Elastis. Untuk informasi selengkapnya, lihat tab IPv4 Alamat Publik di halaman harga Amazon VPC.

Daftar berikut berisi tindakan yang dapat Anda lakukan untuk mengoptimalkan jumlah IPv4 alamat publik yang Anda gunakan:

- Gunakan penyeimbang beban elastis untuk memuat lalu lintas keseimbangan ke instans EC2 Anda dan nonaktifkan Auto-assign IP publik pada ENI utama yang ditetapkan ke instans. Load balancer menggunakan satu IPv4 alamat publik, jadi ini mengurangi jumlah IPv4 alamat publik Anda. Anda mungkin juga ingin mengkonsolidasikan penyeimbang beban yang ada untuk lebih mengurangi jumlah alamat publik IPv4 .
- Jika satu-satunya alasan untuk menggunakan gateway NAT adalah SSH ke instans EC2 di subnet pribadi untuk pemeliharaan atau keadaan darurat, pertimbangkan untuk menggunakan EC2 Instance Connect Endpoint sebagai gantinya. Dengan EC2 Instance Connect Endpoint, Anda dapat terhubung ke instans dari internet tanpa mengharuskan instans memiliki alamat publik IPv4 .
- Jika instans EC2 Anda berada di subnet publik dengan alamat IP publik yang dialokasikan untuk mereka, pertimbangkan untuk memindahkan instans ke subnet pribadi, menghapus alamat IP

publik, dan menggunakan gateway NAT publik untuk memungkinkan akses ke dan dari instans EC2 Anda. Ada pertimbangan biaya untuk menggunakan gateway NAT. Gunakan metode perhitungan ini untuk memutuskan apakah gateway NAT hemat biaya. Anda bisa mendapatkan yang `Number of public IPv4 addresses` diperlukan untuk perhitungan ini dengan membuat Laporan Biaya dan Penggunaan AWS Penagihan.

```
NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
 public IP cost
```

Di mana:

- `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
- `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`
- `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
- `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

Jika totalnya kurang dari 1, gateway NAT lebih murah daripada alamat publik. IPv4

- Gunakan AWS PrivateLinkuntuk terhubung secara pribadi ke AWS layanan atau layanan yang dihosting oleh AWS akun lain daripada menggunakan IPv4 alamat publik dan gateway internet.
- Bawa rentang alamat IP Anda sendiri (BYOIP) ke AWS dan gunakan rentang untuk IPv4 alamat publik daripada menggunakan alamat publik milik Amazon. IPv4
- Matikan auto-assign IPv4 alamat publik untuk instance yang diluncurkan ke subnet. Opsi ini umumnya dinonaktifkan secara default VPCs saat Anda membuat subnet, tetapi Anda harus memeriksa subnet yang ada untuk memastikannya dinonaktifkan.
- Jika Anda memiliki instans EC2 yang tidak memerlukan IPv4 alamat publik, periksa apakah antarmuka jaringan yang dilampirkan ke instans Anda menonaktifkan IP publik secara otomatis.
- Konfigurasikan titik akhir akselerator AWS Global Accelerator untuk instans EC2 di subnet pribadi untuk memungkinkan lalu lintas internet mengalir langsung ke titik akhir di Anda VPCs tanpa memerlukan alamat IP publik. Anda juga dapat membawa alamat Anda sendiri ke AWS Global Accelerator dan menggunakan alamat Anda sendiri untuk IPv4 alamat IP statis akselerator Anda.

IPv6 alamat

IPv6 alamat unik secara global dan dapat dikonfigurasi agar tetap pribadi atau dapat dijangkau melalui Internet. IPv6 Pengalamatan publik dan pribadi tersedia di AWS:

- Pribadi IPv6: AWS mempertimbangkan IPv6 alamat pribadi yang tidak diiklankan dan tidak dapat diiklankan di Internet dari. AWS
- Publik IPv6: AWS mempertimbangkan IPv6 alamat publik yang diiklankan di Internet dari AWS.

Untuk informasi selengkapnya tentang IPv6 alamat publik dan pribadi, lihat IPv6alamat di Panduan Pengguna Amazon VPC.

Semua jenis instans mendukung IPv6 alamat kecuali untuk yang berikut: C1, M1, M2, M3, dan T1.

Instans EC2 Anda menerima IPv6 alamat jika blok IPv6 CIDR dikaitkan dengan VPC dan subnet Anda, dan jika salah satu dari berikut ini benar:

- Subnet Anda dikonfigurasi untuk secara otomatis menetapkan IPv6 alamat ke instance selama peluncuran. Untuk informasi selengkapnya, lihat Memodifikasi atribut pengalamatan IP subnet Anda.
- Anda menetapkan IPv6 alamat ke instans Anda selama peluncuran.
- Anda menetapkan IPv6 alamat ke antarmuka jaringan utama instans Anda setelah peluncuran.
- Anda menetapkan IPv6 alamat ke antarmuka jaringan di subnet yang sama, dan melampirkan antarmuka jaringan ke instance Anda setelah peluncuran.

Ketika instans Anda menerima IPv6 alamat selama peluncuran, alamat tersebut dikaitkan dengan antarmuka jaringan utama (indeks 0) dari instance. Anda dapat mengelola IPv6 alamat untuk antarmuka jaringan utama instans Anda sebagai berikut:

- Tetapkan dan batalkan IPv6 alamat dari antarmuka jaringan. Jumlah alamat IPv6 yang dapat Anda tetapkan ke antarmuka jaringan dan jumlah antarmuka jaringan yang dapat Anda sertakan ke sebuah instans bervariasi tergantung jenis instans. Untuk informasi selengkapnya, lihat Alamat IP maksimum per antarmuka jaringan.
- Aktifkan IPv6 alamat utama. IPv6 Alamat utama memungkinkan Anda untuk menghindari mengganggu lalu lintas ke instance atau. ENIs Untuk informasi selengkapnya, lihat Buat antarmuka jaringan untuk instans EC2 Anda atau Kelola alamat IP untuk antarmuka jaringan Anda.

IPv6 Alamat tetap ada saat Anda berhenti dan memulai, atau hibernasi dan memulai, instance Anda, dan dirilis saat Anda menghentikan instance Anda. Anda tidak dapat menetapkan ulang alamat IPv6 saat ditetapkan ke antarmuka jaringan lain—Anda harus membatalkan penetapannya terlebih dahulu.

Anda dapat mengontrol apakah instance dapat dijangkau melalui IPv6 alamatnya dengan mengontrol perutean untuk subnet Anda atau dengan menggunakan grup keamanan dan aturan ACL jaringan. Untuk informasi selengkapnya, lihat Privasi lalu lintas Internetwork di Panduan Pengguna Amazon VPC.

Untuk informasi selengkapnya tentang rentang IPv6 alamat yang dipesan, lihat Registri Alamat IPv6 Tujuan Khusus IANA dan. RFC4291

Beberapa alamat IP

Anda dapat menentukan beberapa pribadi IPv4 dan IPv6 alamat untuk instance Anda. Jumlah antarmuka jaringan dan pribadi IPv4 dan IPv6 alamat yang dapat Anda tentukan untuk sebuah instance tergantung pada jenis instans. Untuk informasi selengkapnya, lihat Alamat IP maksimum per antarmuka jaringan.

Kasus penggunaan

- Melakukan hosting beberapa situs web di satu server dengan menggunakan beberapa sertifikat SSL di satu server dan mengaitkan setiap sertifikat dengan alamat IP tertentu.
- Mengoperasikan peralatan jaringan, seperti firewall atau load balancer, yang memiliki beberapa alamat IP untuk setiap antarmuka jaringan.
- Mengalihkan traffic internal ke instans siaga jika instans Anda gagal, dengan menetapkan kembali alamat IP sekunder ke instans siaga.

Cara kerja beberapa alamat IP

- Anda dapat menetapkan IPv4 alamat pribadi sekunder ke antarmuka jaringan apa pun.
- Anda dapat menetapkan beberapa IPv6 alamat ke antarmuka jaringan yang ada di subnet yang memiliki blok IPv6 CIDR terkait.
- Anda harus memilih IPv4 alamat sekunder dari rentang blok IPv4 CIDR subnet untuk antarmuka jaringan.
- Anda harus memilih IPv6 alamat dari rentang blok IPv6 CIDR subnet untuk antarmuka jaringan.

- Anda mengaitkan grup keamanan dengan antarmuka jaringan, bukan alamat IP individu. Oleh karena itu, setiap alamat IP yang Anda tentukan dalam antarmuka jaringan tunduk pada grup keamanan antarmuka jaringannya.
- Beberapa alamat IP dapat ditetapkan dan tidak ditetapkan ke antarmuka jaringan yang disertakan ke instans yang berjalan atau dihentikan.
- IPv4 Alamat pribadi sekunder yang ditetapkan ke antarmuka jaringan dapat dipindahkan ke yang lain jika Anda secara eksplisit mengizinkannya.
- IPv6 Alamat tidak dapat dipindahkan ke antarmuka jaringan lain; Anda harus terlebih dahulu membatalkan penetapan IPv6 alamat dari antarmuka jaringan yang ada.
- Saat menetapkan beberapa alamat IP ke antarmuka jaringan menggunakan alat baris perintah atau API, seluruh operasi gagal jika salah satu alamat IP tidak dapat ditetapkan.
- IPv4 Alamat pribadi primer, alamat pribadi sekunder, IPv4 alamat IP Elastis, dan IPv6 alamat tetap dengan antarmuka jaringan sekunder ketika terlepas dari sebuah instance atau dilampirkan ke sebuah instance.
- Meskipun Anda tidak dapat melepaskan antarmuka jaringan utama dari sebuah instance, Anda dapat menetapkan kembali IPv4 alamat pribadi sekunder dari antarmuka jaringan utama ke antarmuka jaringan lain.

Untuk informasi selengkapnya, lihat the section called “Alamat IP sekunder”.

Nama host instans EC2

Saat Anda membuat instance EC2, buat nama host untuk AWS instance itu. Untuk informasi selengkapnya tentang jenis nama host dan cara AWS penyediaannya, lihat. Nama host dan domain instans EC2 Amazon menyediakan server DNS yang menyelesaikan nama host dan alamat yang disediakan Amazon. IPv4 IPv6 Server Amazon DNS terletak di dasar rentang jaringan VPC Anda plus dua. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda di Panduan Pengguna Amazon VPC.

Alamat link-lokal

Alamat link-lokal adalah alamat IP yang terkenal dan tidak dapat dirutekan. Amazon EC2 menggunakan alamat dari ruang alamat link-local untuk menyediakan layanan yang hanya dapat diakses dari instans EC2. Layanan ini tidak berjalan pada instans, mereka berjalan di host yang mendasarinya. Saat Anda mengakses alamat link-lokal untuk layanan ini, Anda berkomunikasi dengan hypervisor Xen atau pengontrol Nitro.

Rentang alamat link-lokal

- IPv4 — 169.254.0.0/16 (169.254.0.0 ke 169.254.255.255)
- IPv6 — Fe80: :/10

Layanan yang Anda akses menggunakan alamat link-lokal

- Layanan Metadata Instans
- Amazon Route 53 Resolver (juga dikenal sebagai server DNS Amazon)
- Layanan Amazon Time Sync
- AWS Server KMS

Kelola alamat IPv4 untuk instans EC2 Anda

Anda dapat menetapkan IPv4 alamat publik ke instans Anda saat meluncurkannya. Anda dapat melihat IPv4 alamat instans Anda di konsol melalui halaman Instans atau halaman Antarmuka Jaringan.

Tugas

- Tetapkan IPv4 alamat publik saat peluncuran
- Tetapkan IPv4 alamat pribadi saat peluncuran
- Lihat IPv4 alamat utama
- Lihat IPv4 alamat menggunakan metadata instance

Tetapkan IPv4 alamat publik saat peluncuran

Setiap subnet memiliki atribut yang menentukan apakah instans yang diluncurkan ke subnet tersebut diberi alamat IP publik. Secara default, subnet non-default mengatur atribut ini ke false, dan subnet default mengatur atribut ini ke true. Saat meluncurkan instance, fitur IPv4 pengalamatan publik juga tersedia bagi Anda untuk mengontrol apakah instans Anda diberi IPv4 alamat publik; Anda dapat mengganti perilaku default atribut pengalamatan IP subnet. IPv4Alamat publik ditetapkan dari kumpulan IPv4 alamat publik Amazon, dan ditetapkan ke antarmuka jaringan dengan indeks perangkat 0. Fitur ini bergantung pada kondisi tertentu pada saat Anda meluncurkan instans Anda.

Pertimbangan-pertimbangan

- Anda dapat membatalkan penetapan alamat IP publik dari instans Anda setelah peluncuran dengan mengelola alamat IP yang terkait dengan antarmuka jaringan. Untuk informasi selengkapnya tentang IPv4 alamat publik, lihatIPv4 Alamat publik.
- Anda tidak dapat menetapkan alamat IP publik secara otomatis jika Anda menentukan lebih dari satu antarmuka jaringan. Selain itu, Anda tidak dapat mengganti pengaturan subnet menggunakan fitur IP publik penetapan otomatis jika Anda menentukan antarmuka jaringan yang ada untuk indeks perangkat 0.
- Apakah Anda menetapkan alamat IP publik ke instans Anda selama peluncuran atau tidak, Anda dapat mengaitkan alamat IP Elastis dengan instans Anda setelah diluncurkan. Untuk informasi selengkapnya, lihat Alamat Elastic IP. Anda juga dapat memodifikasi perilaku IPv4 pengalamatan publik subnet Anda. Untuk informasi selengkapnya, lihat Memodifikasi atribut IPv4 pengalamatan publik untuk subnet Anda.

Console

Untuk menetapkan IPv4 alamat publik saat peluncuran

Ikuti prosedur untuk meluncurkan instans, dan saat Anda mengonfigurasi Pengaturan Jaringan, pilih opsi untuk menetapkan IP Publik secara otomatis.

AWS CLI

Untuk menetapkan IPv4 alamat publik saat peluncuran

Gunakan perintah run-instance dengan opsi. `--associate-public-ip-address`

```
--associate-public-ip-address
```

PowerShell

Untuk menetapkan IPv4 alamat publik saat peluncuran

Gunakan New-EC2Instancecmdlet dengan parameter. `-AssociatePublicIp`

```
-AssociatePublicIp $true
```

Tetapkan IPv4 alamat pribadi saat peluncuran

Anda dapat menentukan alamat IPv4 pribadi dari rentang alamat IPv4 subnet, atau membiarkan Amazon EC2 memilihnya untuk Anda. Alamat ini ditetapkan ke antarmuka jaringan utama.

Untuk menetapkan IPv4 alamat setelah peluncuran, lihatthe section called “Tetapkan alamat IP sekunder ke sebuah instance”.

Console

Untuk menetapkan IPv4 alamat pribadi saat peluncuran

Ikuti prosedur untuk meluncurkan instans. Saat Anda mengkonfigurasi Pengaturan Jaringan, perluas konfigurasi jaringan lanjutan dan masukkan nilai untuk IP Utama.

AWS CLI

Untuk menetapkan IPv4 alamat pribadi saat peluncuran

Gunakan perintah run-instance dengan opsi. `--private-ip-address`

```
--private-ip-addresses 10.251.50.12
```

Untuk membiarkan Amazon EC2 memilih alamat IP, hilangkan opsi ini.

PowerShell

Untuk menetapkan IPv4 alamat pribadi saat peluncuran

Gunakan New-EC2Instancecmdlet dengan parameter. `-PrivateIpAddress`

```
-PrivateIpAddress 10.251.50.12
```

Untuk membiarkan Amazon EC2 memilih alamat IP, hilangkan parameter ini.

Lihat IPv4 alamat utama

IPv4 Alamat publik ditampilkan sebagai properti antarmuka jaringan di konsol, tetapi dipetakan ke IPv4 alamat pribadi utama melalui NAT. Oleh karena itu, jika Anda memeriksa properti antarmuka jaringan Anda pada instance Anda, misalnya, melalui `ifconfig` (Linux) atau `ipconfig` (Windows), IPv4 alamat publik tidak ditampilkan.

Console

Untuk melihat IPv4 alamat untuk sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pada tab Jaringan, temukan IPv4 Alamat publik dan IPv4 alamat pribadi.
5. (Opsional) Tab Networking juga berisi antarmuka jaringan dan alamat IP Elastis untuk instance.

AWS CLI

Untuk melihat IPv4 alamat utama untuk sebuah instance

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].PrivateIpAddress" \
    --output text
```

Berikut ini adalah output contoh.

```
10.251.50.12
```

PowerShell

Untuk melihat IPv4 alamat utama untuk sebuah instance

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.PrivateIpAddress
```

Berikut ini adalah output contoh.

```
10.251.50.12
```

Lihat IPv4 alamat menggunakan metadata instance

Anda bisa mendapatkan IPv4 alamat untuk instance Anda dengan mengambil metadata instance. Untuk informasi selengkapnya, lihat Gunakan metadata instans untuk mengelola instans EC2.

Untuk melihat IPv4 alamat menggunakan metadata instance

1. Connect ke instans Anda. Untuk informasi selengkapnya, lihat Connect ke instans EC2.
2. Gunakan salah satu perintah berikut ini.

   IMDSv2

   Linux

   Jalankan perintah berikut dari instance Linux Anda.

   ```
   TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/local-ipv4
   ```

   Windows

   Jalankan perintah berikut dari instance Windows Anda.

   ```
   [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
   seconds" = "21600"} `
       -Method PUT -Uri http://169.254.169.254/latest/api/token
   ```

   ```
   Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
       -Method GET -Uri http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   IMDSv1

   Linux

   Jalankan perintah berikut dari instance Linux Anda.

   ```
   curl http://169.254.169.254/latest/meta-data/local-ipv4
   ```

Windows

Jalankan perintah berikut dari instance Windows Anda.

```
Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Gunakan salah satu perintah berikut untuk mengakses alamat IP publik. Jika ada alamat IP Elastis yang terkait dengan instance, perintah mengembalikan alamat IP Elastis.

IMDSv2

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/public-ipv4
```

Windows

Jalankan perintah berikut dari instance Windows Anda.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/public-ipv4
```

IMDSv1

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
curl http://169.254.169.254/latest/meta-data/public-ipv4
```

Windows

Jalankan perintah berikut dari instance Windows Anda.

```
Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
```

Kelola alamat IPv6 untuk instans EC2 Anda

Jika VPC dan subnet Anda memiliki blok IPv6 CIDR yang terkait dengannya, Anda dapat menetapkan IPv6 alamat ke instans Anda selama atau setelah peluncuran. Anda dapat mengakses IPv6 alamat untuk instans Anda di konsol di halaman Instans atau halaman Antarmuka Jaringan. Tugas-tugas berikut mengonfigurasi alamat IP untuk instans Anda. Untuk mengonfigurasi alamat IP untuk antarmuka jaringan Anda, lihatthe section called “Mengelola alamat IP”.

Tugas

- Menetapkan IPv6 alamat ke sebuah instance
- Lihat IPv6 alamat untuk sebuah instance
- Lihat IPv6 alamat menggunakan metadata instance
- Membatalkan IPv6 alamat dari sebuah instance

Menetapkan IPv6 alamat ke sebuah instance

Anda dapat menentukan alamat IPv6 dari rentang alamat IPv6 subnet, atau membiarkan Amazon EC2 memilih satu untuk Anda. Alamat ini ditetapkan ke antarmuka jaringan utama. Perhatikan bahwa jenis contoh berikut tidak mendukung IPv6 alamat: C1, M1, M2, M3, dan T1.

Console

Untuk menetapkan IPv6 alamat saat peluncuran

Ikuti prosedur untuk meluncurkan instans. Saat Anda mengonfigurasi Pengaturan Jaringan, pilih opsi untuk Tetapkan IP secara otomatis IPv6 . Jika Anda tidak melihat opsi ini, subnet yang dipilih tidak memiliki blok IPv6 CIDR terkait.

Untuk menetapkan IPv6 alamat setelah peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.

3. Pilih instans Anda, dan pilih Tindakan, Jaringan, Kelola alamat IP.
4. Bentangkan antarmuka jaringan. Di alamat IPv6, pilih Tetapkan alamat IP baru.
5. Masukkan alamat IPv6 dari rentang subnet, atau biarkan bidang kosong untuk membiarkan Amazon EC2 memilih alamat untuk Anda. IPv6 Jika Anda tidak melihat opsi ini, subnet instance tidak memiliki blok IPv6 CIDR terkait.
6. Pilih Simpan.

AWS CLI

Untuk menetapkan IPv6 alamat saat peluncuran

Gunakan perintah run-instance dengan opsi. `--ipv6-addresses` Contoh berikut memberikan dua IPv6 alamat.

```
--ipv6-addresses Ipv6Address=2001:db8::1234:5678:1.2.3.4
 Ipv6Address=2001:db8::1234:5678:5.6.7.8
```

Untuk membiarkan Amazon EC2 memilih IPv6 alamat, gunakan `--ipv6-address-count` opsi sebagai gantinya. Contoh berikut memberikan dua IPv6 alamat.

```
--ipv6-address-count 2
```

Untuk menetapkan IPv6 alamat setelah peluncuran

Gunakan perintah assign-ipv6-address. Contoh berikut memberikan dua IPv6 alamat.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4 2001:db8::1234:5678:5.6.7.8
```

Untuk membiarkan Amazon EC2 memilih IPv6 alamat, gunakan `--ipv6-address-count` opsi sebagai gantinya. Contoh berikut memberikan dua IPv6 alamat.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-address-count 2
```

PowerShell

Untuk menetapkan IPv6 alamat saat peluncuran

Gunakan New-EC2Instancecmdlet dengan parameter. `-Ipv6Address` Contoh berikut memberikan dua IPv6 alamat.

```
-Ipv6Address $ipv6addr1,$ipv6addr2
```

Tentukan IPv6 alamat sebagai berikut.

```
$ipv6addr1 = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr1.Ipv6Address = "2001:db8::1234:5678:1.2.3.4"
$ipv6addr2 = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr2.Ipv6Address = "2001:db8::1234:5678:5.6.7.8"
```

Untuk membiarkan Amazon EC2 memilih IPv6 alamat, gunakan `-Ipv6AddressCount` parameter sebagai gantinya. Contoh berikut memberikan dua IPv6 alamat.

```
-Ipv6AddressCount 2
```

Untuk menetapkan IPv6 alamat setelah peluncuran

Gunakan Register-EC2Ipv6 AddressList cmdlet. Contoh berikut memberikan dua IPv6 alamat.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address "2001:db8::1234:5678:1.2.3.4","2001:db8::1234:5678:5.6.7.8"
```

Untuk membiarkan Amazon EC2 memilih IPv6 alamat, gunakan `-Ipv6AddressCount` parameter sebagai gantinya. Contoh berikut memberikan dua IPv6 alamat.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6AddressCount 2
```

Lihat IPv6 alamat untuk sebuah instance

Anda dapat melihat IPv6 alamat untuk instans Anda.

Console

Untuk melihat IPv6 alamat untuk sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pada tab Jaringan, tempatkan alamat IPv6 .

AWS CLI

Untuk melihat IPv6 alamat untuk sebuah instance

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[].Ipv6Address" \
    --output text
```

Berikut ini adalah output contoh.

```
2001:db8::1234:5678:1.2.3.4
```

PowerShell

Untuk melihat IPv6 alamat untuk sebuah instance

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.Ipv6Address
```

Berikut ini adalah output contoh.

```
2001:db8::1234:5678:1.2.3.4
```

Lihat IPv6 alamat menggunakan metadata instance

Setelah Anda terhubung ke instans Anda, Anda dapat mengambil IPv6 alamat menggunakan metadata instance. Pertama, Anda harus mendapatkan alamat MAC dari instance dari`http://169.254.169.254/latest/meta-data/network/interfaces/macs/`.

IMDSv2

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/mac-address/ipv6s
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/mac-address/ipv6s
```

IMDSv1

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/
ipv6s
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/mac-address/ipv6s
```

Membatalkan IPv6 alamat dari sebuah instance

Anda dapat membatalkan penetapan IPv6 alamat dari sebuah instans kapan saja.

Console

Untuk membatalkan penugasan IPv6 alamat dari sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans Anda, dan pilih Tindakan, Jaringan, Kelola alamat IP.
4. Bentangkan antarmuka jaringan. Di bawah IPv6alamat, pilih Unassign di sebelah alamat. IPv6
5. Pilih Simpan.

AWS CLI

Untuk membatalkan penetapan IPv6 alamat dari sebuah instance

Gunakan perintah unassign-ipv6-address.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4
```

PowerShell

Untuk membatalkan penetapan IPv6 alamat dari sebuah instance

Gunakan Unregister-EC2Ipv6 AddressList cmdlet.

```
Unregister-EC2Ipv6AddressList `
```

```
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8::1234:5678:1.2.3.4
```

Alamat IP sekunder untuk instans EC2 Anda

IPv4 Alamat pertama yang ditetapkan ke antarmuka jaringan dikenal sebagai alamat IP utama. Alamat IP sekunder adalah IPv4 alamat tambahan yang ditetapkan ke antarmuka jaringan. Untuk informasi selengkapnya, lihat the section called “Beberapa alamat IP”.

Anda juga dapat menetapkan beberapa IPv6 alamat ke sebuah instance. Untuk informasi selengkapnya, lihat the section called “IPv6 alamat”.

Tugas

- Tetapkan alamat IP sekunder ke sebuah instance
- Konfigurasikan sistem operasi untuk menggunakan alamat IP sekunder
- Membatalkan alamat IP sekunder dari sebuah instans

Tetapkan alamat IP sekunder ke sebuah instance

Anda dapat menetapkan alamat IP sekunder ke antarmuka jaringan untuk sebuah instance saat Anda meluncurkan instance, atau setelah instance berjalan.

Console

Untuk menetapkan alamat IP sekunder saat peluncuran

1. Ikuti prosedur untuk meluncurkan instans. Saat Anda mengonfigurasi Pengaturan Jaringan, perluas Konfigurasi jaringan lanjutan.
2. Untuk IP Sekunder, pilih Tetapkan secara otomatis dan masukkan jumlah alamat IP untuk Amazon EC2 yang akan ditetapkan. Atau, pilih Tetapkan secara manual dan masukkan IPv4 alamat.
3. Selesaikan langkah-langkah selanjutnya untuk meluncurkan instans.

Untuk menetapkan alamat IP sekunder setelah peluncuran

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Di panel navigasi, pilih Instans.
3. Pilih instans Anda, dan pilih Tindakan, Jaringan, Kelola alamat IP.
4. Bentangkan antarmuka jaringan.
5. Untuk menambahkan IPv4 alamat, di bawah IPv4alamat, pilih Tetapkan alamat IP baru. Masukkan alamat IPv4 dari rentang subnet, atau biarkan bidang kosong untuk membiarkan Amazon EC2 memilih satu untuk Anda.
6. Pilih Simpan.

AWS CLI

Untuk menetapkan alamat IP sekunder saat peluncuran

Gunakan perintah run-instance dengan opsi. `--secondary-private-ip-addresses`

```
--secondary-private-ip-addresses 10.251.50.12
```

Untuk membiarkan Amazon EC2 memilih alamat IP, gunakan `--secondary-private-ip-address-count` opsi sebagai gantinya. Contoh berikut memberikan satu alamat IP sekunder.

```
--secondary-private-ip-address-count 1
```

Atau, Anda dapat membuat antarmuka jaringan. Untuk informasi selengkapnya, lihat the section called “Membuat antarmuka jaringan”.

Untuk menetapkan alamat IP sekunder setelah peluncuran

Gunakan perintah assign-private-ip-addresses dengan opsi `--private-ip-addresses`.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-ids eni-1234567890abcdef0 \
    --private-ip-addresses 10.251.50.12
```

Untuk membiarkan Amazon EC2 memilih IPv4 alamat, gunakan `--secondary-private-ip-address-count` parameter sebagai gantinya. Contoh berikut memberikan satu IPv4 alamat.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-ids eni-1234567890abcdef0 \
```

```
    --secondary-private-ip-address-count 1
```

PowerShell

Untuk menetapkan alamat IP sekunder saat peluncuran

Anda harus membuat antarmuka jaringan. Untuk informasi selengkapnya, lihat the section called "Membuat antarmuka jaringan".

Untuk menetapkan alamat IP sekunder setelah peluncuran

Gunakan Register-EC2PrivateIpAddresscmdlet dengan parameter. `-PrivateIpAddress`

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.251.50.12
```

Untuk membiarkan Amazon EC2 memilih IPv4 alamat, gunakan `-SecondaryPrivateIpAddressCount` parameter sebagai gantinya. Contoh berikut memberikan satu IPv4 alamat.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -SecondaryPrivateIpAddressCount 1
```

Konfigurasikan sistem operasi untuk menggunakan alamat IP sekunder

Setelah Anda menetapkan alamat IP sekunder ke instans Anda, Anda harus mengkonfigurasi sistem operasi pada instans Anda untuk mengenali IPv4 alamat pribadi tambahan.

Instans Linux

- Jika Anda menggunakan Amazon Linux, paket ec2-net-utils dapat menangani langkah ini untuk Anda. Ini mengonfigurasi antarmuka jaringan tambahan yang Anda lampirkan saat instance berjalan, menyegarkan IPv4 alamat sekunder selama pembaruan sewa DHCP, dan memperbarui aturan perutean terkait. Anda dapat segera menyegarkan daftar antarmuka dengan menggunakan salah satu perintah berikut, tergantung pada sistem Anda: `sudo systemctl restart systemd-networkd` (AL2023) atau `sudo service network restart` (Amazon Linux 2). Anda dapat melihat up-to-date daftar menggunakan perintah berikut:`ip addr li`. Jika Anda

memerlukan kontrol manual atas konfigurasi jaringan Anda, Anda dapat menghapus paket ec2-net-utils. Untuk informasi selengkapnya, lihat Mengkonfigurasi antarmuka jaringan menggunakan ec2-net-utils.

- Jika Anda menggunakan distribusi Linux lain, lihat dokumentasi untuk distribusi Linux Anda. Cari informasi tentang mengkonfigurasi antarmuka jaringan tambahan dan alamat sekunder IPv4 . Jika instans memiliki dua atau beberapa antarmuka di subnet yang sama, cari informasi tentang menggunakan aturan perutean untuk mengatasi perutean asimetris.

Instans Windows

Untuk informasi selengkapnya, lihat Konfigurasikan IPv4 alamat pribadi sekunder untuk instance Windows.

Membatalkan alamat IP sekunder dari sebuah instans

Jika Anda tidak lagi memerlukan alamat IP sekunder, Anda dapat membatalkan penetapannya dari instance atau antarmuka jaringan. Ketika IPv4 alamat pribadi sekunder tidak ditetapkan dari antarmuka jaringan, alamat IP Elastis (jika ada) juga dipisahkan.

Console

Untuk membatalkan penetapan IPv4 alamat pribadi sekunder dari sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans, lalu pilih Tindakan, Jaringan, Kelola Alamat IP.
4. Bentangkan antarmuka jaringan. Untuk IPv4alamat, pilih Unassign untuk IPv4 alamat yang akan dibatalkan penetapan.
5. Pilih Simpan.

AWS CLI

Untuk membatalkan penugasan alamat IP pribadi sekunder

Gunakan perintah unassign-private-ip-addresses.

```
aws ec2 unassign-private-ip-addresses \
```

```
    --network-interface eni-1234567890abcdef0\
    --private-ip-addresses 10.251.50.12
```

PowerShell

Untuk membatalkan penugasan alamat IP pribadi sekunder

Gunakan Unregister-EC2PrivateIpAddresscmdlet.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterface eni-1234567890abcdef0 `
    -PrivateIpAddress 10.251.50.12
```

Konfigurasikan IPv4 alamat pribadi sekunder untuk instance Windows

Anda dapat menentukan beberapa IPv4 alamat pribadi untuk instance Anda. Setelah Anda menetapkan IPv4 alamat pribadi sekunder ke sebuah instans, Anda harus mengkonfigurasi sistem operasi pada instance untuk mengenali IPv4 alamat pribadi sekunder.

> **Note**
>
> Instruksi ini didasarkan pada Windows Server 2022. Implementasi langkah-langkah ini mungkin bervariasi berdasarkan sistem operasi instance Windows.

Tugas

- Prasyarat
- Langkah 1: Konfigurasikan alamat IP statis dalam instans Anda
- Langkah 2: Konfigurasikan alamat IP privat sekunder untuk instans Anda
- Langkah 3: Konfigurasikan aplikasi untuk Menggunakan alamat IP privat sekunder

Prasyarat

- Tetapkan IPv4 alamat pribadi sekunder ke antarmuka jaringan untuk instance. Anda dapat menetapkan IPv4 alamat pribadi sekunder saat meluncurkan instance, atau setelah instance berjalan. Untuk informasi selengkapnya, lihat Tetapkan alamat IP sekunder ke sebuah instance.

Langkah 1: Konfigurasikan alamat IP statis dalam instans Anda

Untuk mengaktifkan instans Windows Anda untuk menggunakan banyak alamat IP, Anda harus mengonfigurasi instans Anda untuk menggunakan pengalamatan IP statis, bukan server DHCP.

> **Important**
>
> Saat Anda mengonfigurasi pengalamatan IP statis dalam instans Anda, alamat IP harus sama persis dengan apa yang ditampilkan di konsol, CLI, atau API. Jika Anda salah memasukkan alamat IP ini, instans bisa jadi tidak dapat dijangkau.

Untuk mengonfigurasi pengalamatan IP statis pada instans Windows

1. Hubungkan ke instans Anda.
2. Temukan alamat IP, subnet mask, dan alamat gateway default untuk instans dengan melakukan langkah-langkah berikut:
   - Jalankan perintah berikut di PowerShell:

     ```
     ipconfig /all
     ```

     Tinjau output dan catat nilai IPv4 Address, Subnet Mask, Default Gateway, dan DNS Server untuk antarmuka jaringan. Output Anda harus menyerupai contoh berikut:

     ```
     ...

     Ethernet adapter Ethernet 4:

        Connection-specific DNS Suffix  . : us-west-2.compute.internal
        Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
        Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
        IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
        Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
        Default Gateway . . . . . . . . . : 10.200.0.1
        DHCP Server . . . . . . . . . . . : 10.200.0.1
     ```

```
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

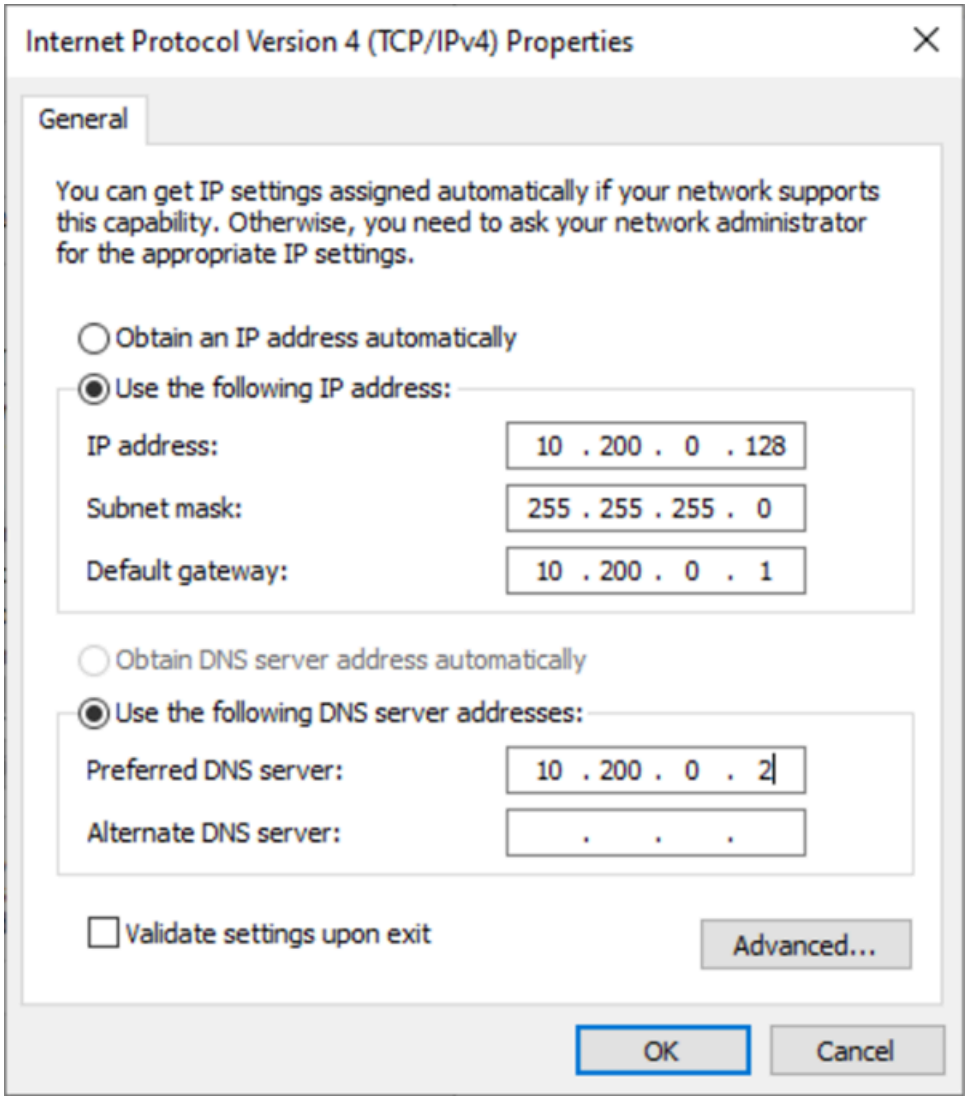
3. Buka Network and Sharing Center dengan menjalankan perintah berikut di PowerShell:

```
& $env:SystemRoot\system32\control.exe ncpa.cpl
```

4. Buka menu konteks (klik kanan) untuk antarmuka jaringan (Local Area Connection atau Ethernet) dan pilih Properties.
5. Pilih Internet Protocol Version 4 (TCP/IPv4), Properties.
6. Dalam Internet Protocol Version 4 (TCP/IPv4) Properties kotak dialog, pilih Gunakan alamat IP berikut, masukkan nilai berikut, lalu pilih OK.

Bidang	Nilai
Alamat IP	IPv4 Alamat yang diperoleh pada langkah 2 di atas.
Subnet mask	Subnet mask diperoleh pada langkah 2 di atas.
Gateway default	Alamat gateway default diperoleh pada langkah 2 di atas.
Server DNS pilihan	Server DNS diperoleh pada langkah 2 di atas.
Server DNS alternatif	Server DNS alternatif diperoleh pada langkah 2 di atas. Jika server DNS alternatif tidak terdaftar, biarkan bidang ini kosong.

> **Important**
>
> Jika Anda menyetel alamat IP ke nilai apa pun selain alamat IP saat ini, Anda akan kehilangan konektivitas ke instans.



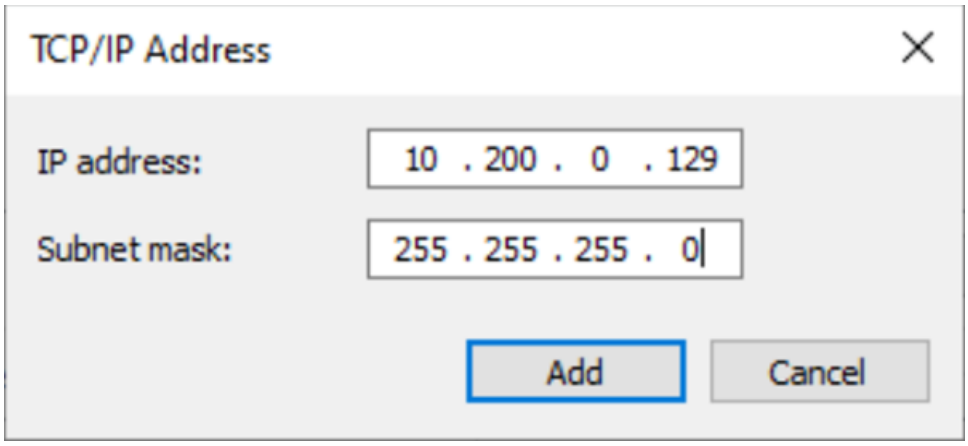
Anda akan kehilangan konektivitas RDP ke instans Windows selama beberapa detik saat instans tersebut diubah dari menggunakan DHCP menjadi pengalamatan statis. Instans tersebut mempertahankan informasi alamat IP yang sama seperti sebelumnya, tetapi sekarang informasi ini statis dan tidak dikelola oleh DHCP.

Langkah 2: Konfigurasikan alamat IP privat sekunder untuk instans Anda

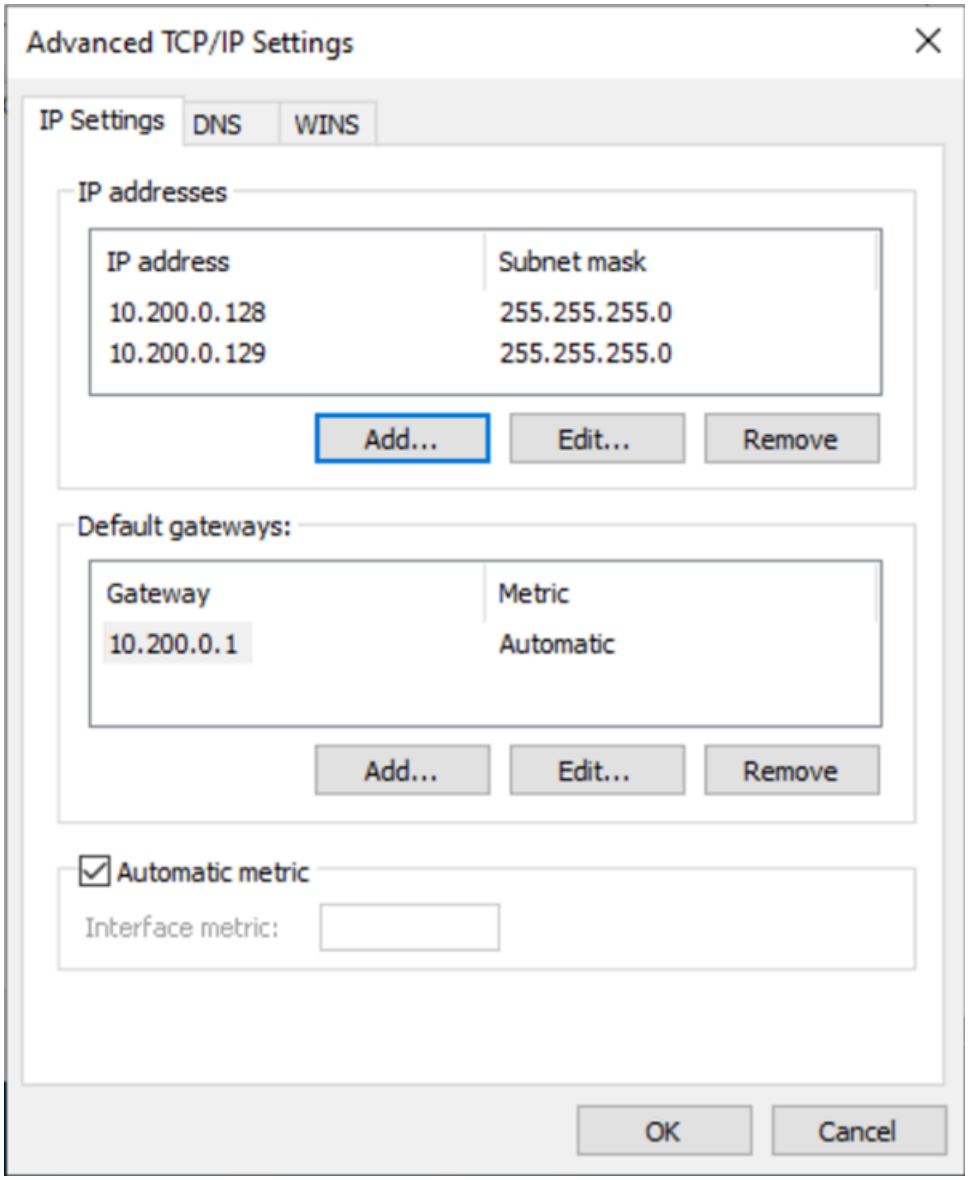
Setelah menyiapkan pengalamatan IP statis pada instans Windows, Anda siap untuk menyiapkan alamat IP privat kedua.

Untuk mengonfigurasi alamat IP sekunder

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, pilih Instans (dan pilih instans Anda.
3. Di bagian Jaringan, catat alamat IP sekunder.
4. Hubungkan ke instans Anda.
5. Pada instans Windows Anda, pilih Mulai, Panel Kontrol.
6. Pilih Jaringan dan Internet, Jaringan dan Pusat Berbagi.
7. Pilih antarmuka jaringan (Local Area Connection atau Ethernet) dan pilih Properties.
8. Pada halaman Local Area Connection Properties, pilih Internet Protocol Version 4 (TCP/IPv4), Properties, Advanced.
9. Pilih Tambahkan.
10. Di kotak dialog Alamat TCP/IP, ketik alamat IP pribadi sekunder untuk alamat IP. Untuk Subnet mask, ketik subnet mask yang sama dengan yang Anda masukkan untuk alamat IP privat primerLangkah 1: Konfigurasikan alamat IP statis dalam instans Anda, lalu pilih Tambahkan.



11. Verifikasi pengaturan alamat IP dan pilih OK.



12. Pilih OK, Tutup.
13. Untuk mengonfirmasi bahwa alamat IP sekunder telah ditambahkan ke sistem operasi, jalankan `ipconfig /all` perintah di PowerShell. Output Anda harus menyerupai yang berikut:

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
```

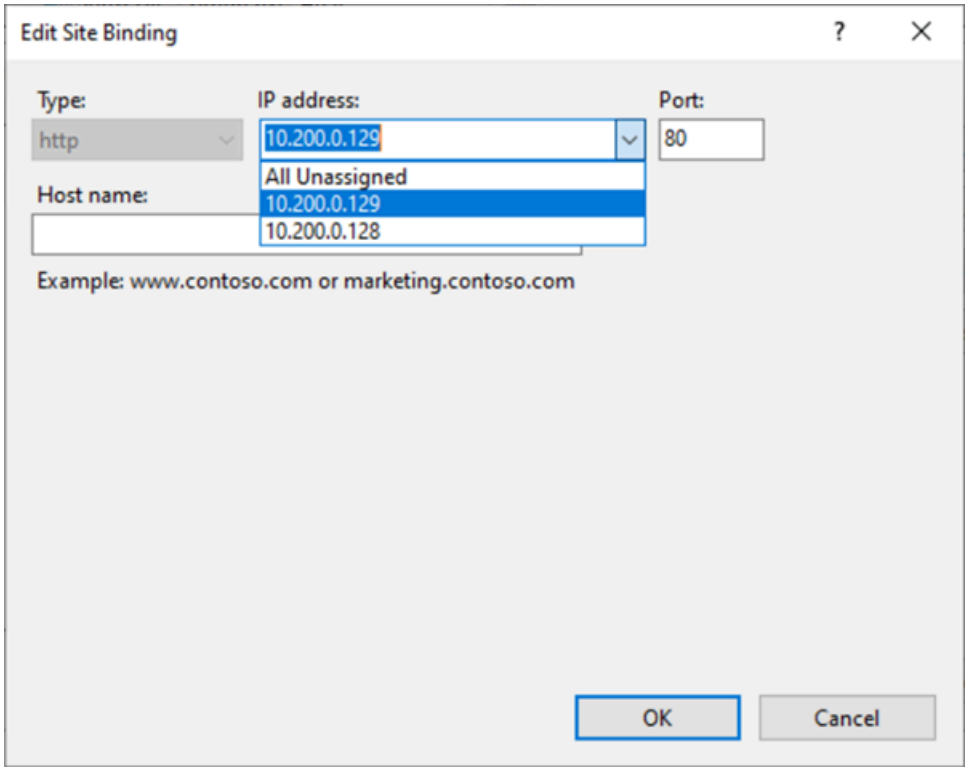
```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Langkah 3: Konfigurasikan aplikasi untuk Menggunakan alamat IP privat sekunder

Anda dapat mengonfigurasi aplikasi apa pun untuk menggunakan alamat IP privat sekunder. Misalnya, jika instans Anda menjalankan situs web di IIS, Anda dapat mengonfigurasi IIS untuk menggunakan alamat IP privat sekunder.

Untuk mengonfigurasi IIS untuk menggunakan alamat IP privat sekunder

1. Terhubung ke instans Anda.
2. Buka Manajer Layanan Informasi Internet (IIS).
3. Di panel koneksi, perluas Situs.
4. Buka menu konteks (klik kanan) untuk situs web Anda dan pilih Edit Bindings.
5. Di kotak dialog Ikatan Situs, pada Tipe, pilih http, Edit.
6. Di kotak dialog Edit Ikatan Situs, pada Alamat IP, pilih alamat IP privat sekunder. (Secara default, setiap situs web menerima permintaan HTTP dari semua alamat IP.)



7. Pilih OK, Tutup.

Nama host dan domain instans EC2

Memahami nama host dan domain instans EC2 penting untuk mengelola dan mengakses instans Amazon EC2 Anda secara efektif. Setiap instans EC2 dapat memiliki berbagai jenis nama host - pribadi dan publik - yang melayani tujuan yang berbeda dan mengikuti konvensi penamaan tertentu.

Topik ini menjelaskan struktur nama host instans EC2, cara pembuatannya, dan berbagai jenis nama host yang tersedia. Anda akan mempelajari cara melihat dan memodifikasi setelan nama host, memahami kapan harus menggunakan setiap jenis, dan mempelajari praktik terbaik untuk pengelolaan nama host di lingkungan Anda AWS .

Daftar Isi

- Memahami nama host dan domain instans EC2
- Jenis nama host

Memahami nama host dan domain instans EC2

Alamat instans EC2 terdiri dari komponen yang berbeda. Berikut ini adalah contoh alamat instans EC2 yang menggunakan IPv4 alamat pribadi instance:

```
   IP address         Domain name
   #--------# #-----------------------#
ip-10-24-34-0.us-west-2.compute.internal
#-----------#
  Hostname
#-------------------------------------#
    Fully qualified domain name (FQDN)
```

Di mana:

- Alamat IP: IPv4 Alamat utama dari antarmuka jaringan utama yang terkait dengan sebuah instance.
- Nama host: Nama lokal dari instans EC2 tertentu (digunakan oleh sistem operasi dan untuk identifikasi jaringan lokal)
- Nama domain: Bagian dari FQDN yang menyediakan AWS
- Nama domain yang sepenuhnya memenuhi syarat (FQDN): Alamat lengkap yang mencakup nama host dan nama domain. Ini adalah pengenal lengkap dan unik secara global yang digunakan untuk menjangkau instans Anda di seluruh jaringan.

Bergantung pada jenis nama host yang Anda pilih untuk instance atau antarmuka jaringan utama yang dilampirkan ke instance, format nama host dan nama domain akan berbeda dari contoh di atas. Bagian ini menjelaskan opsi jenis nama host.

Jenis nama host

AWS menyediakan dua jenis nama host: pribadi dan publik. Tabel berikut membandingkan perbedaan utama antara nama host pribadi dan publik, termasuk bagaimana mereka menyelesaikannya, bagaimana mereka dikonfigurasi, dan kapan menggunakan setiap jenis.

	Nama host pribadi	Nama host publik
Resolusi DNS	Nama host pribadi memungkinkan pribadi FQDNs yang tidak dapat	Nama host publik memungkinkan publik FQDNs yang dapat diakses

	Nama host pribadi	Nama host publik
	diakses dari internet publik. Nama host pribadi hanya mengizinkan permintaan untuk menyelesaikan ke alamat pribadi IPv4 dan IPv6 GUA dalam VPC.	dari internet publik. Nama host publik memungkinkan permintaan untuk menyelesaikan ke pribadi IPv4 dan IPv6 GUA dalam VPC dan IPs publik dari internet (DNS split-horizon).
Konfigurasi	Nama host pribadi dikonfigurasi pada tingkat instans.	Nama host publik dikonfigurasi pada tingkat antarmuka jaringan.
Kapan harus digunakan	• Untuk nama host yang diselesai kan hanya dalam VPC Anda, untuk komunikasi internal • Untuk menjaga skema penamaan internal Anda tetap pribadi • Untuk menyederhanakan manajemen sumber daya internal tanpa pertimbangan DNS eksternal	• Untuk mengakses instance melalui keduanya IPv4 dan IPv6 dari internet • Untuk mengaktifkan migrasi yang lancar dari IPv4 ke IPv6 lingkungan

Daftar Isi

- Nama host publik
- Nama host pribadi

Nama host publik

Anda dapat menggunakan nama host publik untuk mengakses instans EC2 menggunakan nama host yang menyelesaikan ke publik IPv4 atau IPv6 alamat instans dan memudahkan transisi Anda. IPv6

Nama host publik memungkinkan Anda untuk:

- Akses instans EC2 Anda melalui keduanya IPv4 dan IPv6, memberi Anda lebih banyak fleksibilitas dalam cara Anda terhubung ke sumber daya Anda.
- Bermigrasi dari IPv4 ke IPv6 lingkungan dengan kecepatan Anda sendiri. Anda dapat, misalnya, memisahkan database dan migrasi aplikasi Anda, mengurangi kompleksitas dan risiko.

- Gunakan beberapa opsi nama host (IPv4-only, IPv6 -only, dan dual-stack) yang secara otomatis menyelesaikan ke alamat IP yang sesuai.
- Manfaatkan peningkatan keamanan dengan DNS split-horizon, yang menyelesaikan nama host ke alamat IP pribadi saat ditanyakan dari dalam VPC Anda.

Daftar Isi

- Jenis nama host publik dan kapan menggunakannya
- Lihat nama host publik
- Ubah jenis nama host publik

Jenis nama host publik dan kapan menggunakannya

Untuk menggunakan nama host publik, Anda harus memodifikasi antarmuka jaringan yang ada. Bagian ini menjelaskan tiga opsi jenis nama host publik dan membantu Anda memutuskan mana yang akan digunakan:

- Dual-stack - nama berbasis IP
  - Ini adalah opsi terbaik jika Anda bermigrasi atau berencana untuk bermigrasi dari IPv4 ke. IPv6 Opsi ini memungkinkan konektivitas melalui keduanya IPv4 dan IPv6, memberikan fleksibilitas kepada klien yang mungkin menggunakan salah satu protokol dan memungkinkan klien untuk menyimpan nama host yang sama selama migrasi ke IPv6.
  - Permintaan dari dalam VPC menyelesaikan IPv4 alamat pribadi dan IPv6 Global Unicast Address (GUA) dari antarmuka jaringan. Permintaan dari internet menyelesaikan ke publik IPv4 dan alamat IPv6 GUA dari antarmuka jaringan.
  - Contoh
    - Ketika Anda memilih opsi ini, FQDN dual-stack akan dihasilkan untuk antarmuka jaringan ini. Ini adalah contoh FQDN yang akan dihasilkan:
      - F5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdpo.ap-tenggara 2.ip.aws
    - Di mana:
      - F5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdpo adalah nama host yang merupakan representasi base36 dari alamat publik utama (f5lnz-0khrm-nt2u3-gyqqt-nbdl5) pada antarmuka jaringan bersama dengan representasi base36 dari alamat publik utama (Q3cdpo) pada antarmuka jaringan. IPv6 IPv4

    - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 diselesaikan oleh penyelesai DNS Amazon ke alamat GUA FFFF: 1407:4:f 000:81 d: 2689:1066:4489. IPv6 Ini adalah IPv6 GUA pertama yang ditugaskan ke antarmuka jaringan.
    - Q3cdpo diselesaikan ke IPv4 alamat 52.54.55.56. Ini adalah IPv4 alamat publik yang dilampirkan ke antarmuka jaringan utama.
    - ap-southeast-2 adalah Wilayah subnet tempat antarmuka jaringan berada.
    - ip.aws adalah domain yang disediakan oleh. AWS
- IPv6 - Nama berbasis IP
  - Ini adalah opsi yang baik jika Anda telah bermigrasi ke IPv6 dan hanya memerlukan konektivitas. IPv6
  - Permintaan dari dalam VPC atau dari internet menyelesaikan ke IPv6 GUA antarmuka jaringan.
  - Contoh
    - Ketika Anda memilih opsi ini, FQDN akan dihasilkan untuk antarmuka jaringan ini. Ini adalah contoh FQDN yang akan dihasilkan:
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-southeast-2.ip.aws
    - Di mana:
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 adalah nama host yang merupakan representasi base36 dari alamat publik utama pada antarmuka jaringan. IPv6
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 diselesaikan oleh penyelesai DNS Amazon ke alamat GUA FFFF: 1407:4:f 000:81 d: 2689:1066:4489. IPv6 Ini adalah IPv6 GUA pertama yang ditugaskan ke antarmuka jaringan.
      - ap-southeast-2 adalah Wilayah subnet tempat antarmuka jaringan berada.
      - ip.aws adalah domain yang disediakan oleh. AWS
- IPv4 - Nama berbasis IP
  - Ini adalah pilihan yang baik jika instance yang menggunakan antarmuka jaringan ini perlu mempertahankan IPv4 akses selama transisi ke IPv6 atau jika aplikasi atau sistem yang berjalan pada instance hanya mendukung IPv4. Ini adalah pilihan terbaik jika Anda hanya perlu mempertahankan IPv4 konektivitas dan beban kerja Anda tidak memerlukan IPv6 dukungan. Misalnya, jika Anda bermigrasi ke IPv6, Anda dapat memutuskan untuk tetap mengaktifkan beberapa aplikasi IPv4 sementara yang lain pindah ke IPv6.
  - Permintaan dari dalam VPC menyelesaikan ke IPv4 alamat utama pribadi antarmuka jaringan. Permintaan dari internet menyelesaikan ke IPv4 alamat publik antarmuka jaringan.
  - Contoh

- Jika Anda memilih opsi ini, nama host publik IPv4 yang diaktifkan akan dibuat untuk antarmuka jaringan ini. Ini adalah contoh nama DNS yang akan dihasilkan:
  - ec2-52-54-55-66.ap-southeast-2.compute.amazonaws.com
- Di mana:
  - ec2-52-54-55-66 adalah nama host yang merupakan representasi base36 dari alamat publik utama antarmuka jaringan. IPv4
  - ec2-52-54-55-66 menyelesaikan ke alamat 52.54.55.56. IPv4 Ini adalah IPv4 alamat publik yang dilampirkan ke antarmuka jaringan utama.
  - ap-southeast-2 adalah Wilayah subnet tempat antarmuka jaringan berada.
  - ip.aws adalah domain yang disediakan oleh. AWS

> **Important**
>
> Pada contoh di atas, Anda dapat melihat bahwa alamat IP digunakan untuk menghasilkan nama host. Jika Anda mengubah IPv4 alamat pribadi utama atau IPv6 GUA pertama yang ditetapkan ke antarmuka jaringan, bagian dari nama host yang diterjemahkan ke alamat IP akan berubah dan nama host publik yang dihasilkan sebelumnya tidak lagi valid. Selain itu, mengubah alamat IPv4 publik utama memaksa penyegaran hilir Layanan Metadata Instans (IMDS) di Panduan Pengguna Amazon EC2, sehingga metadata IMDS instans EC2 diperbarui secara otomatis.

Lihat nama host publik

Jika VPC tempat antarmuka jaringan berada tidak memiliki keduanya EnableDnsHostnames dan EnableDnsSupport diaktifkan, tidak ada jenis nama host yang ditentukan atau dihasilkan.

Console

Anda dapat melihat nama host publik untuk instance atau antarmuka jaringan utama.

Untuk melihat jenis nama host dan nama DNS dari sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih kotak centang untuk instans.

4. Pada tab Jaringan, di bawah Hostname dan DNS, temukan yang berikut ini:

   - Jenis nama host publik
   - DNS Publik
   - IPv4-hanya nama berbasis IP
   - IPv6-only - nama berbasis IP
   - Dualstack - nama berbasis IP

Untuk melihat jenis nama host dan nama DNS dari antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Di bidang pencarian, masukkan ID instance. Pilih ID antarmuka jaringan untuk membuka halaman detailnya.
4. Di bawah Hostname dan DNS, temukan yang berikut ini:

   - Jenis nama host publik
   - Nama DNS publik
   - Nama IPv4 DNS publik
   - Nama IPv6 DNS publik
   - Nama DNS Dualstack Publik

AWS CLI

Untuk melihat jenis nama host dan nama DNS dari antarmuka jaringan

Gunakan perintah describe-network-interfaces.

```
aws ec2 describe-network-interfaces \
    --network-interface-id eni-1234567890abcdef0 \
    --query NetworkInterfaces[].PublicIpDnsNameOptions
```

Berikut ini adalah output contoh. Karena jenis hostname adalah`public-dual-stack-dns-name`, nama host DNS sama dengan. `PublicDualStackDnsName`

```
[
```

```
    {
        "DnsHostnameType": "public-dual-stack-dns-name",
        "PublicIpv4DnsName": "ec2-52-54-55-66.ap-
southeast-2.compute.amazonaws.com",
        "PublicIpv6DnsName": "f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-
southeast-2.ip.aws",
        "PublicDualStackDnsName": "f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp0.ap-
southeast-2.ip.aws"
    }
]
```

PowerShell

Untuk melihat jenis nama host dan nama DNS dari antarmuka jaringan

Gunakan Get-EC2NetworkInterfacecmdlet.

```
(Get-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0).PublicIpDnsNameOptions
```

Berikut ini adalah output contoh. Karena jenis hostname adalah`public-dual-stack-dns-name`, nama host DNS sama dengan. `PublicDualStackDnsName`

```
DnsHostnameType        : public-dual-stack-dns-name
PublicDualStackDnsName : f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp0.ap-southeast-2.ip.aws
PublicIpv4DnsName      : ec2-52-54-55-66.ap-southeast-2.compute.amazonaws.com
PublicIpv6DnsName      : f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-southeast-2.ip.aws
```

Ubah jenis nama host publik

Opsi jenis nama host publik bergantung pada alamat IP yang terkait dengan antarmuka jaringan:

- Jika antarmuka jaringan hanya memiliki IPv4 alamat publik, jenis nama host harus IPv4 - nama berbasis IP.
- Jika antarmuka jaringan hanya memiliki IPv6 alamat, jenis nama host harus IPv6 - nama berbasis IP.
- Jika antarmuka jaringan memiliki IPv4 alamat publik dan IPv6 alamat, jenis nama host dapat berupa Dual-stack - nama berbasis IP.

Prasyarat

- Antarmuka jaringan harus memiliki IPv4 alamat publik atau IPv6 alamat yang terkait.
- VPC tempat antarmuka jaringan berada harus dimiliki EnableDnsHostnames dan EnableDnsSupport diaktifkan. Lihat Melihat dan memperbarui atribut DNS untuk VPC Anda di Panduan Pengguna Amazon VPC.

Console

Untuk memodifikasi jenis nama host publik

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Di bidang pencarian, masukkan ID instance. Pilih kotak centang untuk antarmuka jaringan.

   Atau, dari halaman detail instance, pilih tab Jaringan dan pilih ID antarmuka jaringan untuk indeks perangkat 0.
4. Pilih Tindakan, Ubah jenis nama host publik.
5. Pilih satu opsi:

   - Dual-stack - Nama berbasis IP: Nama host publik dual-stack untuk antarmuka jaringan. Permintaan dari dalam VPC menyelesaikan IPv4 alamat pribadi dan Alamat Unicast IPv6 Global dari antarmuka jaringan. Permintaan dari internet menyelesaikan ke publik IPv4 dan alamat IPv6 GUA dari antarmuka jaringan.
   - IPv4 - Nama berbasis IP: Nama host publik yang IPv4 diaktifkan untuk antarmuka jaringan. Permintaan dari dalam VPC menyelesaikan ke IPv4 alamat utama pribadi antarmuka jaringan. Permintaan dari internet menyelesaikan ke IPv4 alamat publik antarmuka jaringan.
   - IPv6 - Nama berbasis IP: Nama host publik yang IPv6 diaktifkan untuk antarmuka jaringan. Permintaan dari dalam VPC atau dari internet menyelesaikan ke IPv6 GUA antarmuka jaringan.
6. Pilih Ubah.

AWS CLI

Untuk memodifikasi jenis nama host publik

Gunakan perintah modify-public-ip-dns-name-options.

```
aws ec2 modify-public-ip-dns-name-options \
    --network-interface-id eni-1234567890abcdef0 \
    --hostname-type public-dual-stack-dns-name
```

Berikut ini adalah output contoh.

```
{
    "Successful": true
}
```

PowerShell

Untuk memodifikasi jenis nama host publik

Gunakan Edit-EC2PublicIpDnsNameOptioncmdlet.

```
Edit-EC2PublicIpDnsNameOption `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -HostNameType public-dual-stack-dns-name
```

Nama host pribadi

Bagian ini menjelaskan nama host pribadi instans Amazon EC2 yang tersedia saat Anda meluncurkan instance ke subnet VPC Anda.

Nama host pribadi membedakan instans EC2 di jaringan Anda. Anda dapat menggunakan nama host pribadi dari sebuah instance jika, misalnya, Anda ingin menjalankan skrip untuk berkomunikasi dengan beberapa atau semua instance di jaringan Anda.

Daftar Isi

- Jenis nama host pribadi
- Di mana menemukan nama sumber daya dan nama IP
- Memilih antara nama sumber daya dan nama IP
- Ubah opsi penamaan berbasis sumber daya untuk Amazon EC2

Jenis nama host pribadi

Ada dua jenis nama host pribadi untuk nama host OS tamu saat instans EC2 diluncurkan di VPC:

- Nama IP: Skema penamaan lama di mana, ketika Anda meluncurkan sebuah instance, IPv4 alamat pribadi instance disertakan dalam nama host instance. Nama IP ada selama masa pakai instans EC2. Ketika digunakan sebagai nama host DNS Pribadi, itu hanya akan mengembalikan IPv4 alamat pribadi (Catatan).
- Nama sumber daya: Saat Anda meluncurkan instans, ID instans EC2 disertakan dalam nama host instans. Nama sumber daya ada selama masa pakai instans EC2. Ketika digunakan sebagai nama host DNS Pribadi, itu dapat mengembalikan IPv4 alamat pribadi (Catatan) and/or Alamat Unicast IPv6 Global (catatan AAAA).

Tipe nama host OS tamu instans EC2 bergantung pada pengaturan subnet:

- Jika instance diluncurkan ke subnet IPv4 -only, Anda dapat memilih nama IP atau nama sumber daya.
- Jika instance diluncurkan ke subnet dual-stack (IPv4+IPv6), Anda dapat memilih nama IP atau nama sumber daya.
- Jika instance diluncurkan ke subnet IPv6 -only, nama sumber daya digunakan secara otomatis.

Daftar Isi

- Nama IP
- Nama sumber daya
- Perbedaan antara nama IP dan nama Sumber Daya

Nama IP

Saat Anda meluncurkan instans EC2 dengan jenis nama IP Hostname, nama host OS tamu dikonfigurasi untuk menggunakan alamat pribadi. IPv4

- Format untuk sebuah instans di us-east-1: *`private-ipv4-address`*`.ec2.internal`
- Contoh: *`ip-10-24-34-0`*`.ec2.internal`
- Format untuk sebuah instance di AWS Wilayah lain: *`private-ipv4-address.region`*`.compute.internal`

- Contoh: *ip-10-24-34-0.us-west-2*.compute.internal

Nama sumber daya

Saat Anda meluncurkan instans EC2 di subnet IPv6 -only, jenis nama Sumber Daya Hostname dipilih secara default. Saat Anda meluncurkan instance di subnet IPv4 -only atau dual-stack (IPv4+IPv6), Resource name adalah opsi yang dapat Anda pilih. Setelah Anda meluncurkan sebuah instans, Anda dapat mengelola konfigurasi nama host. Untuk informasi selengkapnya, lihat Ubah opsi penamaan berbasis sumber daya untuk Amazon EC2.

Saat Anda meluncurkan instans EC2 dengan tipe nama host dari Nama sumber daya, nama host OS tamu dikonfigurasi untuk menggunakan ID instans EC2.

- Format untuk sebuah instans di us-east-1: *ec2-instance-id*.ec2.internal
- Contoh: *i-0123456789abcdef*.ec2.internal
- Format untuk sebuah instance di AWS Wilayah lain: *ec2-instance-id.region*.compute.internal
- Contoh: *i-0123456789abcdef.us-west-2*.compute.internal

Perbedaan antara nama IP dan nama Sumber Daya

Kueri DNS untuk nama IP dan nama sumber daya hidup berdampingan untuk memastikan kompatibilitas mundur dan memungkinkan Anda bermigrasi dari penamaan berbasis IP untuk nama host ke penamaan berbasis sumber daya. Untuk nama host DNS privat berdasarkan nama IP, Anda tidak dapat mengonfigurasi apakah kueri catatan DNS A untuk instans ditanggapi atau tidak. Catatan DNS A selalu ditanggapi terlepas dari pengaturan nama host OS tamu. Sebaliknya, untuk nama host DNS pribadi berdasarkan nama sumber daya, Anda dapat mengonfigurasi apakah kueri DNS A and/or DNS AAAA untuk instance ditanggapi atau tidak. Anda mengonfigurasi perilaku respons saat meluncurkan instans atau memodifikasi subnet. Untuk informasi selengkapnya, lihat Ubah opsi penamaan berbasis sumber daya untuk Amazon EC2.

Di mana menemukan nama sumber daya dan nama IP

Anda dapat melihat jenis nama host, nama sumber daya, dan nama IP, di konsol Amazon EC2.

Daftar Isi

- Saat membuat instans EC2
- Saat melihat detail instans EC2 yang sudah ada

Saat membuat instans EC2

Saat Anda membuat instans EC2, tergantung pada tipe subnet yang Anda pilih, Tipe nama host dari Nama sumber daya mungkin tersedia atau mungkin dipilih dan tidak dapat dimodifikasi. Bagian ini menjelaskan skenario di mana Anda melihat nama sumber daya tipe nama host dan nama IP.

Skenario 1

Anda membuat instans EC2 di wizard (lihatLuncurkan instans EC2 menggunakan wizard instans peluncuran di konsol) dan, ketika Anda mengonfigurasi detailnya, Anda memilih subnet yang Anda konfigurasikan menjadi IPv6 -only.

Dalam hal ini, Tipe nama host dari Nama sumber daya dipilih secara otomatis dan tidak dapat dimodifikasi. Opsi DNS Hostname dari Aktifkan nama IP IPv4 (Catatan) Permintaan DNS dan Aktifkan permintaan DNS berbasis sumber daya IPv4 (Catatan) tidak dipilih secara otomatis dan tidak dapat dimodifikasi. Aktifkan permintaan DNS berbasis sumber daya IPv6 (catatan AAAA) dipilih secara default tetapi dapat dimodifikasi. Jika dipilih, permintaan DNS ke nama sumber daya akan diselesaikan ke alamat IPv6 (catatan AAAA) dari instans EC2 ini.

Skenario 2

Anda membuat instans EC2 di wizard (lihatLuncurkan instans EC2 menggunakan wizard instans peluncuran di konsol) dan, ketika Anda mengonfigurasi detailnya, Anda memilih subnet yang dikonfigurasi dengan blok CIDR atau blok IPv4 CIDR IPv4 dan IPv6 CIDR (“tumpukan ganda”).

Dalam hal ini, Aktifkan nama IP IPv4 (Catatan) Permintaan DNS dipilih secara otomatis dan tidak dapat diubah. Ini berarti bahwa permintaan ke nama IP akan diselesaikan ke alamat IPv4 (catatan A) dari instans EC2 ini.

Opsi default ke konfigurasi subnet, tetapi Anda dapat memodifikasi opsi untuk instans ini tergantung pada pengaturan subnet:

- Tipe nama host: Menentukan apakah Anda ingin nama host OS tamu dari instans EC2 menjadi nama sumber daya atau nama IP. Nilai default-nya adalah nama IP.
- Aktifkan permintaan DNS berbasis sumber daya IPv4 (Catatan): Menentukan apakah permintaan ke nama sumber daya Anda diselesaikan ke alamat IPv4 pribadi (Catatan) dari instans EC2 ini. Opsi ini tidak dipilih secara default.
- Aktifkan permintaan DNS berbasis sumber daya IPv6 (catatan AAAA): Menentukan apakah permintaan ke nama sumber daya Anda diselesaikan ke alamat IPv6 GUA (catatan AAAA) dari instans EC2 ini. Opsi ini tidak dipilih secara default.

Saat melihat detail instans EC2 yang sudah ada

Anda dapat melihat nilai nama host untuk instans EC2 yang ada di tab Detail untuk instans EC2:

- Tipe nama host: Nama host dalam nama IP atau format nama sumber daya.
- Nama DNS IP Pribadi (IPv4 hanya): Nama IP yang akan selalu diselesaikan ke IPv4 alamat pribadi instance.
- Nama DNS sumber daya privat: Nama sumber daya yang menyelesaikan catatan DNS yang dipilih untuk instans ini.
- Jawab nama DNS sumber daya pribadi: Nama sumber daya menyelesaikan catatan DNS IPv4 (A), (AAAA) atau IPv4 dan IPv6 IPv6 (A dan AAAA).

Selain itu, jika Anda terhubung ke instans EC2 Anda langsung melalui SSH dan memasukkan perintah `hostname`, Anda akan melihat nama host baik dalam nama IP atau format nama sumber daya.

Memilih antara nama sumber daya dan nama IP

Saat Anda meluncurkan instans EC2 (lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol), jika Anda memilih Tipe nama host dari Nama sumber daya, instans EC2 akan diluncurkan dengan nama host dalam format nama sumber daya. Dalam kasus seperti itu, catatan DNS untuk instans EC2 ini juga dapat menunjuk ke nama sumber daya. Ini memberi Anda fleksibilitas untuk memilih apakah nama host tersebut menyelesaikan IPv4 alamat, IPv6 alamat, atau keduanya IPv4 dan IPv6 alamat instance. Jika Anda berencana untuk menggunakan IPv6 di masa depan atau jika Anda menggunakan subnet dual-stack hari ini, yang terbaik adalah menggunakan jenis nama Sumber Daya Hostname sehingga Anda mengubah resolusi DNS untuk nama host instance Anda tanpa membuat perubahan apa pun pada catatan DNS itu sendiri. Nama sumber daya memungkinkan Anda untuk menambah dan menghapus resolusi DNS IPv4 dan IPv6 pada instans EC2.

Jika sebaliknya Anda memilih jenis nama IP Hostname, dan menggunakannya sebagai nama host DNS, itu hanya dapat menyelesaikan ke IPv4 alamat instance. Ini tidak akan menyelesaikan ke IPv6 alamat instance bahkan jika instance memiliki IPv4 alamat dan IPv6 alamat yang terkait dengannya.

Ubah opsi penamaan berbasis sumber daya untuk Amazon EC2

Anda dapat mengubah jenis nama host dan konfigurasi nama host DNS untuk subnet, yang memengaruhi semua peluncuran instance berikutnya dalam subjek tersebut, atau Anda dapat mengubahnya untuk instans EC2 setelah Anda meluncurkannya.

Opsi penamaan berbasis sumber daya

- Jenis nama host: Menentukan pengaturan default untuk nama host OS tamu dari instans EC2 yang diluncurkan di subnet. Ini adalah nama sumber daya atau nama IP.
- Aktifkan permintaan nama host DNS IPv4 (Catatan): Menentukan apakah DNS requests/queries ke nama sumber daya diselesaikan ke alamat IPv4 pribadi (Catatan) dari instans EC2.
- Aktifkan permintaan nama host DNS IPv6 (catatan AAAA): Menentukan apakah DNS requests/queries ke nama sumber daya diselesaikan ke alamat IPv6 (catatan AAAA) dari instans EC2.

Subnet

Mengubah pengaturan subnet tidak mengubah konfigurasi instans EC2 yang sudah diluncurkan di subnet.

Console

Untuk memodifikasi opsi untuk subnet

Buka konsol Amazon VPC dan pilih subnet. Pilih Tindakan, Edit pengaturan subnet. Ubah pengaturan sesuai kebutuhan dan kemudian simpan perubahan Anda.

AWS CLI

Untuk memodifikasi opsi untuk subnet

Gunakan perintah modify-subnet-attribute.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-0abcdef1234567890 \
    --private-dns-hostname-type-on-launch resource-name \
    --enable-resource-name-dns-a-record-on-launch \
    --enable-resource-name-dns-aaaa-record-on-launch
```

PowerShell

Untuk memodifikasi opsi untuk subnet

Gunakan Edit-EC2SubnetAttributecmdlet.

```
Edit-EC2SubnetAttribute `
    -SubnetId subnet-0abcdef1234567890 `
```

```
    -PrivateDnsHostnameTypeOnLaunch ResourceName `
    -EnableResourceNameDnsAAAARecordOnLaunch $true `
    -EnableResourceNameDnsARecordOnLaunch $true
```

Instans EC2

Pertimbangan-pertimbangan

- Untuk mengubah jenis nama host, Anda harus terlebih dahulu menghentikan instance. Tidak perlu menghentikan instance untuk mengubah dua opsi lainnya.
- Karena Anda tidak dapat menghentikan instance dengan volume root penyimpanan instance, Anda hanya dapat mengonfigurasi jenis nama host dan opsi nama host DNS saat peluncuran instance. Hanya jenis instance berikut yang mendukung volume root penyimpanan instance: C1, C3, D2, I2, M1, M2, M3, R3, dan X1.

Console

Untuk memodifikasi jenis nama host dan opsi nama host DNS untuk sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Jika Anda akan mengubah pengaturan Gunakan penamaan berbasis sumber daya sebagai nama host OS tamu, pertama-tama hentikan instans EC2. Jika tidak, lewati langkah ini.

   Untuk menghentikan instans, pilih instans dan pilih Status instans, Setop instans.
3. Pilih instans dan pilih Tindakan, Pengaturan instans, Ubah opsi penamaan berbasis sumber daya.

   - Gunakan penamaan berbasis sumber daya sebagai nama host OS tamu: Menentukan apakah Anda ingin nama host OS tamu dari instans EC2 menjadi nama sumber daya atau nama IP.
   - Menjawab permintaan nama host DNS IPv4 (Catatan): Menentukan apakah DNS requests/queries ke nama sumber daya Anda diselesaikan ke alamat IPv4 pribadi dari instans EC2 ini.
   - Jawab permintaan nama host DNS IPv6 (catatan AAAA): Menentukan apakah DNS requests/queries ke nama sumber daya Anda diselesaikan ke alamat IPv6 (catatan AAAA) dari instans EC2 ini.
4. Pilih Simpan.

5. Jika Anda menghentikan instans, mulai lagi.

AWS CLI

Untuk memodifikasi jenis nama host dan opsi nama host DNS untuk sebuah instance

Gunakan perintah modify-private-dns-name-options.

```
aws ec2 modify-private-dns-name-options \
    --instance-id i-1234567890abcdef0 \
    --private-dns-hostname-type resource-name \
    --enable-resource-name-dns-a-record \
    --enable-resource-name-dns-aaaa-record
```

PowerShell

Untuk memodifikasi jenis nama host dan opsi nama host DNS untuk sebuah instance

Gunakan Edit-EC2PrivateDnsNameOptioncmdlet.

```
Edit-EC2PrivateDnsNameOption `
    -InstanceId i-1234567890abcdef0 `
    -PrivateDnsHostnameType ResourceName `
    -EnableResourceNameDnsAAAARecord $true`
    -EnableResourceNameDnsARecord $true
```

Bawa alamat IP Anda sendiri (BYOIP) ke Amazon EC2

Anda dapat membawa sebagian atau seluruh rentang IPv6 alamat yang dapat dirutekan IPv4 secara publik dari jaringan lokal ke jaringan lokal Anda. Akun AWS Anda terus mengontrol rentang alamat dan Anda dapat mengiklankan rentang alamat di internet melalui AWS. Setelah Anda membawa rentang alamat ke Amazon EC2, itu muncul di kumpulan alamat Anda Akun AWS .

> **Note**
>
> Dokumentasi ini menjelaskan cara membawa rentang alamat IP Anda sendiri untuk digunakan di Amazon EC2 saja. Untuk membawa rentang alamat IP Anda sendiri untuk digunakan AWS Global Accelerator, lihat Membawa alamat IP Anda sendiri (BYOIP) di

Panduan AWS Global Accelerator Pengembang. Untuk membawa rentang alamat IP Anda sendiri untuk digunakan Amazon VPC IP Address Manager, lihat Tutorial: Membawa alamat IP Anda ke IPAM di Panduan Pengguna Amazon VPC IPAM.

Saat Anda membawa rentang alamat IP ke AWS, AWS memvalidasi bahwa Anda mengontrol rentang alamat IP. Ada dua metode yang dapat Anda gunakan untuk menunjukkan bahwa Anda mengontrol rentang:

- Jika rentang alamat IP Anda terdaftar dengan Internet Registry yang mendukung RDAP (seperti ARIN, RIPE dan APNIC), Anda dapat memverifikasi kontrol domain Anda dengan sertifikat X.509 dengan menggunakan proses di halaman ini. Sertifikat hanya boleh berlaku selama proses penyediaan. Anda dapat menghapus sertifikat dari catatan RIR Anda setelah penyediaan selesai.
- Terlepas dari apakah Registri Internet Anda mendukung RDAP, Anda dapat menggunakan Amazon VPC IPAM untuk memverifikasi kontrol domain Anda dengan catatan DNS TXT. Proses itu didokumentasikan dalam Tutorial: Bawa alamat IP Anda ke IPAM di panduan Pengguna Amazon VPC IPAM.

Untuk informasi lebih lanjut, lihat AWS Online Tech talk Deep Dive on Bring Your Own IP.

Daftar Isi

- Definisi BYOIP
- Persyaratan dan kuota
- Ketersediaan wilayah
- Ketersediaan Local Zone
- Prasyarat untuk BYOIP di Amazon EC2
- Mengonboard rentang alamat Anda untuk digunakan di Amazon EC2
- Gunakan rentang alamat BYOIP Anda di Amazon EC2

Definisi BYOIP

- Sertifikat X.509 Self-sign — Standar sertifikat yang paling umum digunakan untuk mengenkripsi dan mengautentikasi data dalam jaringan. Ini adalah sertifikat yang digunakan oleh AWS untuk memvalidasi kontrol atas ruang IP dari catatan RDAP. Untuk informasi selengkapnya tentang sertifikat X.509, lihat RFC 3280.

- Nomor Sistem Otonom (ASN) — Pengidentifikasi unik global yang menentukan sekelompok prefiks IP yang dijalankan oleh satu atau lebih operator jaringan yang mempertahankan satu kebijakan perutean yang ditentukan dengan jelas.
- Regional Internet Registry (RIR) — Organisasi yang mengelola alokasi dan pendaftaran alamat IP dan ASNs dalam wilayah dunia.
- Registry Data Access Protocol (RDAP) — Protokol read-only untuk menanyakan data registrasi saat ini dalam RIR. Entri dalam basis data RIR yang ditanyakan disebut sebagai “catatan RDAP”. Tipe catatan tertentu perlu diperbarui oleh pelanggan melalui mekanisme yang disediakan RIR. Catatan ini ditanyakan oleh AWS untuk memverifikasi kontrol ruang alamat di RIR.
- Route Origin Authorization (ROA) — Objek yang dibuat oleh pelanggan RIRs untuk mengotentikasi iklan IP dalam sistem otonom tertentu. Untuk ikhtisar, lihat Otorisasi Asal Rute (ROAs) di situs web ARIN.
- Local Internet Registry (LIR) — Organisasi seperti penyedia layanan internet yang mengalokasikan blok alamat IP dari RIR untuk pelanggan mereka.

Persyaratan dan kuota

- Rentang alamat harus terdaftar di Regional Internet Registry (RIR) Anda. Lihat RIR Anda untuk kebijakan apa pun terkait wilayah geografis. BYOIP saat ini mendukung pendaftaran di American Registry for Internet Numbers (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE), atau Asia-Pacific Network Information Centre (APNIC). Rentang alamat ini harus didaftarkan untuk entitas bisnis atau kelembagaan dan tidak dapat didaftarkan untuk perorangan.
- Rentang IPv4 alamat paling spesifik yang dapat Anda bawa adalah/24.
- Rentang IPv6 alamat paling spesifik yang dapat Anda bawa adalah/48 untuk CIDRs yang dapat diiklankan secara publik dan /60 untuk CIDRs yang tidak dapat diiklankan secara publik.
- ROAs tidak diperlukan untuk rentang CIDR yang tidak dapat diiklankan secara publik, tetapi catatan RDAP masih perlu diperbarui.
- Anda dapat membawa setiap rentang alamat ke satu AWS Wilayah pada satu waktu.
- Anda dapat membawa total lima BYOIP IPv4 dan rentang IPv6 alamat per AWS Wilayah ke akun Anda AWS . Anda tidak dapat menyesuaikan kuota untuk BYOIP CIDRs menggunakan konsol Service Quotas, tetapi Anda dapat meminta peningkatan kuota dengan menghubungi Pusat AWS Dukungan seperti yang dijelaskan dalam kuota layanan di.AWSReferensi Umum AWS
- Anda tidak dapat membagikan rentang alamat IP Anda dengan akun lain AWS RAM kecuali Anda menggunakan Amazon VPC IP Address Manager (IPAM) dan mengintegrasikan IPAM dengan

Organizations. AWS Untuk informasi selengkapnya, lihat Mengintegrasikan IPAM dengan AWS Organizations di Panduan Pengguna Amazon VPC IPAM.

- Alamat dalam rentang alamat IP harus memiliki riwayat yang bersih. Kami mungkin menginvestigasi reputasi rentang alamat IP dan berhak menolak rentang alamat IP jika berisi alamat IP yang memiliki reputasi buruk atau terkait dengan perilaku jahat.
- Ruang alamat lama, ruang IPv4 alamat yang didistribusikan oleh registri pusat Internet Assigned Numbers Authority (IANA) sebelum pembentukan sistem Regional Internet Registry (RIR), masih membutuhkan objek ROA yang sesuai.
- Karena LIRs, adalah umum bahwa mereka menggunakan proses manual untuk memperbarui catatan mereka. Deployment bisa memakan waktu berhari-hari, tergantung pada LIR.
- Objek ROA tunggal dan catatan RDAP diperlukan untuk blok CIDR yang besar. Anda dapat membawa beberapa blok CIDR yang lebih kecil dari rentang itu ke AWS, bahkan di beberapa AWS Wilayah, menggunakan objek tunggal dan catatan.
- BYOIP tidak didukung untuk Wavelength Zones atau on. AWS Outposts
- Jangan membuat perubahan manual untuk BYOIP di RADb atau IRR lainnya. BYOIP akan diperbarui secara otomatis. RADb Setiap perubahan manual yang menyertakan ASN BYOIP akan menyebabkan operasi penyediaan BYOIP gagal.
- Setelah Anda membawa rentang IPv4 alamat AWS, Anda dapat menggunakan semua alamat IP dalam rentang tersebut, termasuk alamat pertama (alamat jaringan) dan alamat terakhir (alamat siaran).

Ketersediaan wilayah

Fitur BYOIP saat ini tersedia di semua Wilayah AWS komersial kecuali untuk Wilayah Tiongkok.

Ketersediaan Local Zone

Zona Lokal adalah perpanjangan dari AWS Wilayah dalam kedekatan geografis dengan pengguna Anda. Local Zones dikelompokkan ke dalam “grup perbatasan jaringan”. Di AWS, grup perbatasan jaringan adalah kumpulan Availability Zones (AZs), Local Zones, atau Wavelength Zones AWS tempat mengiklankan alamat IP publik. Local Zones mungkin memiliki grup perbatasan jaringan yang berbeda dari AZs di AWS Wilayah untuk memastikan latensi minimum atau jarak fisik antara AWS jaringan dan pelanggan yang mengakses sumber daya di Zona ini.

Anda dapat memberikan rentang BYOIPv4 alamat dan mengiklankannya di grup perbatasan jaringan Zona Lokal berikut menggunakan `--network-border-group` opsi:

- af-selatan-1-los-1
- ap-timur laut-1-tpe-1
- ap-selatan-1-ccu-1
- ap-selatan-1-del-1
- ap-tenggara 1-bkk-1
- ap-tenggara 1-mnl-1
- ap-tenggara 2-akl-1
- ap-tenggara 2-per-1
- eu-sentral-1-ham-1
- eu-sentral-1-waw-1
- eu-utara-1-cph-1
- eu-utara-1-hel-1
- saya-selatan-1-mct-1
- kami-timur-1-atl-2
- kami-timur-1-bos-1
- kami-timur-1-bue-1
- us-timur-1-chi-2
- us-east-1-dfw-2
- kami-timur-1-iah-2
- us-timur-1-lim-1
- us-timur-1-mci-1
- kami-timur-1-mia-2
- us-timur-1-msp-1
- kami-timur-1-nyc-1
- kami-timur-1-nyc-2
- kami-timur-1-phl-1
- us-timur-1-qro-1
- us-timur-1-scl-1
- us-barat-2-den-1
- kami-barat-2-hnl-1

- kami-barat-2-las-1
- us-west-2-lax-1
- kami-barat-2-pdx-1
- us-west-2-phx-2
- kami-barat-2-laut-1

Jika Local Zones diaktifkan (lihat Mengaktifkan Zona Lokal), Anda dapat memilih grup perbatasan jaringan untuk Local Zones saat Anda menyediakan dan mengiklankan BYOIPv4 CIDR. Pilih grup perbatasan jaringan dengan hati-hati karena EIP dan AWS sumber daya yang terkait dengannya harus berada di grup perbatasan jaringan yang sama.

> **Note**
>
> Anda tidak dapat menyediakan atau mengiklankan rentang BYOIPv6 alamat di Local Zones saat ini.

Prasyarat untuk BYOIP di Amazon EC2

Proses orientasi untuk BYOIP memiliki dua fase, di mana Anda harus melakukan tiga langkah. Langkah-langkah ini sesuai dengan langkah-langkah yang digambarkan dalam diagram berikut. Kami menyertakan langkah-langkah manual dalam dokumentasi ini, tetapi RIR Anda mungkin menawarkan layanan terkelola untuk membantu Anda dengan langkah-langkah ini.

> **Tip**
>
> Tugas-tugas pada bagian ini memerlukan terminal Linux dan dapat dijalankan menggunakan Linux, AWS CloudShell, atau Windows Subsystem for Linux.

Daftar Isi

- Ikhtisar
- Buat kunci privat dan buat sertifikat X.509
- Unggah sertifikat X.509 ke catatan RDAP di RIR Anda
- Membuat objek ROA di RIR Anda

Ikhtisar

Fase persiapan

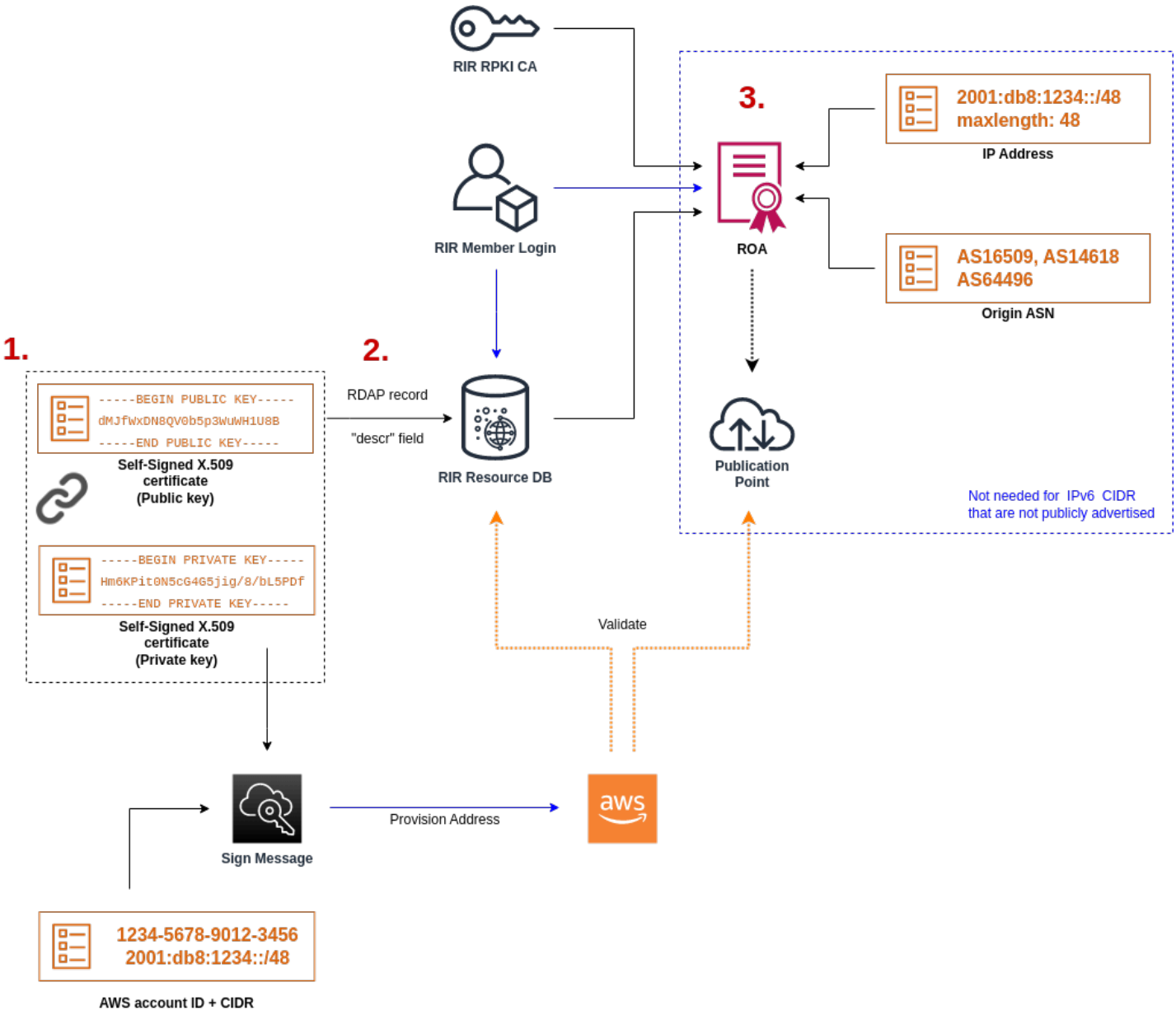
[1] Buat kunci pribadi dan gunakan untuk menghasilkan sertifikat X.509 yang ditandatangani sendiri untuk tujuan otentikasi. Sertifikat ini hanya digunakan selama fase penyediaan. Anda dapat menghapus sertifikat dari catatan RIR Anda setelah penyediaan selesai

Fase konfigurasi RIR

[2] Unggah sertifikat yang ditandatangani sendiri ke komentar catatan RDAP Anda.

[3] Buat objek ROA di RIR Anda. ROA mendefinisikan rentang alamat yang diinginkan, Nomor Sistem Otonom (ASNs) diizinkan untuk mengiklankan rentang alamat, dan tanggal kedaluwarsa untuk mendaftar dengan Resource Public Key Infrastructure (RPKI) RIR Anda.

> **Note**
>
> ROA tidak diperlukan untuk ruang alamat yang tidak dapat diiklankan secara publik. IPv6



Untuk membawa beberapa rentang alamat yang tidak berdekatan, Anda harus mengulangi proses ini dengan setiap rentang alamat. Namun, persiapan dan langkah konfigurasi RIR tidak perlu diulang jika memisahkan blok yang berdekatan di beberapa Wilayah yang berbeda. AWS

Membawa rentang alamat tidak berpengaruh pada setiap rentang alamat yang Anda bawa sebelumnya.

Buat kunci privat dan buat sertifikat X.509

Gunakan prosedur berikut untuk membuat sertifikat X.509 yang ditandatangani sendiri dan menambahkannya ke catatan RDAP untuk RIR Anda. Pasangan kunci ini digunakan untuk

mengautentikasi rentang alamat dengan RIR. Perintah openssl memerlukan OpenSSL versi 1.0.2 atau lebih baru.

Salin perintah berikut dan mengganti nilai placeholder saja (dalam teks miring berwarna).

Prosedur ini mengikuti praktik terbaik mengenkripsi kunci RSA privat Anda dan memerlukan frasa sandi untuk mengaksesnya.

1. Buat kunci privat RSA 2048 bit seperti yang ditunjukkan berikut ini.

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
 private-key.pem
```

Parameter `-aes256` menentukan algoritma yang digunakan untuk mengenkripsi kunci privat. Perintah mengembalikan output berikut, termasuk petunjuk untuk mengatur frasa sandi:

```
......+++
.+++
Enter PEM pass phrase: xxxxxxx
Verifying - Enter PEM pass phrase: xxxxxxx
```

Anda dapat memeriksa kunci menggunakan perintah berikut:

```
$ openssl pkey -in private-key.pem -text
```

Ini mengembalikan prompt frasa-sandi dan isi kunci, yang harus mirip dengan berikut ini:

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
```

```
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
```

```
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
```

```
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Simpan kunci privat Anda di lokasi yang aman saat tidak digunakan.

2. Buat sertifikat X.509 menggunakan kunci privat yang dibuat pada langkah sebelumnya. Dalam contoh ini, sertifikat kedaluwarsa dalam 365 hari, setelahnya sertifikat tidak dapat dipercaya. Pastikan Anda mengatur waktu kedaluwarsa dengan tepat. Sertifikat hanya boleh berlaku selama proses penyediaan. Anda dapat menghapus sertifikat dari catatan RIR Anda setelah penyediaan selesai. Perintah `tr -d "\n"` menghapus karakter baris baru (jeda baris) dari output. Anda harus memberikan Nama Umum saat diminta, tetapi bidang lainnya dapat dibiarkan kosong.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Ini menghasilkan output serupa dengan yang berikut ini:

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
```

```
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> Nama Umum tidak diperlukan untuk AWS penyediaan. Itu bisa berupa nama domain internal atau publik.

Anda dapat memeriksa sertifikat dengan perintah berikut:

```
$ cat certificate.pem
```

Output harus berupa string panjang, dengan enkode PEM tanpa jeda baris, diawali dengan `-----BEGIN CERTIFICATE-----` dan diikuti oleh `-----END CERTIFICATE-----`.

Unggah sertifikat X.509 ke catatan RDAP di RIR Anda

Tambahkan sertifikat yang telah Anda buat sebelumnya ke catatan RDAP untuk RIR Anda. Pastikan untuk memasukkan string `-----BEGIN CERTIFICATE-----` dan `-----END CERTIFICATE-----` sebelum dan sesudah bagian yang dikodekan. Semua konten ini harus dalam satu baris panjang. Prosedur untuk memperbarui RDAP tergantung pada RIR Anda:

- Untuk ARIN, gunakan portal Manajer Akun untuk menambahkan sertifikat di bagian “Komentar Publik” untuk objek “Informasi Jaringan” yang mewakili rentang alamat Anda. Jangan menambahkannya ke bagian komentar untuk organisasi Anda.
- Untuk RIPE, tambahkan sertifikat sebagai bidang “descr” baru ke objek “inetnum” atau “inet6num” yang mewakili rentang alamat Anda. Ini biasanya dapat ditemukan di bagian “Sumber Daya Saya” di portal Basis Data RIPE. Jangan menambahkannya ke bagian komentar untuk organisasi Anda atau bidang “komentar” dari objek di atas.
- Untuk APNIC, tambahkan sertifikat dengan mengedit komentar pada catatan “inetnum” atau “inet6num”.

Anda dapat menghapus sertifikat dari catatan RIR Anda setelah tahap penyediaan di bawah ini selesai.

Membuat objek ROA di RIR Anda

Buat objek ROA untuk mengotorisasi Amazon ASNs 16509 dan 14618 untuk mengiklankan rentang alamat Anda, serta ASNs yang saat ini berwenang untuk mengiklankan rentang alamat. Untuk AWS GovCloud (US) Regions, otorisasi ASN 8987 bukan 16509 dan 14618. Anda harus mengatur panjang maksimum ke ukuran CIDR yang Anda bawa. IPv4 Awalan paling spesifik yang dapat Anda bawa adalah/24. Rentang IPv6 alamat paling spesifik yang dapat Anda bawa adalah/48 untuk CIDRs yang dapat diiklankan secara publik dan /60 untuk CIDRs yang tidak dapat diiklankan secara publik.

> **Important**
>
> Jika Anda membuat objek ROA untuk Amazon VPC IP Address Manager (IPAM), saat Anda membuat ROAs, IPv4 CIDRs untuk Anda harus mengatur panjang maksimum awalan alamat IP ke. `/24` Karena IPv6 CIDRs, jika Anda menambahkannya ke kumpulan yang dapat diiklankan, panjang maksimum awalan alamat IP harus. `/48` Ini memastikan bahwa Anda memiliki fleksibilitas penuh untuk membagi alamat IP publik Anda di seluruh AWS Wilayah. IPAM memberlakukan panjang maksimum yang Anda tetapkan. Untuk informasi selengkapnya tentang alamat BYOIP ke IPAM, lihat Tutorial: Alamat BYOIP ke IPAM CIDRs di Panduan Pengguna Amazon VPC IPAM.

Ini mungkin perlu waktu hingga 24 jam agar ROA tersedia di Amazon. Untuk informasi lebih lanjut, konsultasikan RIR Anda:

- ARIN — Permintaan ROA
- RIPE - Mengelola ROAs
- APNIC — Manajemen Rute

Saat memigrasikan iklan dari beban kerja lokal ke tempat AWS, Anda harus membuat ROA untuk ASN yang ada sebelum membuat untuk Amazon. ROAs ASNs Jika tidak, Anda mungkin melihat dampak pada perutean dan iklan yang ada.

> **Important**
>
> Agar Amazon dapat mengiklankan dan terus mengiklankan rentang alamat IP Anda ROAs , Amazon Anda ASNs harus mematuhi pedoman di atas. Jika Anda ROAs tidak valid atau tidak sesuai dengan pedoman di atas, Amazon berhak untuk berhenti mengiklankan rentang alamat IP Anda.

> **Note**
>
> Langkah ini tidak diperlukan untuk ruang alamat yang tidak dapat diiklankan secara publik. IPv6

Mengonboard rentang alamat Anda untuk digunakan di Amazon EC2

Proses orientasi untuk BYOIP mencakup tugas-tugas berikut, tergantung pada kebutuhan Anda.

Tugas

- Menyediakan rentang alamat yang dapat diiklankan secara publik di AWS
- Menyediakan rentang IPv6 alamat yang tidak dapat diiklankan secara publik
- Iklankan rentang alamat melalui AWS
- Mencabut akses rentang alamat
- Validasi BYOIP Anda

Menyediakan rentang alamat yang dapat diiklankan secara publik di AWS

Saat Anda memberikan rentang alamat untuk digunakan AWS, Anda mengonfirmasi bahwa Anda mengontrol rentang alamat dan mengizinkan Amazon untuk mengiklankannya. Kami juga memverifikasi bahwa Anda mengontrol rentang alamat melalui pesan otorisasi yang ditandatangani. Pesan ini ditandatangani dengan key pair X.509 yang ditandatangani sendiri yang Anda gunakan saat memperbarui catatan RDAP dengan sertifikat X.509. AWS memerlukan pesan otorisasi yang ditandatangani secara kriptografis yang disajikan kepada RIR. RIR mengotentikasi tanda tangan terhadap sertifikat yang ditambahkan ke RDAP, dan memeriksa rincian otorisasi terhadap ROA.

Untuk menyediakan rentang alamat

1. Membuat pesan

   Menulis pesan otorisasi teks biasa. Format pesan adalah sebagai berikut, di mana tanggal tersebut adalah tanggal kedaluwarsa pesan:

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Ganti nomor akun, rentang alamat, dan tanggal kedaluwarsa dengan nilai Anda sendiri untuk membuat pesan yang menyerupai hal berikut ini:

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Ini agar tidak menjadi bingung dengan pesan ROA, yang memiliki tampilan serupa.

2. Menandatangani pesan

   Menandatangani pesan teks biasa menggunakan kunci privat yang telah Anda buat sebelumnya. Tanda tangan yang dikembalikan oleh perintah ini adalah string panjang yang perlu Anda gunakan pada langkah berikutnya.

   > **Important**
   >
   > Kami sarankan Anda menyalin dan menempelkan perintah ini. Kecuali untuk isi pesan, jangan mengubah atau mengganti nilai apa pun.

   ```
   signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
    rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
    | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
   ```

3. Penyediaan alamat

   Gunakan AWS CLI provision-byoip-cidrperintah untuk menyediakan rentang alamat. Opsi `--cidr-authorization-context` menggunakan string pesan dan tanda tangan yang telah Anda buat sebelumnya.

> **Important**
>
> Anda harus menentukan AWS Wilayah di mana rentang BYOIP harus disediakan jika berbeda dari Konfigurasi. AWS CLI `Default region name`

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --region us-east-1
```

Penyediaan rentang alamat adalah operasi asinkron, sehingga panggilan segera kembali, tetapi rentang alamat belum siap untuk digunakan hingga statusnya berubah dari `pending-provision` menjadi `provisioned`.

4. Memantau kemajuan

   Meskipun sebagian besar penyediaan akan selesai dalam waktu dua jam, mungkin diperlukan waktu hingga satu minggu untuk menyelesaikan proses penyediaan untuk rentang yang dapat diiklankan secara publik. Gunakan describe-byoip-cidrsperintah untuk memantau kemajuan, seperti dalam contoh ini:

   ```
   aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
   ```

   Jika ada masalah selama penyediaan dan status masuk ke `failed-provision`, Anda harus menjalankan perintah `provision-byoip-cidr` lagi setelah masalah terpecahkan.

Menyediakan rentang IPv6 alamat yang tidak dapat diiklankan secara publik

Secara default, rentang alamat disediakan agar dapat diiklankan secara publik ke internet. Anda dapat memberikan rentang IPv6 alamat yang tidak dapat diiklankan secara publik. Untuk rute yang tidak dapat diakses secara publik, proses penyediaan umumnya selesai dalam hitungan menit. Saat Anda mengaitkan blok IPv6 CIDR dari rentang alamat non-publik dengan VPC, IPv6 CIDR hanya dapat diakses melalui opsi konektivitas hibrida yang mendukung IPv6, seperti, Direct ConnectVPN, AWS Site-to-Site atau Amazon VPC Transit Gateway.

ROA tidak diperlukan untuk menyediakan rentang alamat non-publik.

> **Important**
>
> - Anda hanya dapat menentukan apakah rentang alamat dapat diiklankan secara publik selama penyediaan. Anda tidak dapat mengubah status yang dapat diiklankan dari rentang alamat di lain waktu.
> - Amazon VPC tidak mendukung alamat lokal unik (ULA). CIDRs Semua VPCs harus memiliki keunikan IPv6 CIDRs. Dua tidak VPCs dapat memiliki rentang IPv6 CIDR yang sama.

Untuk menyediakan rentang IPv6 alamat yang tidak dapat diiklankan secara publik, gunakan perintah berikut. provision-byoip-cidr

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Iklankan rentang alamat melalui AWS

Setelah rentang alamat disediakan, rentang alamat tersebut siap untuk diiklankan. Anda harus mengiklankan rentang alamat persis yang Anda sediakan. Anda tidak dapat mengiklankan hanya sebagian dari rentang alamat yang disediakan.

Jika Anda menyediakan rentang IPv6 alamat yang tidak akan diiklankan secara publik, Anda tidak perlu menyelesaikan langkah ini.

Kami menyarankan Anda berhenti mengiklankan rentang alamat atau bagian dari rentang dari lokasi lain sebelum Anda mengiklankannya. AWS Jika Anda terus mengiklankan rentang alamat IP Anda atau bagiannya dari lokasi lain, kami tidak dapat mendukung atau memecahkan masalah dengan andal. Secara khusus, kami tidak dapat menjamin bahwa lalu lintas ke rentang alamat atau sebagian dari rentang akan memasuki jaringan kami.

Untuk meminimalkan waktu henti, Anda dapat mengonfigurasi AWS sumber daya Anda untuk menggunakan alamat dari kumpulan alamat Anda sebelum diiklankan, dan kemudian secara bersamaan berhenti mengiklankannya dari lokasi saat ini dan mulai mengiklankannya. AWS Untuk informasi lebih lanjut tentang pengalokasian alamat IP Elastis dari kumpulan alamat Anda, lihat Mengalokasikan alamat IP Elastis.

Batasan

- Anda dapat menjalankan perintah advertise-byoip-cidr maksimal sekali setiap 10 detik, meskipun Anda menentukan rentang alamat yang berbeda setiap kali melakukannya.
- Anda dapat menjalankan perintah withdraw-byoip-cidr maksimal sekali setiap 10 detik, meskipun Anda menentukan rentang alamat yang berbeda setiap kali melakukannya.

Untuk mengiklankan rentang alamat, gunakan advertise-byoip-cidrperintah berikut.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Untuk berhenti mengiklankan rentang alamat, gunakan withdraw-byoip-cidrperintah berikut.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Mencabut akses rentang alamat

Untuk berhenti menggunakan rentang alamat Anda AWS, pertama-tama lepaskan alamat IP Elastis apa pun dan lepaskan blok IPv6 CIDR yang masih dialokasikan dari kumpulan alamat. Kemudian, hentikan iklan rentang alamat, dan terakhir, cabut akses rentang alamat.

Anda tidak dapat mencabut akses sebagian rentang alamat. Jika Anda ingin menggunakan rentang alamat yang lebih spesifik AWS, hentikan penyediaan seluruh rentang alamat dan berikan rentang alamat yang lebih spesifik.

(IPv4) Untuk melepaskan setiap alamat IP Elastis, gunakan perintah alamat rilis berikut.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Untuk memisahkan blok IPv6 CIDR, gunakan perintah berikut disassociate-vpc-cidr-block.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Untuk berhenti mengiklankan rentang alamat, gunakan withdraw-byoip-cidrperintah berikut.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Untuk menghentikan rentang alamat, gunakan deprovision-byoip-cidrperintah berikut.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

Diperlukan waktu hingga satu hari untuk mencabut akses rentang alamat.

Validasi BYOIP Anda

1. Validasi pasangan kunci x.509 yang ditandatangani sendiri

   Validasi bahwa sertifikat telah diunggah dan valid melalui perintah whois.

   Untuk ARIN, gunakan `whois -h whois.arin.net r + 2001:0DB8:6172::/48` untuk mencari catatan RDAP untuk rentang alamat Anda. Periksa `Public Comments` bagian untuk `NetRange` (rentang jaringan) di output perintah. Sertifikat harus ditambahkan di `Public Comments` bagian untuk rentang alamat.

   Anda dapat memeriksa sertifikat yang `Public Comments` berisi menggunakan perintah berikut:

   ```
   whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
   ```

   Ini mengembalikan output dengan isi kunci, yang harus mirip dengan berikut ini:

   ```
   Public Comments:
   -----BEGIN CERTIFICATE-----
   MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
   LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
   hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
   wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
   NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
   rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
   VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
   W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
   R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
   prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
   mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
   Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
   xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
   3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
   AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
   QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
   08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
   Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
   ```

```
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Untuk RIPE, gunakan `whois -r -h whois.ripe.net` *`2001:0DB8:7269::/48`* untuk mencari catatan RDAP untuk rentang alamat Anda. Periksa bagian `descr` untuk objek `inetnum` (rentang jaringan) di output perintah. Sertifikat harus ditambahkan sebagai bidang `descr` baru untuk rentang alamat.

Anda dapat memeriksa sertifikat yang `descr` berisi menggunakan perintah berikut:

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Ini mengembalikan output dengan isi kunci, yang harus mirip dengan berikut ini:

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Untuk APNIC, gunakan `whois -h whois.apnic.net` *`2001:0DB8:6170::/48`* untuk mencari catatan RDAP untuk rentang alamat BYOIP Anda. Periksa bagian `remarks` untuk objek `inetnum` (rentang jaringan) di output perintah. Sertifikat harus ditambahkan sebagai bidang `remarks` baru untuk rentang alamat.

Anda dapat memeriksa sertifikat yang `remarks` berisi menggunakan perintah berikut:

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Ini mengembalikan output dengan isi kunci, yang harus mirip dengan berikut ini:

```
remarks:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Validasi pembuatan objek ROA

   Validasi keberhasilan pembuatan objek ROA menggunakan RIPEstat Data API. Pastikan untuk menguji rentang alamat Anda terhadap Amazon ASNs 16509 dan 14618, ditambah ASNs yang saat ini berwenang untuk mengiklankan rentang alamat.

Anda dapat memeriksa objek ROA dari Amazon yang berbeda ASNs dengan rentang alamat Anda dengan menggunakan perintah berikut:

```
curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
resource=ASN&prefix=CIDR
```

Dalam contoh output ini, respons memiliki hasil `"status": "valid"` untuk Amazon ASN 16509. Ini menunjukkan objek ROA untuk rentang alamat berhasil dibuat:


```
{
    "messages": [],
    "see_also": [],
    "version": "0.3",
    "data_call_name": "rpki-validation",
    "data_call_status": "supported",
    "cached": false,
    "data": {
        "validating_roas": [
            {
                "origin": "16509",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "valid"
            },
            {
                "origin": "14618",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            },
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
```

```
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```

Status "`unknown`" menunjukkan objek ROA untuk rentang alamat belum dibuat. Status "`invalid_asn`" menunjukkan bahwa objek ROA untuk rentang alamat tidak berhasil dibuat.

Gunakan rentang alamat BYOIP Anda di Amazon EC2

Anda dapat melihat dan menggunakan rentang IPv6 alamat IPv4 dan yang telah Anda sediakan di akun Anda. Untuk informasi selengkapnya, lihat the section called "Di atas jangkauan alamat Anda".

IPv4 rentang alamat

Anda dapat membuat alamat IP Elastis dari kumpulan IPv4 alamat Anda dan menggunakannya dengan AWS sumber daya Anda, seperti instans EC2, gateway NAT, dan Network Load Balancers.

Untuk melihat informasi tentang kumpulan IPv4 alamat yang telah Anda sediakan di akun, gunakan perintah describe-public-ipv4-pool berikut.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Untuk membuat alamat IP Elastis dari kumpulan IPv4 alamat Anda, gunakan perintah allocate-address. Anda dapat menggunakan opsi `--public-ipv4-pool` untuk menentukan ID dari kumpulan alamat yang dikembalikan oleh `describe-byoip-cidrs`. Atau Anda dapat menggunakan opsi `--address` untuk menentukan alamat dari rentang alamat yang Anda sediakan.

IPv6 rentang alamat

Untuk melihat informasi tentang kumpulan IPv6 alamat yang telah Anda sediakan di akun, gunakan perintah describe-ipv6-pools berikut.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Untuk membuat VPC dan menentukan IPv6 CIDR dari kumpulan IPv6 alamat Anda, gunakan perintah create-vpc berikut. Untuk membiarkan Amazon memilih IPv6 CIDR dari kumpulan IPv6 alamat Anda, hilangkan opsi. `--ipv6-cidr-block`

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Untuk mengaitkan blok IPv6 CIDR dari kumpulan IPv6 alamat Anda dengan VPC, gunakan perintah berikut. associate-vpc-cidr-block Untuk membiarkan Amazon memilih IPv6 CIDR dari kumpulan IPv6 alamat Anda, hilangkan opsi. `--ipv6-cidr-block`

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Untuk melihat informasi kumpulan IPv6 alamat Anda VPCs dan yang terkait, gunakan perintah deskripsi-vpcs. Untuk melihat informasi tentang blok IPv6 CIDR terkait dari kumpulan IPv6 alamat tertentu, gunakan perintah get-associated-ipv6-pool-cidrs berikut.

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Jika Anda memisahkan blok IPv6 CIDR dari VPC Anda, itu dilepaskan kembali ke kumpulan alamat Anda. IPv6

Alamat Elastic IP

Alamat IP Elastis adalah IPv4 alamat statis yang dirancang untuk komputasi awan dinamis. Alamat IP Elastis dialokasikan ke AWS akun Anda, dan menjadi milik Anda sampai Anda melepaskannya. Dengan alamat IP Elastis, Anda dapat menutupi kegagalan suatu instans atau perangkat lunak dengan meremajakan secara cepat alamat ke instans lain di akun Anda. Atau, Anda dapat menentukan alamat IP Elastis dalam catatan DNS untuk domain Anda, sehingga domain Anda menunjuk ke instans Anda. Untuk informasi selengkapnya, lihat dokumentasi untuk registrar domain Anda.

Alamat IP Elastis adalah IPv4 alamat publik, yang dapat dijangkau dari internet. Jika Anda perlu terhubung ke instans yang tidak memiliki IPv4 alamat publik, Anda dapat mengaitkan alamat IP Elastis dengan instans Anda untuk mengaktifkan komunikasi dengan internet.

Daftar Isi

- Harga alamat IP Elastis
- Dasar alamat IP Elastis
- Kuota alamat IP Elastis
- Mengaitkan alamat IP Elastis dengan instans
- Transfer alamat IP Elastis antara Akun AWS
- Merilis alamat IP Elastis
- Buat catatan DNS terbalik untuk email di Amazon EC2

Harga alamat IP Elastis

Ada biaya untuk semua alamat IP Elastic apakah mereka sedang digunakan (dialokasikan ke sumber daya, seperti instans EC2) atau idle (dibuat di akun Anda tetapi tidak dialokasikan).

AWS mengenakan biaya untuk semua IPv4 alamat publik, termasuk IPv4 alamat publik yang terkait dengan instans yang sedang berjalan dan alamat IP Elastis. Untuk informasi selengkapnya, lihat tab IPv4 Alamat Publik di halaman harga Amazon VPC.

Dasar alamat IP Elastis

Berikut adalah karakteristik dasar dari alamat IP Elastis:

- Alamat IP Elastis bersifat statis; alamat ini tidak berubah seiring waktu.
- Alamat IP Elastis hanya untuk digunakan di Wilayah tertentu saja, dan tidak dapat dipindahkan ke Wilayah yang berbeda.
- Alamat IP Elastis berasal dari kumpulan IPv4 alamat Amazon, atau dari kumpulan IPv4 alamat khusus yang telah Anda bawa ke alamat Anda Akun AWS. Kami tidak mendukung alamat IP Elastis untuk IPv6.
- Untuk menggunakan alamat IP Elastis, pertama-tama Anda mengalokasikannya ke akun Anda, lalu mengaitkannya dengan instans atau antarmuka jaringan.
- Ketika Anda mengaitkan alamat IP Elastis dengan sebuah instans, alamat ini juga dikaitkan dengan antarmuka jaringan primer instans tersebut. Ketika Anda mengaitkan alamat IP Elastis dengan sebuah antarmuka jaringan yang ditambahkan ke sebuah instans, alamat ini juga dikaitkan dengan instans tersebut.
- Saat Anda mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan utamanya, jika instans sudah memiliki IPv4 alamat publik yang terkait dengannya, IPv4 alamat publik tersebut

dilepaskan kembali ke kumpulan IPv4 alamat publik Amazon dan alamat IP Elastis dikaitkan dengan instans sebagai gantinya. Anda tidak dapat menggunakan kembali IPv4 alamat publik yang sebelumnya terkait dengan instans dan Anda tidak dapat mengonversi IPv4 alamat publik tersebut menjadi alamat IP Elastis. Untuk informasi selengkapnya, lihat IPv4 Alamat publik.

- Anda dapat memisahkan alamat IP Elastis dari sumber daya, kemudian mengaitkannya dengan sumber daya yang berbeda. Untuk menghindari perilaku yang tidak terduga, pastikan semua koneksi aktif ke sumber daya yang disebutkan dalam kaitan yang ada ditutup sebelum Anda melakukan perubahan. Setelah Anda mengaitkan alamat IP Elastis Anda ke sumber daya yang berbeda, Anda dapat membuka kembali koneksi Anda ke sumber daya yang baru saja dikaitkan.
- Alamat IP Elastis yang tidak terkait tetap dialokasikan ke akun Anda hingga Anda secara eksplisit melepasnya. Anda dikenakan biaya untuk semua alamat IP Elastic di akun Anda, terlepas dari apakah alamat tersebut terkait atau tidak terkait dengan instans. Untuk informasi selengkapnya, lihat tab IPv4 Alamat Publik di halaman harga Amazon VPC.
- Saat Anda mengaitkan alamat IP Elastis dengan instance yang sebelumnya memiliki IPv4 alamat publik, nama host DNS publik dari instance tersebut berubah agar sesuai dengan alamat IP Elastis.
- Kami menyelesaikan nama host DNS publik ke IPv4 alamat publik atau alamat IP Elastis dari instance di luar jaringan instance, dan ke IPv4 alamat pribadi instance dari dalam jaringan instance.
- Ketika Anda mengalokasikan alamat IP Elastis dari kumpulan alamat IP yang telah Anda bawa ke AWS akun Anda, itu tidak dihitung terhadap batas alamat IP Elastis Anda. Untuk informasi selengkapnya, lihat Kuota alamat IP Elastis.
- Saat Anda mengalokasikan alamat IP Elastis, Anda dapat mengaitkan alamat IP Elastis dengan grup border jaringan. Ini adalah lokasi tempat kita mengiklankan blok CIDR. Mengatur grup perbatasan jaringan membatasi blok CIDR ke grup ini. Jika Anda tidak menentukan grup batas jaringan, kami menetapkan grup batas yang berisi semua Zona Ketersediaan di Wilayah tersebut (misalnya, `us-west-2`).
- Alamat IP Elastis hanya untuk digunakan dalam grup batas jaringan tertentu.

Kuota alamat IP Elastis

Secara default, semua Akun AWS memiliki kuota lima (5) alamat IP elastis per Wilayah, karena alamat internet publik (IPv4) adalah sumber daya publik yang langka. Kami sangat menyarankan agar Anda menggunakan alamat IP Elastic terutama karena kemampuannya memetakan ulang alamat ke instans lain jika terjadi kegagalan instans, dan menggunakan nama host DNS untuk semua komunikasi antar simpul lainnya.

Jika menurut Anda arsitektur Anda menjamin alamat IP Elastis tambahan, Anda dapat meminta peningkatan kuota secara langsung dari konsol Kuota Layanan. Untuk meminta kenaikan kuota, pilih Permintaan peningkatan di tingkat akun. Untuk informasi selengkapnya, lihat Kuota EC2 layanan Amazon.

Mengaitkan alamat IP Elastis dengan instans

Setelah Anda mengalokasikan alamat IP Elastis, Anda dapat mengaitkannya dengan AWS sumber daya, seperti instans EC2, gateway NAT, atau Network Load Balancer. Untuk mengaitkan alamat IP Elastis dengan AWS sumber daya yang berbeda nanti, Anda dapat memisahkannya dari sumber daya saat ini dan kemudian mengaitkannya dengan sumber daya baru.

Tugas

- Mengalokasikan alamat IP Elastis
- Kaitkan sebuah alamat IP Elastis
- Pisahkan alamat IP Elastis

Mengalokasikan alamat IP Elastis

Anda dapat mengalokasikan alamat IP Elastis untuk digunakan di Wilayah. Ada biaya untuk semua alamat IP Elastic apakah mereka sedang digunakan (terkait dengan sumber daya, seperti instans EC2) atau idle (dibuat di akun Anda tetapi tidak terkait).

Console

Untuk mengalokasikan Alamat IP elastis

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Jaringan & Keamanan, Elastis IPs.
3. Pilih Alokasi alamat IP elastis.
4. (Opsional) Ketika Anda mengalokasikan alamat IP elastis (EIP), Anda memilih grup batas jaringan untuk mengalokasikan EIP. Grup perbatasan jaringan adalah kumpulan Availability Zones (AZs), Local Zones, atau Wavelength Zones AWS yang mengiklankan alamat IP publik. Local Zones dan Wavelength Zones mungkin memiliki grup perbatasan jaringan yang berbeda dari AZs di Wilayah untuk memastikan latensi minimum atau jarak fisik antara jaringan dan pelanggan yang mengakses sumber AWS daya di Zona ini.

> **Important**
>
> Anda harus mengalokasikan EIP dalam grup perbatasan jaringan yang sama dengan AWS sumber daya yang akan dikaitkan dengan EIP. EIP dalam satu grup perbatasan jaringan hanya dapat diiklankan di zona dalam grup perbatasan jaringan tersebut dan tidak di zona lain yang diwakili oleh grup perbatasan jaringan lainnya.

Jika Anda mengaktifkan Local Zones atau Wavelength Zone (untuk informasi selengkapnya, lihat Mengaktifkan Zona Lokal atau Aktifkan Zona Wavelength), Anda dapat memilih grup perbatasan jaringan untuk, Local Zones, atau Wavelength Zones. AZs Pilih grup perbatasan jaringan dengan hati-hati karena EIP dan sumber daya AWS yang terkait dengannya harus berada di grup perbatasan jaringan yang sama. Anda dapat menggunakan konsol EC2 untuk melihat grup perbatasan jaringan tempat Availability Zone, Local Zones, atau Wavelength Zone Anda berada. Biasanya, semua Zona Ketersediaan di Wilayah milik grup perbatasan jaringan yang sama, sedangkan Local Zones atau Wavelength Zone milik grup perbatasan jaringan mereka sendiri yang terpisah.

Jika Anda tidak mengaktifkan Local Zones atau Wavelength Zones, ketika Anda mengalokasikan EIP, grup perbatasan jaringan yang mewakili semua untuk Wilayah (`us-west-2`seperti) telah ditentukan sebelumnya untuk Anda dan Anda tidak dapat mengubahnya. AZs Ini berarti bahwa EIP yang Anda alokasikan ke grup perbatasan jaringan ini akan diiklankan AZs di semua wilayah tempat Anda berada.

5. Untuk kumpulan IPv4 alamat Publik, pilih salah satu dari berikut ini:

   - Kumpulan IPv4 alamat Amazon —Jika Anda ingin IPv4 alamat dialokasikan dari kumpulan alamat Amazon. IPv4
   - IPv4 Alamat publik yang Anda bawa ke AWS akun Anda —Jika Anda ingin mengalokasikan alamat publik yang tidak bersebelahan (tidak berurutan) dari kumpulan IPv4 alamat IP yang telah Anda bawa ke akun Anda. AWS Opsi ini dinonaktifkan jika Anda tidak memiliki kumpulan alamat IP. Untuk informasi selengkapnya tentang membawa rentang alamat IP Anda sendiri ke AWS akun Anda, lihatBawa alamat IP Anda sendiri (BYOIP) ke Amazon EC2.
   - Kumpulan IPv4 alamat milik pelanggan —Jika Anda ingin mengalokasikan IPv4 alamat dari kumpulan yang dibuat dari jaringan lokal untuk digunakan dengan Outpost. AWS Opsi ini dinonaktifkan jika Anda tidak memiliki AWS Outpost.

- Alokasikan menggunakan IPv4 kolam IPAM: Jika Anda ingin mengalokasikan alamat IP Elastis berurutan dari blok publik yang berdekatan di kolam IPAM. IPv4 Mengalokasikan alamat IP Elastis berurutan dapat secara signifikan mengurangi overhead manajemen untuk daftar kontrol akses keamanan dan menyederhanakan alokasi dan pelacakan alamat IP untuk penskalaan perusahaan. AWS Untuk informasi selengkapnya, lihat Mengalokasikan alamat IP Elastis berurutan dari kumpulan IPAM di Panduan Pengguna Amazon VPC IPAM.

6. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.

AWS CLI

Untuk mengalokasikan alamat Elastic IP

Gunakan perintah AWS CLI allocate-address.

Dalam contoh berikut, Amazon EC2 memilih alamat dari kumpulan alamat Amazon.

```
aws ec2 allocate-address
```

Dalam contoh berikut, Amazon EC2 memilih alamat dari kumpulan tertentu yang Anda bawa menggunakan BYOIP. AWS

```
aws ec2 allocate-address \
    --public-ipv4-pool ipv4pool-ec2-012345abcdef67890
```

Contoh berikut menentukan alamat dari kolam IPv4 IPAM tertentu.

```
aws ec2 allocate-address \
    --ipam-pool-id ipam-pool-1234567890abcdef0 \
    --address 192.0.2.0
```

PowerShell

Untuk mengalokasikan Alamat IP elastis

Gunakan New-EC2Addresscmdlet.

Dalam contoh berikut, Amazon EC2 memilih alamat dari kumpulan alamat Amazon.

```
New-EC2Address
```

Dalam contoh berikut, Amazon EC2 memilih alamat dari kumpulan tertentu yang Anda bawa menggunakan BYOIP. AWS

```
New-EC2Address `
    -PublicIpv4Pool ipv4pool-ec2-012345abcdef67890
```

Contoh berikut menentukan alamat dari kolam IPv4 IPAM tertentu.

```
New-EC2Address `
    -IpamPoolId ipam-pool-1234567890abcdef0 `
    -Address 192.0.2.0
```

Kaitkan sebuah alamat IP Elastis

Jika Anda mengaitkan sebuah alamat IP Elastis dengan instans Anda untuk mengaktifkan komunikasi dengan internet, Anda juga harus memastikan bahwa instans Anda berada dalam subnet publik. Untuk informasi selengkapnya, lihat Mengaktifkan akses internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.

Console

Untuk mengaitkan alamat IP Elastis dengan sebuah instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Elastic IPs.
3. Pilih alamat IP Elastis untuk dikaitkan dan pilih Tindakan, Kaitkan alamat IP Elastis.
4. Untuk Tipe sumber daya, pilih Instans.
5. Untuk instans, pilih instans yang akan dikaitkan dengan alamat IP Elastis. Anda juga dapat memasukkan teks untuk mencari instans tertentu.
6. (Opsional) Untuk Alamat IP privat, tentukan IT alamat IP privat yang akan dikaitkan dengan alamat IP Elastis.
7. Pilih Kaitkan.

Untuk mengaitkan alamat IP Elastis dengan antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Elastic IPs.
3. Pilih alamat IP Elastis untuk dikaitkan dan pilih Tindakan, Kaitkan alamat IP Elastis.
4. Untuk Tipe sumber daya, pilih Antarmuka jaringan.
5. Untuk Antarmuka jaringan, pilih antarmuka jaringan yang akan dikaitkan dengan alamat IP Elastis. Anda juga dapat memasukkan teks untuk mencari antarmuka jaringan spesifik.
6. (Opsional) Untuk Alamat IP privat, tentukan IT alamat IP privat yang akan dikaitkan dengan alamat IP Elastis.
7. Pilih Kaitkan.

AWS CLI

Untuk mengaitkan alamat IP Elastis

Gunakan perintah asosiasi-alamat AWS CLI .

```
aws ec2 associate-address \
    --instance-id i-0b263919b6498b123 \
    --allocation-id eipalloc-64d5890a
```

PowerShell

Untuk mengaitkan alamat IP Elastis

Gunakan Register-EC2Addresscmdlet.

```
Register-EC2Address `
    -InstanceId i-0b263919b6498b123 `
    -AllocationId eipalloc-64d5890a
```

Pisahkan alamat IP Elastis

: Untuk melepaskan pengaitan alamat IP Elastis dari instans atau antarmuka jaringan. Setelah Anda melepaskan alamat IP elastis, Anda dapat mengaitkannya dengan sumber daya lain.

Console

Untuk memisahkan dan mengaitkan alamat IP Elastis

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Elastic IPs.
3. Pilih alamat IP Elastis yang akan dipisahkan, pilih Tindakan, Pisahkan alamat IP Elastis.
4. Pilih Pisahkan.

AWS CLI

Untuk memisahkan alamat IP Elastis

Gunakan perintah disassociate-address AWS CLI .

```
aws ec2 disassociate-address --association-id eipassoc-12345678
```

PowerShell

Untuk memisahkan alamat IP Elastis

Gunakan Unregister-EC2Addresscmdlet.

```
Unregister-EC2Address -AssociationId eipassoc-12345678
```

Transfer alamat IP Elastis antara Akun AWS

Anda dapat mentransfer alamat IP Elastis dari satu Akun AWS ke yang lain. Ini dapat membantu dalam situasi berikut:

- Pemulihan bencana - Memetakan ulang alamat IP dengan cepat untuk beban kerja internet yang dihadapi publik selama acara darurat.
- Restrukturisasi organisasi — Pindahkan beban kerja dengan cepat dari satu Akun AWS ke yang lain. Transfer alamat menghindari kebutuhan untuk menunggu alamat IP Elastis baru diizinkan oleh grup keamanan dan jaringan ACLs Anda.
- Administrasi keamanan terpusat — Gunakan akun AWS keamanan terpusat untuk melacak dan mentransfer alamat IP Elastis yang telah diperiksa untuk kepatuhan keamanan.

Harga

Tidak ada biaya untuk mentransfer alamat IP Elastis.

Tugas

- Aktifkan transfer alamat IP Elastis
- Menerima alamat IP Elastis yang ditransfer
- Nonaktifkan transfer alamat IP Elastis

Aktifkan transfer alamat IP Elastis

Bagian ini menjelaskan cara menerima alamat IP Elastis yang ditransfer. Perhatikan batasan berikut yang terkait dengan mengaktifkan alamat IP Elastis untuk transfer:

- Anda dapat mentransfer alamat IP Elastis dari Akun AWS (akun sumber) apa pun ke akun lain Akun AWS yang sama AWS Region (akun transfer). Anda tidak dapat mentransfer alamat IP Elastis ke Wilayah lain.
- Saat Anda mentransfer alamat IP Elastis, ada jabat tangan dua langkah di antara. Akun AWS Ketika akun sumber memulai transfer, akun transfer memiliki tujuh hari untuk menerima transfer alamat IP Elastis. Selama tujuh hari itu, akun sumber dapat melihat transfer yang tertunda (misalnya di AWS konsol atau dengan menggunakan describe-address-transfersperintah). Setelah tujuh hari, transfer berakhir dan kepemilikan alamat IP Elastis kembali ke akun sumber.
- Transfer yang diterima dapat dilihat oleh akun sumber (misalnya di AWS konsol atau dengan menggunakan describe-address-transfersperintah) selama 14 hari setelah transfer diterima.
- AWS tidak memberi tahu akun transfer tentang permintaan transfer alamat IP Elastis yang tertunda. Pemilik akun sumber harus memberi tahu pemilik akun transfer bahwa ada permintaan transfer alamat IP Elastis yang harus mereka terima.
- Tanda apa pun yang terkait dengan alamat IP Elastis yang ditransfer diatur ulang saat transfer selesai.
- Anda tidak dapat mentransfer alamat IP Elastis yang dialokasikan dari kumpulan IPv4 alamat publik yang Anda bawa ke kumpulan Akun AWS alamat Bring Your Own IP (BYOIP).
- Anda tidak dapat mentransfer alamat IP Elastis yang dialokasikan dari kolam Amazon VPC IP Address Manager (IPAM) publik yang disediakan IPv4 Amazon. Sebaliknya, IPAM memungkinkan Anda untuk berbagi kolam IPAM di seluruh AWS akun dengan mengintegrasikan IPAM dengan AWS Organizations dan menggunakan. AWS RAM Untuk informasi selengkapnya, lihat

Mengalokasikan alamat IP Elastis berurutan dari kumpulan IPAM di Panduan Pengguna Amazon VPC IPAM.

- Jika Anda mencoba mentransfer alamat IP Elastis yang memiliki catatan DNS terbalik yang terkait dengannya, Anda dapat memulai proses transfer, tetapi akun transfer tidak akan dapat menerima transfer sampai catatan DNS terkait dihapus.
- Jika Anda telah mengaktifkan dan mengonfigurasi AWS Outposts, Anda mungkin telah mengalokasikan alamat IP Elastic dari kumpulan alamat IP milik pelanggan (CoIP). Anda tidak dapat mentransfer alamat IP Elastis yang dialokasikan dari CoIP. Namun, Anda dapat menggunakan AWS RAM untuk berbagi CoIP dengan akun lain. Untuk informasi selengkapnya, lihat Alamat IP milik pelanggan di Panduan Pengguna AWS Outposts .
- Anda dapat menggunakan Amazon VPC IPAM untuk melacak transfer alamat IP Elastis ke akun di organisasi AWS Organizations. Untuk informasi selengkapnya, lihat Lihat riwayat alamat IP. Jika alamat IP Elastis ditransfer ke Akun AWS luar organisasi, riwayat audit IPAM dari alamat IP Elastis hilang.

Langkah-langkah ini harus diselesaikan oleh akun sumber.

Console

Untuk mengaktifkan transfer alamat IP Elastis

1. Pastikan Anda menggunakan AWS akun sumber.
2. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
3. Di panel navigasi, pilih Elastic IPs.
4. Pilih satu atau beberapa alamat IP elastis untuk mengaktifkan transfer dan pilih Tindakan, Aktifkan transfer.
5. Jika Anda mentransfer beberapa alamat IP Elastis, Anda akan melihat opsi Tipe transfer. Pilih salah satu opsi berikut:
   - Pilih Akun tunggal jika Anda mentransfer alamat IP Elastis ke satu AWS akun.
   - Pilih Beberapa akun jika Anda mentransfer alamat IP Elastis ke beberapa AWS akun.
6. Di bawah Transfer ID akun, masukkan AWS akun yang ingin Anda transfer alamat IP Elastis. IDs
7. Konfirmasikan transfer dengan memasukkan **`enable`** dalam kotak teks.
8. Pilih Kirim.

9. Untuk menerima transfer, lihat Menerima alamat IP Elastis yang ditransfer. Untuk menonaktifkan transfer, lihat Nonaktifkan transfer alamat IP Elastis.

AWS CLI

Untuk mengaktifkan transfer alamat IP Elastis

Gunakan perintah enable-address-transfer.

```
aws ec2 enable-address-transfer \
    --allocation-id eipalloc-09ad461b0d03f6aaf \
    --transfer-account-id 123456789012
```

PowerShell

Untuk mengaktifkan transfer alamat IP Elastis

Gunakan Enable-EC2AddressTransfercmdlet.

```
Enable-EC2AddressTransfer `
    -AllocationId eipalloc-09ad461b0d03f6aaf `
    -TransferAccountId 123456789012
```

Menerima alamat IP Elastis yang ditransfer

Bagian ini menjelaskan cara menerima alamat IP Elastis yang ditransfer.

Saat Anda mentransfer alamat IP Elastis, ada jabat tangan dua langkah di antara. Akun AWS Ketika akun sumber memulai transfer, akun transfer memiliki tujuh hari untuk menerima transfer alamat IP Elastis. Selama tujuh hari itu, akun sumber dapat melihat transfer yang tertunda (misalnya di AWS konsol atau dengan menggunakan describe-address-transfersperintah). Setelah tujuh hari, transfer berakhir dan kepemilikan alamat IP Elastis kembali ke akun sumber.

Saat menerima transfer, perhatikan pengecualian berikut yang mungkin terjadi dan cara mengatasinya:

- AddressLimitExceeded: Jika akun transfer Anda telah melebihi kuota alamat IP Elastic, akun sumber dapat mengaktifkan transfer alamat IP Elastic, tetapi pengecualian ini terjadi ketika akun transfer mencoba menerima transfer. Secara default, semua AWS akun dibatasi hingga 5 alamat IP Elastis per Wilayah. Lihat Kuota alamat IP Elastis untuk instruksi tentang meningkatkan batas.

- InvalidTransfer. AddressCustomPtrSet: Jika Anda atau seseorang di organisasi Anda telah mengonfigurasi alamat IP Elastis yang Anda coba transfer untuk menggunakan pencarian DNS terbalik, akun sumber dapat mengaktifkan transfer untuk alamat IP Elastis, tetapi pengecualian ini terjadi ketika akun transfer mencoba menerima transfer. Untuk mengatasi masalah ini, akun sumber harus menghapus catatan DNS untuk alamat IP Elastis. Untuk informasi selengkapnya, lihat Buat catatan DNS terbalik untuk email di Amazon EC2.
- InvalidTransfer. AddressAssociated: Jika alamat IP Elastis dikaitkan dengan instans ENI atau EC2, akun sumber dapat mengaktifkan transfer untuk alamat IP Elastis, tetapi pengecualian ini terjadi ketika akun transfer mencoba menerima transfer. Untuk mengatasi masalah ini, akun sumber harus memisahkan alamat IP Elastis. Untuk informasi selengkapnya, lihat Pisahkan alamat IP Elastis.

Untuk pengecualian lainnya, hubungi Dukungan.

Langkah-langkah ini harus diselesaikan oleh akun transfer.

Console

Untuk menerima transfer alamat IP Elastis

1. Pastikan Anda menggunakan akun transfer.
2. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
3. Di panel navigasi, pilih Elastic IPs.
4. Pilih Tindakan, Terima transfer.
5. Tidak ada tanda yang terkait dengan alamat IP Elastis yang ditransfer dengan alamat IP Elastis saat Anda menerima transfer. Jika Anda ingin menentukan tanda Nama untuk alamat IP Elastis yang Anda terima, pilih Buat tanda dengan kunci 'Nama' dan nilai yang Anda tentukan.
6. Masukkan alamat IP Elastis yang ingin Anda transfer.
7. Jika Anda menerima beberapa alamat IP Elastis yang ditransfer, pilih Tambah alamat untuk memasukkan alamat IP Elastis tambahan.
8. Pilih Kirim.

AWS CLI

Untuk menerima transfer alamat IP Elastis

Gunakan perintah accept-address-transfer.

```
aws ec2 accept-address-transfer --address 100.21.184.216
```

PowerShell

Untuk menerima transfer alamat IP Elastis

Gunakan Approve-EC2AddressTransfercmdlet.

```
Approve-EC2AddressTransfer -Address 100.21.184.216
```

Nonaktifkan transfer alamat IP Elastis

Bagian ini menjelaskan cara menonaktifkan transfer IP Elastis setelah transfer diaktifkan.

Langkah-langkah ini harus diselesaikan oleh akun sumber yang mengaktifkan transfer.

Console

Untuk menonaktifkan transfer alamat IP Elastis

1. Pastikan Anda menggunakan sumbernya Akun AWS.
2. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
3. Di panel navigasi, pilih Elastic IPs.
4. Dalam daftar sumber daya Elastic IPs, pastikan properti Anda diaktifkan yang menampilkan status Transfer kolom.
5. Pilih satu atau beberapa alamat IP elastis yang memiliki status Transfer Tertunda, dan pilih Tindakan, Nonaktifkan transfer.
6. Konfirmasikan dengan memasukkan **`disable`** di kotak teks.
7. Pilih Kirim.

AWS CLI

Untuk menonaktifkan transfer alamat IP Elastis

Gunakan perintah disable-address-transfer.

```
aws ec2 disable-address-transfer --allocation-id eipalloc-09ad461b0d03f6aaf
```

PowerShell

Untuk menonaktifkan transfer alamat IP Elastis

Gunakan Disable-EC2AddressTransfercmdlet.

```
Disable-EC2AddressTransfer -AllocationId eipalloc-09ad461b0d03f6aaf
```

Merilis alamat IP Elastis

Jika Anda tidak lagi memerlukan alamat IP Elastis, kami menyarankan Anda melepaskannya. Alamat IP Elastis yang akan dirilis saat ini tidak boleh dikaitkan dengan AWS sumber daya.

Console

Untuk merilis alamat IP Elastis

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Elastic IPs.
3. Pilih alamat IP Elastis yang akan dilepas dan pilih Tindakan, Lepas alamat IP Elastis.
4. Pilih Lepas.

AWS CLI

Untuk merilis alamat IP Elastis

Gunakan perintah release-address AWS CLI .

```
aws ec2 release-address --allocation-id eipalloc-64d5890a
```

PowerShell

Untuk merilis alamat IP Elastis

Gunakan Remove-EC2Addresscmdlet.

```
Remove-EC2Address -AllocationId eipalloc-64d5890a
```

Setelah Anda merilis alamat IP Elastis Anda, Anda mungkin dapat memulihkan. Aturan-aturan berikut berlaku:

- Anda tidak dapat memulihkan alamat IP Elastis jika telah dialokasikan ke AWS akun lain, atau jika itu akan mengakibatkan Anda melebihi batas alamat IP Elastis Anda.
- Anda tidak dapat memulihkan tag yang terkait dengan alamat IP Elastis.

AWS CLI

Untuk memulihkan alamat IP Elastis

Gunakan perintah allocate-address.

```
aws ec2 allocate-address \
    --domain vpc \
    --address 203.0.113.3
```

PowerShell

Untuk memulihkan alamat IP Elastis

Gunakan New-EC2Addresscmdlet.

```
New-EC2Address `
    -Address 203.0.113.3 `
    -Domain vpc `
    -Region us-east-1
```

Buat catatan DNS terbalik untuk email di Amazon EC2

Jika Anda bermaksud mengirim email ke pihak ketiga dari instans EC2, sebaiknya Anda menyediakan satu atau lebih alamat IP Elastis dan menetapkan data DNS terbalik statis ke alamat IP Elastis yang Anda gunakan untuk mengirim email. Ini dapat membantu Anda menghindari email Anda ditandai sebagai spam oleh beberapa organisasi anti-spam. AWS bekerja dengan ISPs dan organisasi anti-spam internet untuk mengurangi kemungkinan email Anda yang dikirim dari alamat ini akan ditandai sebagai spam.

Pertimbangan-pertimbangan

- Sebelum Anda membuat catatan DNS terbalik, Anda harus mengatur catatan DNS lanjutan yang sesuai (tipe catatan A) yang menunjuk ke alamat IP Elastis Anda.
- Jika catatan DNS terbalik dikaitkan dengan alamat IP Elastis, alamat IP Elastis terkunci ke akun Anda dan tidak dapat dikeluarkan dari akun Anda hingga rekaman dihapus.
- Jika Anda menghubungi Dukungan untuk mengatur DNS terbalik untuk alamat IP Elastis, Anda dapat menghapus DNS terbalik, tetapi Anda tidak dapat melepaskan alamat IP Elastis karena dikunci oleh. Dukungan Untuk membuka kunci alamat IP Elastis, hubungi AWS Dukungan. Setelah alamat IP elastis dibuka, Anda dapat melepaskannya.
- [AWS GovCloud (US) Region] Anda tidak dapat membuat rekaman DNS terbalik. AWS harus menetapkan catatan DNS terbalik statis untuk Anda. Buka kasus dukungan untuk menghapus DNS terbalik dan batasan pengiriman email. Anda harus memberikan alamat IP Elastis Anda dan membalikkan catatan DNS.

Membuat catatan DNS terbalik

Anda dapat membuat catatan DNS terbalik untuk alamat IP Elastis Anda sebagai berikut.

Console

Untuk membuat catatan DNS terbalik

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Elastic IPs.
3. Pilih alamat IP Elastis dan pilih Tindakan, Memperbarui DNS terbalik.
4. Untuk Membalikkan nama domain DNS, masukkan nama domain.
5. Masukkan **`update`** untuk mengonfirmasi.
6. Pilih Perbarui.

AWS CLI

Untuk membuat catatan DNS terbalik

Gunakan perintah modify-address-attribute.

```
aws ec2 modify-address-attribute \
```

```
    --allocation-id eipalloc-abcdef01234567890 \
    --domain-name example.com
```

Berikut ini adalah output contoh.

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net.",
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
            }
        }
    ]
}
```

PowerShell

Untuk membuat catatan DNS terbalik

Gunakan Edit-EC2AddressAttributecmdlet.

```
Edit-EC2AddressAttribute `
    -AllocationId 'eipalloc-abcdef01234567890' `
    -DomainName 'example.com' |
Format-List `
    AllocationId, PtrRecord, PublicIp,
    @{Name='PtrRecordUpdate';Expression={$_.PtrRecordUpdate | Format-List | Out-
String}}
```

Berikut ini adalah output contoh.

```
AllocationId    : eipalloc-abcdef01234567890
PtrRecord       : example.net.
PublicIp        : 192.0.2.0
PtrRecordUpdate :
                  Reason :
                  Status : PENDING
                  Value  : example.com.
```

Membuat catatan DNS terbalik

Anda dapat menghapus catatan DNS terbalik dari alamat IP Elastis Anda sebagai berikut.

Jika Anda menerima kesalahan berikut, Anda dapat mengirimkan Permintaan untuk menghapus pembatasan pengiriman email Dukungan untuk bantuan.

```
The address cannot be released because it is locked to your account.
```

Console

Untuk menghapus catatan DNS terbalik

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Elastic IPs.
3. Pilih alamat IP Elastis dan pilih Tindakan, Memperbarui DNS terbalik.
4. Untuk nama domain DNS Terbalik, hapus nama domain.
5. Masukkan **`update`** untuk mengonfirmasi.
6. Pilih Perbarui.

AWS CLI

Untuk menghapus catatan DNS terbalik

Gunakan perintah reset-address-attribute.

```
aws ec2 reset-address-attribute \
    --allocation-id eipalloc-abcdef01234567890 \
    --attribute domain-name
```

Berikut ini adalah output contoh.

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com.",
            "PtrRecordUpdate": {
                "Value": "example.net.",
```

```
                "Status": "PENDING"
            }
        }
    ]
}
```

PowerShell

Untuk menghapus catatan DNS terbalik

Gunakan Reset-EC2AddressAttributecmdlet.

```
Reset-EC2AddressAttribute `
    -AllocationId 'eipalloc-abcdef01234567890' `
    -Attribute domain-name |
Format-List `
    AllocationId, PtrRecord, PublicIp,
    @{Name='PtrRecordUpdate';Expression={$_.PtrRecordUpdate | Format-List | Out-
String}}
```

Berikut ini adalah output contoh.

```
AllocationId    : eipalloc-abcdef01234567890
PtrRecord       : example.com.
PublicIp        : 192.0.2.0
PtrRecordUpdate :
                  Reason :
                  Status : PENDING
                  Value  : example.net.
```

Antarmuka jaringan elastis

Antarmuka jaringan elastis adalah komponen jaringan logis dalam VPC yang mewakili kartu jaringan virtual. Anda dapat membuat dan mengonfigurasi antarmuka jaringan dan melampirkannya ke instance yang Anda luncurkan di Availability Zone yang sama. Atribut antarmuka jaringan mengikutinya saat dilampirkan atau dilepaskan dari sebuah instans dan dilampirkan kembali ke instans lain. Ketika Anda memindahkan antarmuka jaringan dari satu instance ke yang lain, lalu lintas jaringan dialihkan dari instance asli ke instance baru.

Perhatikan bahwa AWS sumber daya ini disebut sebagai antarmuka jaringan di Konsol Manajemen AWS dan Amazon EC2 API. Oleh karena itu, kami menggunakan "antarmuka jaringan" dalam

dokumentasi ini daripada "antarmuka jaringan elastis". Istilah "antarmuka jaringan" dalam dokumentasi ini selalu berarti "antarmuka jaringan elastis".

Atribut antarmuka jaringan

Antarmuka jaringan dapat mencakup atribut berikut:

- IPv4 Alamat pribadi utama dari rentang IPv4 alamat subnet Anda
- IPv6 Alamat utama dari rentang IPv6 alamat subnet Anda
- IPv4 Alamat pribadi sekunder dari rentang IPv4 alamat subnet Anda
- Satu alamat IP Elastis (IPv4) untuk setiap IPv4 alamat pribadi
- Satu IPv4 alamat publik
- IPv6 Alamat sekunder
- Grup keamanan
- Alamat MAC
- Bendera source/destination cek
- Deskripsi

Memantau lalu lintas

Anda dapat mengaktifkan log aliran VPC pada antarmuka jaringan Anda untuk menangkap informasi tentang lalu lintas yang pergi ke dan dari antarmuka jaringan. Setelah membuat log aliran, Anda dapat melihat dan mengambil datanya di Amazon CloudWatch Logs. Untuk informasi selengkapnya, lihat Log Alur VPC di Panduan Pengguna Amazon VPC.

Daftar Isi

- Konsep antarmuka jaringan
- Kartu jaringan
- Alamat IP maksimum per antarmuka jaringan
- Buat antarmuka jaringan untuk instans EC2 Anda
- Lampiran antarmuka jaringan untuk instans EC2 Anda
- Kelola alamat IP untuk antarmuka jaringan Anda
- Memodifikasi atribut antarmuka jaringan
- Beberapa antarmuka jaringan untuk instans Amazon EC2 Anda
- Antarmuka jaringan yang dikelola pemohon

- Delegasi awalan untuk antarmuka jaringan Amazon EC2
- Menghapus antarmuka jaringan

Konsep antarmuka jaringan

Berikut ini adalah konsep penting untuk dipahami saat Anda mulai menggunakan antarmuka jaringan.

Antarmuka jaringan primer

Setiap instans memiliki antarmuka jaringan default, yang disebut antarmuka jaringan primer. Anda tidak dapat melepaskan antarmuka jaringan utama dari sebuah instance.

Antarmuka jaringan sekunder

Anda dapat membuat dan melampirkan antarmuka jaringan sekunder ke instans Anda. Jumlah maksimum antarmuka jaringan bervariasi menurut jenis instance. Untuk informasi selengkapnya, lihat Alamat IP maksimum per antarmuka jaringan.

IPv4 alamat untuk antarmuka jaringan

Saat Anda meluncurkan instans EC2 ke subnet IPv4 -only atau dual stack, instance menerima alamat IP pribadi utama dari rentang IPv4 alamat subnet. Anda juga dapat menentukan IPv4 alamat pribadi tambahan, yang dikenal sebagai IPv4 alamat pribadi sekunder. Tidak seperti alamat IP privat primer, alamat IP privat sekunder dapat ditetapkan ulang dari satu instans ke instans lainnya.

IPv4 Alamat publik untuk antarmuka jaringan

Semua subnet memiliki atribut yang dapat dimodifikasi yang menentukan apakah antarmuka jaringan yang dibuat di subnet itu (dan oleh karena itu instance yang diluncurkan ke subnet itu) diberi alamat publik. IPv4 Untuk informasi selengkapnya, lihat Pengaturan subnet di Panduan Pengguna Amazon VPC. Saat Anda meluncurkan sebuah instance, alamat IP ditetapkan ke antarmuka jaringan utama. Jika Anda menentukan antarmuka jaringan yang ada sebagai antarmuka jaringan utama saat Anda meluncurkan instance, IPv4 alamat publik ditentukan oleh antarmuka jaringan ini.

Ketika Anda membuat antarmuka jaringan, itu mewarisi atribut IPv4 pengalamatan publik dari subnet. Jika nanti Anda memodifikasi atribut IPv4 pengalamatan publik subnet, antarmuka jaringan menyimpan pengaturan yang berlaku saat dibuat.

Kami merilis alamat IP publik ketika instance dihentikan, hibernasi, atau dihentikan. Kami menetapkan alamat IP publik baru ketika Anda memulai instans berhenti atau hibernasi, kecuali

jika memiliki antarmuka jaringan sekunder atau IPv4 alamat pribadi sekunder yang dikaitkan dengan alamat IP Elastis.

IPv6 alamat untuk antarmuka jaringan

Jika Anda mengaitkan blok IPv6 CIDR dengan VPC dan subnet Anda, Anda dapat IPv6 menetapkan alamat dari rentang subnet ke antarmuka jaringan. Setiap IPv6 alamat dapat ditetapkan ke satu antarmuka jaringan.

Semua subnet memiliki atribut yang dapat dimodifikasi yang menentukan apakah antarmuka jaringan yang dibuat di subnet itu (dan oleh karena itu instance yang diluncurkan ke subnet itu) secara otomatis diberi IPv6 alamat dari rentang subnet. Saat Anda meluncurkan sebuah instance, IPv6 alamat tersebut ditetapkan ke antarmuka jaringan utama.

Alamat IP elastis untuk antarmuka jaringan

Anda dapat mengaitkan alamat IP Elastis dengan salah satu IPv4 alamat pribadi untuk antarmuka jaringan. Anda dapat mengaitkan satu alamat IP Elastis dengan setiap IPv4 alamat pribadi. Jika Anda memisahkan alamat IP Elastis dari antarmuka jaringan, Anda dapat melepaskannya atau mengaitkannya dengan instance yang berbeda.

Perilaku pemutusan hubungan kerja

Anda dapat menyetel perilaku terminasi untuk antarmuka jaringan yang dilampirkan ke sebuah instans. Anda dapat menentukan apakah antarmuka jaringan harus dihapus secara otomatis saat Anda menghentikan instans yang dilampirkan.

Pemeriksaan sumber / tujuan

Anda dapat mengaktifkan atau menonaktifkan source/destination pemeriksaan, yang memastikan bahwa instance adalah sumber atau tujuan dari lalu lintas apa pun yang diterimanya. Source/destination checks are enabled by default. You must disable source/destinationmemeriksa apakah instance menjalankan layanan seperti terjemahan alamat jaringan, perutean, atau firewall.

Antarmuka jaringan yang dikelola pemohon

Antarmuka jaringan ini dibuat dan dikelola oleh Layanan AWS untuk memungkinkan Anda menggunakan beberapa sumber daya dan layanan. Anda tidak dapat mengelola antarmuka jaringan ini sendiri. Untuk informasi selengkapnya, lihat Antarmuka jaringan yang dikelola pemohon.

Delegasi awalan

Awalan adalah rentang pribadi IPv4 atau IPv6 CIDR yang dicadangkan yang Anda alokasikan untuk penugasan otomatis atau manual ke antarmuka jaringan yang terkait dengan sebuah

instance. Dengan menggunakan Prefiks yang Didelegasikan, Anda dapat meluncurkan layanan lebih cepat dengan menetapkan berbagai alamat IP sebagai prefiks tunggal.

Antarmuka jaringan terkelola

Antarmuka jaringan terkelola dikelola oleh penyedia layanan, seperti Amazon EKS Auto Mode. Anda tidak dapat langsung mengubah pengaturan antarmuka jaringan terkelola. Antarmuka jaringan terkelola diidentifikasi oleh nilai sebenarnya di bidang Dikelola. Untuk informasi selengkapnya, lihat Instans terkelola Amazon EC2.

Kartu jaringan

Sebagian besar jenis contoh mendukung satu kartu jaringan. Jenis instans yang mendukung beberapa kartu jaringan memberikan kinerja jaringan yang lebih tinggi, termasuk kemampuan bandwidth di atas 100 Gbps dan peningkatan kinerja packet rate. Ketika Anda melampirkan antarmuka jaringan ke instance yang mendukung beberapa kartu jaringan, Anda dapat memilih kartu jaringan untuk antarmuka jaringan. Antarmuka jaringan primer harus ditetapkan ke indeks kartu jaringan 0.

Antarmuka jaringan EFA dan EFA hanya dihitung sebagai antarmuka jaringan. Anda hanya dapat menetapkan satu antarmuka jaringan EFA atau EFA per kartu jaringan. Antarmuka jaringan utama tidak dapat berupa antarmuka jaringan khusus EFA.

Jenis contoh berikut mendukung beberapa kartu jaringan. Untuk informasi tentang jumlah antarmuka jaringan yang didukung oleh tipe instans, lihatAlamat IP maksimum per antarmuka jaringan.

Tipe instans	Jumlah kartu jaringan
c6in.32xlarge	2
c6in.metal	2
c8gb.48xlarge	2
c8gb.metal-48xl	2
c8gn.48xlarge	2
c8gn.metal-48xl	2

Tipe instans	Jumlah kartu jaringan
dl1.24xlarge	4
g6e.24xlarge	2
g6e.48xlarge	4
g7e.24xlarge	2
g7e.48xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2
hpc7a.48xlarge	2
hpc7a.96xlarge	2
hpc8a.96xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
m8gb.48xlarge	2
m8gb.metal-48xl	2
m8gn.48xlarge	2
m8gn.metal-48xl	2
p4d.24xlarge	4

Tipe instans	Jumlah kartu jaringan
p4de.24xlarge	4
p5.48xlarge	32
p5e.48xlarge	32
p5en.48xlarge	16
p6-b200.48xlarge	8
p6-b300.48xlarge	17
p6e-gb200.36xlarge	17
r8gb.48xlarge	2
r8gb.metal-48xl	2
r8gn.48xlarge	2
r8gn.metal-48xl	2
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8
trn1n.32xlarge	16
trn2.48xlarge	16
trn2u.48xlarge	16
u7in-16tb.224xlarge	2

Tipe instans	Jumlah kartu jaringan
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2
u7inh-32tb.480xlarge	2

Alamat IP maksimum per antarmuka jaringan

Setiap jenis instance mendukung jumlah maksimum antarmuka jaringan, jumlah maksimum IPv4 alamat pribadi per antarmuka jaringan, dan jumlah maksimum IPv6 alamat per antarmuka jaringan. Batas untuk IPv6 alamat terpisah dari batas untuk IPv4 alamat pribadi per antarmuka jaringan. Perhatikan bahwa semua jenis instans mendukung IPv6 pengalamatan kecuali untuk yang berikut: C1, M1, M2, M3, dan T1.

Antarmuka jaringan yang tersedia

Panduan Jenis Instans Amazon EC2 menyediakan informasi tentang antarmuka jaringan yang tersedia untuk setiap jenis instans. Untuk informasi selengkapnya, lihat berikut ini:

- Spesifikasi jaringan — Tujuan umum
- Spesifikasi jaringan — Komputasi dioptimalkan
- Spesifikasi jaringan - Memori dioptimalkan
- Spesifikasi jaringan - Penyimpanan dioptimalkan
- Spesifikasi jaringan — Komputasi yang dipercepat
- Spesifikasi jaringan — Komputasi kinerja tinggi
- Spesifikasi jaringan — Generasi sebelumnya

Console

Untuk mengambil antarmuka jaringan maksimum

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Tipe Instans.

3. Tambahkan filter untuk menentukan jenis instance (Instance type=c5.12xlarge) atau instance family (Instance family=c5).
4. (Opsional) Klik ikon Preferensi dan kemudian nyalakan Jumlah maksimum antarmuka jaringan. Kolom ini menunjukkan jumlah maksimum antarmuka jaringan untuk setiap jenis instance.
5. (Opsional) Pilih jenis instance. Pada tab Jaringan, temukan Jumlah maksimum antarmuka jaringan.

AWS CLI

Untuk mengambil antarmuka jaringan maksimum

Anda dapat menggunakan describe-instance-typesperintah untuk menampilkan informasi tentang jenis instance, seperti antarmuka jaringan yang didukung dan alamat IP per antarmuka. Contoh berikut menampilkan informasi ini untuk semua instance C8i.

```
{ echo -e "InstanceType\tMaximumNetworkInterfaces\tIpv4AddressesPerInterface"; \
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c8i.*" \
    --query 'InstanceTypes[*].[InstanceType, NetworkInfo.MaximumNetworkInterfaces,
 NetworkInfo.Ipv4AddressesPerInterface]' \
    --output text | sort -k2 -n; } | column -t
```

Berikut ini adalah output contoh.

```
InstanceType    MaximumNetworkInterfaces  Ipv4AddressesPerInterface
c8i.large       3                         20
c8i.2xlarge     4                         30
c8i.xlarge      4                         30
c8i.4xlarge     8                         50
c8i.8xlarge     10                        50
c8i.12xlarge    12                        50
c8i.16xlarge    16                        64
c8i.24xlarge    16                        64
c8i.32xlarge    24                        64
c8i.48xlarge    24                        64
c8i.96xlarge    24                        64
c8i.metal-48xl  24                        64
c8i.metal-96xl  24                        64
```

PowerShell

Untuk mengambil antarmuka jaringan maksimum

Anda dapat menggunakan Get-EC2InstanceType PowerShell perintah untuk menampilkan informasi tentang jenis instance, seperti antarmuka jaringan yang didukung dan alamat IP per antarmuka. Contoh berikut menampilkan informasi ini untuk semua instance C8i.

```
Get-EC2InstanceType -Filter @{Name="instance-type"; Values="c8i.*"} |
Select-Object `
    InstanceType,
    @{Name='MaximumNetworkInterfaces';
 Expression={$_.NetworkInfo.MaximumNetworkInterfaces}},
    @{Name='Ipv4AddressesPerInterface';
 Expression={$_.NetworkInfo.Ipv4AddressesPerInterface}} |
Sort-Object MaximumNetworkInterfaces |
Format-Table -AutoSize
```

Berikut ini adalah output contoh.

```
InstanceType   MaximumNetworkInterfaces Ipv4AddressesPerInterface
------------   ------------------------ -------------------------
c8i.large                             3                        20
c8i.xlarge                            4                        30
c8i.2xlarge                           4                        30
c8i.4xlarge                           8                        50
c8i.8xlarge                          10                        50
c8i.12xlarge                         12                        50
c8i.24xlarge                         16                        64
c8i.16xlarge                         16                        64
c8i.96xlarge                         24                        64
c8i.48xlarge                         24                        64
c8i.metal-96xl                       24                        64
c8i.32xlarge                         24                        64
c8i.metal-48xl                       24                        64
```

Buat antarmuka jaringan untuk instans EC2 Anda

Anda dapat membuat antarmuka jaringan untuk digunakan oleh instans EC2 Anda. Saat Anda membuat antarmuka jaringan, Anda menentukan subnet yang membuatnya. Anda tidak dapat

memindahkan antarmuka jaringan ke subnet lain setelah dibuat. Anda harus memasang antarmuka jaringan ke sebuah instans di Zona Ketersediaan yang sama. Anda dapat melepaskan antarmuka jaringan sekunder dari sebuah instance dan kemudian melampirkannya ke instance yang berbeda di Availability Zone yang sama. Anda tidak dapat melepaskan antarmuka jaringan utama dari sebuah instance. Untuk informasi selengkapnya, lihat the section called “Lampiran antarmuka jaringan”.

Console

Untuk membuat antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih Buat antarmuka jaringan.
4. (Opsional) Untuk Deskripsi, masukkan nama deskriptif.
5. Untuk Subnet, pilih subnet. Opsi yang tersedia di langkah berikutnya berubah tergantung pada jenis subnet yang Anda pilih (IPv4-only, IPv6 -only, atau dual-stack (and)). IPv4 IPv6
6. Untuk jenis Antarmuka, pilih salah satu dari berikut ini:
   - ENA: Antarmuka jaringan berkinerja tinggi yang dirancang untuk menangani throughput dan packet-per-second tingkat tinggi untuk TCP/IP protokol sambil meminimalkan penggunaan CPU. Ini adalah nilai default. Untuk informasi lebih lanjut tentang ENA, lihat Adaptor Jaringan Elastis.
   - EFA dengan ENA: Antarmuka jaringan yang mendukung perangkat ENA dan EFA untuk transportasi TCP/IP berbasis tradisional bersama dengan transportasi berbasis SRD. Jika Anda memilih EFA dengan ENA, contoh yang Anda lampirkan harus mendukung EFA. Untuk informasi lebih lanjut tentang EFA, lihat Adaptor Kain Elastis.
   - Khusus EFA: Antarmuka jaringan berkinerja tinggi yang dirancang untuk menangani throughput tinggi, komunikasi antar-node latensi rendah untuk transportasi berbasis SRD sambil melewati tumpukan sistem operasi. Jika Anda memilih opsi ini, instance yang Anda lampirkan harus mendukung EFA. Antarmuka jaringan khusus EFA tidak mendukung alamat IP. Untuk informasi lebih lanjut tentang EFA, lihat Adaptor Kain Elastis.
7. Untuk IPv4 alamat pribadi, lakukan salah satu hal berikut:
   - Pilih Tetapkan otomatis untuk mengizinkan Amazon EC2 memilih alamat dari IPv4 subnet.
   - Pilih Custom dan masukkan IPv4 alamat yang Anda pilih dari subnet.
8. (Subnet dengan IPv6 alamat saja) Untuk IPv6 alamat, lakukan salah satu hal berikut:

- Pilih None jika Anda tidak ingin menetapkan IPv6 alamat ke antarmuka jaringan.
- Pilih Tetapkan otomatis untuk mengizinkan Amazon EC2 memilih alamat dari IPv6 subnet.
- Pilih Custom dan masukkan IPv6 alamat yang Anda pilih dari subnet.

9. (Opsional) Jika Anda membuat antarmuka jaringan di subnet dual-stack atau IPv6 -only, Anda memiliki opsi untuk Menetapkan IP Utama. IPv6 Ini memberikan alamat unicast IPv6 global primer (GUA) ke antarmuka jaringan. Menetapkan IPv6 alamat utama memungkinkan Anda untuk menghindari mengganggu lalu lintas ke instance atau. ENIs Pilih Aktifkan jika instance ENI ini akan dilampirkan bergantung pada IPv6 alamatnya yang tidak berubah. AWS akan secara otomatis menetapkan IPv6 alamat yang terkait dengan ENI yang dilampirkan ke instans Anda untuk menjadi IPv6 alamat utama. Setelah Anda mengaktifkan alamat IPv6 GUA menjadi yang utama IPv6, Anda tidak dapat menonaktifkannya. Saat Anda mengaktifkan alamat IPv6 GUA menjadi primer IPv6, IPv6 GUA pertama akan dijadikan IPv6 alamat utama sampai instance dihentikan atau antarmuka jaringan terlepas. Jika Anda memiliki beberapa IPv6 alamat yang terkait dengan ENI yang dilampirkan ke instans Anda dan Anda mengaktifkan IPv6 alamat utama, alamat IPv6 GUA pertama yang terkait dengan ENI menjadi IPv6 alamat utama.
10. (Opsional) Untuk membuat Elastic Fabric Adapter, pilih Elastic Fabric Adapter, Aktifkan.
11. (Opsional) Di bawah Pengaturan lanjutan, Anda dapat mengatur delegasi awalan IP secara opsional. Untuk informasi selengkapnya, lihat Delegasi awalan.

    - Auto-assign — AWS memilih awalan dari IPv4 atau IPv6 CIDR blok untuk subnet, dan menetapkannya ke antarmuka jaringan.
    - Kustom - Anda menentukan awalan dari blok IPv4 atau IPv6 CIDR untuk subnet, dan AWS memverifikasi bahwa awalan belum ditetapkan ke sumber daya lain sebelum menetapkannya ke antarmuka jaringan.
12. (Opsional) Di bawah Pengaturan lanjutan, untuk Batas waktu pelacakan koneksi idle, modifikasi batas waktu koneksi idle default. Untuk informasi selengkapnya, lihat Waktu habis pelacakan koneksi idle.

    - TCP menetapkan batas waktu: Batas waktu (dalam detik) untuk koneksi TCP idle dalam keadaan mapan.
      - Min: `60` detik
      - Maks: `432000` detik

- Default: 350 detik untuk jenis instans Nitrov6, tidak termasuk P6e-. GB200 Dan 432000 detik untuk jenis contoh lainnya, termasuk P6e-. GB200
- Direkomendasikan: Kurang dari 432000 detik

- Batas waktu UDP: Batas waktu (dalam detik) untuk alur UDP idle yang telah melihat lalu lintas hanya dalam satu arah atau transaksi permintaan-respons tunggal.
  - Min: 30 detik
  - Maks: 60 detik
  - Default: 30 detik
- Batas waktu aliran UDP: Batas waktu (dalam detik) untuk alur UDP idle yang diklasifikasikan sebagai alur yang telah melihat lebih dari satu transaksi permintaan-respons.
  - Min: 60 detik
  - Max: 180 detik
  - Default: 180 detik

13. Untuk Grup keamanan, pilih satu atau beberapa grup keamanan.
14. (Opsional) Untuk setiap tanda, pilih Tambahkan tanda baru dan masukkan kunci tanda dan nilai tanda opsional tersebut.
15. Pilih Buat antarmuka jaringan.

AWS CLI

Contoh 1: Untuk membuat antarmuka jaringan dengan alamat IP yang dipilih oleh Amazon EC2

Gunakan perintah berikut create-network-interface. Contoh ini membuat antarmuka jaringan dengan alamat IPv4 publik dan alamat IPv6 yang dipilih oleh Amazon EC2.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my dual-stack network interface" \
    --ipv6-address-count 1 \
    --groups sg-1234567890abcdef0
```

Contoh 2: Untuk membuat antarmuka jaringan dengan alamat IP tertentu

Gunakan perintah berikut create-network-interface.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my dual-stack network interface" \
    --private-ip-address 10.251.50.12 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4 \
    --groups sg-1234567890abcdef0
```

Contoh 3: Untuk membuat antarmuka jaringan dengan hitungan alamat IP sekunder

Gunakan perintah berikut create-network-interface. Dalam contoh ini, Amazon EC2 memilih alamat IP primer dan alamat IP sekunder.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my network interface" \
    --secondary-private-ip-address-count 2 \
    --groups sg-1234567890abcdef0
```

Contoh 4: Untuk membuat antarmuka jaringan dengan alamat IP sekunder tertentu

Gunakan perintah berikut create-network-interface. Contoh ini menentukan alamat IP primer dan alamat IP sekunder.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my network interface" \
    --private-ip-addresses PrivateIpAddress=10.0.1.30,Primary=true \
                           PrivateIpAddress=10.0.1.31,Primary=false
    --groups sg-1234567890abcdef0
```

PowerShell

Contoh 1: Untuk membuat antarmuka jaringan dengan alamat IP yang dipilih oleh Amazon EC2

Gunakan New-EC2NetworkInterfacecmdlet. Contoh ini membuat antarmuka jaringan dengan alamat IPv4 publik dan alamat IPv6 yang dipilih oleh Amazon EC2.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my dual-stack network interface" `
```

```
    -Ipv6AddresCount 1 `
    -Group sg-1234567890abcdef0
```

Contoh 2: Untuk membuat antarmuka jaringan dengan alamat IP tertentu

Gunakan New-EC2NetworkInterfacecmdlet.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my dual-stack network interface" `
    -PrivateIpAddress 10.251.50.12 `
    -Ipv6Address $ipv6addr `
    -Group sg-1234567890abcdef0
```

Tentukan IPv6 alamatnya sebagai berikut.

```
$ipv6addr = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr1.Ipv6Address = "2001:db8::1234:5678:1.2.3.4"
```

Contoh 3: Untuk membuat antarmuka jaringan dengan hitungan alamat IP sekunder

Gunakan New-EC2NetworkInterfacecmdlet. Dalam contoh ini, Amazon EC2 memilih alamat IP primer dan alamat IP sekunder.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my network interface" `
    -SecondaryPrivateIpAddressCount 2 `
    -Group sg-1234567890abcdef0
```

Contoh 4: Untuk membuat antarmuka jaringan dengan alamat IP sekunder tertentu

Gunakan New-EC2NetworkInterfacecmdlet. Contoh ini menentukan alamat IP primer dan alamat IP sekunder.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my network interface" `
    -PrivateIpAddresses @($primary, $secondary) `
    -Group sg-1234567890abcdef0
```

Tentukan alamat sekunder sebagai berikut.

```
$primary = New-Object Amazon.EC2.Model.PrivateIpAddressSpecification
$primary.PrivateIpAddress = "10.0.1.30"
$primary.Primary = $true
$secondary = New-Object Amazon.EC2.Model.PrivateIpAddressSpecification
$secondary.PrivateIpAddress = "10.0.1.31"
$secondary.Primary = $false
```

Lampiran antarmuka jaringan untuk instans EC2 Anda

Anda dapat membuat antarmuka jaringan untuk digunakan oleh instans EC2 Anda sebagai antarmuka jaringan primer atau sekunder. Anda harus melampirkan antarmuka jaringan ke instans EC2 jika berada di Availability Zone yang sama dengan antarmuka jaringan. Jenis instance dari sebuah instance menentukan berapa banyak antarmuka jaringan yang dapat Anda lampirkan ke instance. Untuk informasi selengkapnya, lihat the section called “Alamat IP per antarmuka jaringan”.

Pertimbangan

- Anda dapat memasang antarmuka jaringan ke sebuah instans saat berjalan (lampirkan panas), saat dihentikan (lampirkan hangat), atau saat instans diluncurkan (lampirkan dingin).
- Anda dapat melepaskan antarmuka jaringan sekunder saat instans sedang berjalan atau dihentikan. Namun, Anda tidak dapat melepaskan antarmuka jaringan primer.
- Anda dapat melepaskan antarmuka jaringan sekunder dari satu instance dan melampirkannya ke instance lain.
- Saat meluncurkan instans menggunakan CLI, API, atau SDK, Anda dapat menentukan antarmuka jaringan primer dan antarmuka jaringan tambahan. Perhatikan bahwa Anda tidak dapat mengaktifkan penetapan otomatis IPv4 alamat publik jika Anda menambahkan antarmuka jaringan sekunder selama peluncuran.
- Meluncurkan instance Amazon Linux atau Windows Server dengan beberapa antarmuka jaringan secara otomatis mengkonfigurasi antarmuka, IPv4 alamat pribadi, dan tabel rute pada sistem operasi instance.
- Lampiran hangat atau panas dari antarmuka jaringan tambahan mungkin mengharuskan Anda untuk membuka antarmuka kedua secara manual, mengonfigurasi IPv4 alamat pribadi, dan memodifikasi tabel rute yang sesuai. Instans yang menjalankan Amazon Linux atau Windows Server secara otomatis mengenali warm atau hot attach dan mengonfigurasi sendiri.

- Anda tidak dapat melampirkan antarmuka jaringan lain ke instance (misalnya, konfigurasi tim NIC) untuk meningkatkan atau menggandakan bandwidth jaringan ke atau dari instance dual-homed.
- Jika Anda melampirkan beberapa antarmuka jaringan dari subnet yang sama ke sebuah instance, Anda mungkin mengalami masalah jaringan seperti perutean asimetris. Jika memungkinkan, tambahkan IPv4 alamat pribadi sekunder pada antarmuka jaringan utama sebagai gantinya.
- Untuk instans EC2 dalam subnet IPv6 -only, jika Anda melampirkan antarmuka jaringan sekunder, nama host DNS pribadi dari antarmuka jaringan sekunder menyelesaikan ke alamat utama untuk antarmuka jaringan utama. IPv6
- [Instans Windows] - Jika Anda menambahkan beberapa antarmuka jaringan ke sebuah instance, Anda harus mengonfigurasi antarmuka jaringan untuk menggunakan perutean statis.

Lampirkan antarmuka jaringan

Anda dapat memasang antarmuka jaringan ke instans apa pun di Zona Ketersediaan yang sama seperti antarmuka jaringan, baik menggunakan halaman Instans atau Antarmuka Jaringan dari konsol Amazon EC2. Atau, Anda dapat menentukan antarmuka jaringan yang ada saat Anda meluncurkan instans.

Jika IPv4 alamat publik pada instans Anda dirilis, itu tidak menerima yang baru jika ada lebih dari satu antarmuka jaringan yang dilampirkan ke instance. Untuk informasi selengkapnya tentang perilaku IPv4 alamat publik, lihatIPv4 Alamat publik.

Console

Untuk melampirkan antarmuka jaringan menggunakan halaman Instances

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih kotak centang untuk instans.
4. Pilih Tindakan, Jaringan, Lampirkan antarmuka jaringan.
5. Pilih VPC. Antarmuka jaringan dapat berada di VPC yang sama dengan instans Anda atau di VPC berbeda yang Anda miliki, selama antarmuka jaringan berada di Availability Zone yang sama dengan instance. Ini memungkinkan Anda membuat instance multi-homed VPCs dengan konfigurasi jaringan dan keamanan yang berbeda.
6. Pilih antarmuka jaringan. Jika instans mendukung beberapa kartu jaringan, Anda dapat memilih kartu jaringan.

7. Pilih Lampirkan.

Untuk melampirkan antarmuka jaringan menggunakan halaman Network Interfaces

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih kotak centang untuk antarmuka jaringan.
4. Pilih Tindakan, Lampirkan.
5. Pilih instans. Jika instans mendukung beberapa kartu jaringan, Anda dapat memilih kartu jaringan.
6. Pilih Lampirkan.

AWS CLI

Untuk melampirkan antarmuka jaringan

Gunakan perintah berikut attach-network-interface.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1
```

PowerShell

Untuk melampirkan antarmuka jaringan

Gunakan Add-EC2NetworkInterfacecmdlet.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1
```

Lepaskan antarmuka jaringan

Anda dapat melepaskan antarmuka jaringan sekunder yang terpasang ke instans EC2 kapan saja, menggunakan halaman Instans atau Antarmuka Jaringan dari konsol Amazon EC2.

Jika Anda mencoba melepaskan antarmuka jaringan yang dilampirkan ke sumber daya dari layanan lain, seperti penyeimbang beban Elastic Load Balancing, fungsi Lambda, WorkSpace a, atau gateway NAT, Anda mendapatkan kesalahan bahwa Anda tidak memiliki izin untuk mengakses sumber daya. Untuk menemukan layanan mana yang menciptakan sumber daya yang melekat pada antarmuka jaringan, periksa deskripsi antarmuka jaringan. Jika Anda menghapus sumber daya, maka antarmuka jaringannya akan dihapus.

Console

Untuk melepaskan antarmuka jaringan menggunakan halaman Instances

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih kotak centang untuk instans. Periksa Antarmuka jaringan bagian tab Jaringan untuk memverifikasi bahwa antarmuka jaringan dilampirkan ke sebuah instans sebagai antarmuka jaringan sekunder.
4. Pilih Tindakan, Jaringan, Lepaskan antarmuka jaringan.
5. Pilih antarmuka jaringan dan pilih Lepaskan.

Untuk melepaskan antarmuka jaringan menggunakan halaman Network Interfaces

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih kotak centang untuk antarmuka jaringan. Periksa Detail instans bagian tab Detail untuk memverifikasi bahwa antarmuka jaringan dilampirkan ke sebuah instans sebagai antarmuka jaringan sekunder.
4. Pilih Tindakan, Lepaskan.
5. Saat diminta konfirmasi, pilih Lepaskan.
6. Jika antarmuka jaringan gagal untuk melepaskan dari instans, pilih Lepaskan paksa, Aktifkan lalu coba lagi. Kami menyarankan lepaskan paksa hanya sebagai pilihan terakhir. Memaksakan pelepasan dapat mencegah Anda melampirkan antarmuka jaringan yang berbeda pada indeks yang sama hingga Anda memulai ulang instans. Ini juga dapat mencegah metadata instans agar tidak mencerminkan bahwa antarmuka jaringan telah dilepaskan hingga Anda memulai ulang instans.

AWS CLI

Untuk melepaskan antarmuka jaringan

Gunakan perintah berikut detach-network-interface.

```
aws ec2 detach-network-interface --attachment-id eni-attach-016c93267131892c9
```

PowerShell

Untuk melepaskan antarmuka jaringan

Gunakan Dismount-EC2NetworkInterfacecmdlet.

```
Dismount-EC2NetworkInterface -AttachmentId eni-attach-016c93267131892c9
```

Kelola alamat IP untuk antarmuka jaringan Anda

Anda dapat mengelola alamat IP berikut untuk antarmuka jaringan Anda:

- Alamat IP elastis (satu per IPv4 alamat pribadi)
- IPv4 alamat
- IPv6 alamat

Console

Untuk mengelola alamat IP antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih kotak centang untuk antarmuka jaringan.
4. Untuk mengelola IPv4 dan IPv6 alamat, lakukan hal berikut:
   a. Pilih Tindakan, Kelola Alamat IP.
   b. Bentangkan antarmuka jaringan.
   c. Untuk IPv4 alamat, edit alamat IP sesuai kebutuhan. Untuk menetapkan IPv4 alamat tambahan, pilih Tetapkan alamat IP baru dan kemudian tentukan IPv4 alamat dari rentang subnet atau biarkan AWS pilih satu untuk Anda.

d. (Tumpukan ganda atau IPv6 hanya) Untuk IPv6 alamat, edit alamat IP sesuai kebutuhan. Untuk menetapkan IPv6 alamat tambahan, pilih Tetapkan alamat IP baru dan kemudian tentukan IPv6 alamat dari rentang subnet atau biarkan AWS pilih satu untuk Anda.

e. Untuk menetapkan atau membatalkan penetapan IPv4 alamat publik ke antarmuka jaringan, pilih Auto-assign IP publik. Anda dapat mengaktifkan atau menonaktifkan ini untuk antarmuka jaringan apa pun, tetapi itu hanya memengaruhi antarmuka jaringan utama.

f. (Dual stack atau IPv6 -only) Untuk Menetapkan IPv6 IP primer, pilih Aktifkan untuk menetapkan alamat utama. IPv6 GUA pertama yang terkait dengan antarmuka jaringan dipilih sebagai IPv6 alamat utama. Setelah Anda menetapkan IPv6 alamat utama, Anda tidak dapat mengubahnya. Alamat ini adalah IPv6 alamat utama sampai instance dihentikan atau antarmuka jaringan terlepas.

g. Pilih Simpan.

5. Untuk mengaitkan alamat IP Elastis, lakukan hal berikut:

   a. Pilih Tindakan, Alamat Asosiasi.

   b. Untuk alamat IP Elastis, pilih alamat IP Elastis.

   c. Untuk IPv4 alamat Pribadi, pilih IPv4 alamat pribadi untuk dikaitkan dengan alamat IP Elastis.

   d. (Opsional) Pilih Izinkan alamat IP Elastis untuk dialihkan jika antarmuka jaringan saat ini terkait dengan instans lain atau antarmuka jaringan.

   e. Pilih Kaitkan.

6. Untuk memisahkan alamat IP Elastis, lakukan hal berikut:

   a. Pilih Tindakan, Pisahkan Alamat.

   b. Untuk Alamat IP publik, pilih alamat IP Elastis.

   c. Pilih Pisahkan.

AWS CLI

Untuk mengelola IPv4 alamat

Gunakan assign-private-ip-addressesperintah berikut untuk menetapkan IPv4 alamat.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-1234567890abcdef0 \
```

```
    --private-ip-addresses 10.0.0.82
```

Gunakan unassign-private-ip-addressesperintah berikut untuk membatalkan penetapan alamat. IPv4

```
aws ec2 unassign-private-ip-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --private-ip-addresses 10.0.0.82
```

Untuk mengelola IPv6 alamat

Gunakan perintah assign-ipv6-address berikut untuk menetapkan alamat. IPv6

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Gunakan perintah unassign-ipv6-address berikut untuk membatalkan penetapan alamat. IPv6

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Untuk mengelola alamat IP Elastis untuk IPv4 alamat pribadi utama

Gunakan perintah asosiasi-alamat berikut untuk mengaitkan alamat IP Elastis dengan alamat pribadi utama. IPv4

```
aws ec2 associate-address \
    --allocation-id eipalloc-0b263919b6EXAMPLE \
    --network-interface-id eni-1234567890abcdef0
```

Gunakan perintah disassociate-address berikut untuk memisahkan alamat IP Elastis dari alamat pribadi utama. IPv4

```
aws ec2 disassociate-address --association-id eipassoc-2bebb745a1EXAMPLE
```

PowerShell

Untuk mengelola IPv4 alamat

Gunakan Register-EC2PrivateIpAddresscmdlet untuk menetapkan alamat. IPv4

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.0.0.82
```

Gunakan Unregister-EC2PrivateIpAddresscmdlet untuk membatalkan penetapan alamat. IPv4

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.0.0.82
```

Untuk mengelola IPv6 alamat

Gunakan AddressList cmdlet Register-EC2Ipv6 untuk menetapkan alamat. IPv6

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Gunakan AddressList cmdlet Unregister-EC2Ipv6 untuk membatalkan penetapan alamat. IPv6

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Untuk mengelola alamat IP Elastis untuk IPv4 alamat pribadi utama

Gunakan Register-EC2Addresscmdlet untuk mengaitkan alamat IP Elastis dengan alamat pribadi IPv4 utama.

```
Register-EC2Address `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -AllocationId eipalloc-0b263919b6EXAMPLE
```

Gunakan Unregister-EC2Addresscmdlet untuk memisahkan alamat IP Elastis dari alamat pribadi utama. IPv4

```
Unregister-EC2Address -AssociationId eipassoc-2bebb745a1EXAMPLE
```

Memodifikasi atribut antarmuka jaringan

Anda dapat mengubah atribut antarmuka jaringan berikut:

- Deskripsi
- Grup keamanan
- Hapus saat penghentian
- Pemeriksaan sumber/tujuan
- Waktu habis pelacakan koneksi idle

Pertimbangan-pertimbangan

Anda tidak dapat mengubah atribut antarmuka jaringan yang dikelola pemohon.

Console

Untuk memodifikasi atribut antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih kotak centang untuk antarmuka jaringan.
4. Untuk mengubah deskripsi, lakukan hal berikut
   a. Pilih Tindakan, Ubah deskripsi.
   b. Untuk Deskripsi, masukkan deskripsi.
   c. Pilih Simpan.
5. Untuk mengubah grup keamanan, lakukan hal berikut:
   a. Pilih Tindakan, Ubah grup keamanan.
   b. Untuk grup keamanan terkait, tambahkan dan hapus grup keamanan sesuai kebutuhan. Grup keamanan dan antarmuka jaringan harus dibuat untuk VPC yang sama.
   c. Pilih Simpan.
6. Untuk mengubah perilaku penghentian, lakukan hal berikut:
   a. Pilih Tindakan, Ubah perilaku penghentian.
   b. Pilih atau hapus Hapus saat penghentian, Aktifkan.

c. Pilih Simpan.

7. Untuk mengubah source/destination pemeriksaan, lakukan hal berikut:

   a. Pilih Tindakan, Ubah pemeriksaan source/dest.

   b. Pilih atau hapus pemeriksaan sumber/tujuan, Aktifkan.

   c. Pilih Simpan.

8. Untuk mengubah batas waktu pelacakan koneksi idle, lakukan hal berikut:

   a. Pilih Tindakan, Ubah batas waktu pelacakan koneksi idle.

   b. Ubah nilai batas waktu sesuai kebutuhan. Untuk informasi selengkapnya, lihat Waktu habis pelacakan koneksi idle.

      - TCP menetapkan batas waktu: Batas waktu (dalam detik) untuk koneksi TCP idle dalam keadaan mapan.
        - Min: `60` detik
        - Max: `432000` detik
        - Default: `350` detik untuk jenis instans Nitrov6, tidak termasuk P6e-. GB200 Dan `432000` detik untuk jenis contoh lainnya, termasuk P6e-. GB200
        - Direkomendasikan: Kurang dari `432000` detik
      - Batas waktu UDP: Batas waktu (dalam detik) untuk alur UDP idle yang telah melihat lalu lintas hanya dalam satu arah atau transaksi permintaan-respons tunggal.
        - Min: `30` detik
        - Max: `60` detik
        - Default: `30` detik
      - Batas waktu aliran UDP: Batas waktu (dalam detik) untuk alur UDP idle yang diklasifikasikan sebagai alur yang telah melihat lebih dari satu transaksi permintaan-respons.
        - Min: `60` detik
        - Max: `180` detik
        - Default: `180` detik

   c. Pilih Simpan.

AWS CLI

Example Contoh: Untuk memodifikasi deskripsi

Gunakan perintah berikut modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --description "my updated description"
```

Example Contoh: Untuk memodifikasi grup keamanan

Gunakan perintah berikut modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --groups sg-1234567890abcdef0
```

Example Contoh: Untuk memodifikasi perilaku penghentian

Gunakan perintah berikut modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --attachment AttachmentId=eni-attach-43348162abEXAMPLE,DeleteOnTermination=false
```

Example Contoh: Untuk mengaktifkan source/destination pemeriksaan

Gunakan perintah berikut modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --source-dest-check
```

Example Contoh: Untuk memodifikasi waktu pelacakan koneksi idle

Gunakan perintah berikut modify-network-interface-attribute. Untuk informasi selengkapnya, lihat Waktu habis pelacakan koneksi idle.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
```

```
    --connection-tracking-specification
 TcpEstablishedTimeout=172800,UdpStreamTimeout=90,UdpTimeout=60
```

PowerShell

Example Contoh: Untuk memodifikasi deskripsi

Gunakan Edit-EC2NetworkInterfaceAttributecmdlet.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Description "my updated description"
```

Example Contoh: Untuk memodifikasi grup keamanan

Gunakan Edit-EC2NetworkInterfaceAttributecmdlet.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Group sg-1234567890abcdef0
```

Example Contoh: Untuk memodifikasi perilaku penghentian

Gunakan Edit-EC2NetworkInterfaceAttributecmdlet.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Attachment_AttachmentId eni-attach-43348162abEXAMPLE `
    -Attachment_DeleteOnTermination $false
```

Example Contoh: Untuk mengaktifkan source/destination pemeriksaan

Gunakan Edit-EC2NetworkInterfaceAttributecmdlet.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -SourceDestCheck $true
```

Example Contoh: Untuk memodifikasi batas waktu pelacakan koneksi idle

Gunakan Edit-EC2NetworkInterfaceAttributecmdlet. Untuk informasi selengkapnya, lihat Waktu habis pelacakan koneksi idle.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -ConnectionTrackingSpecification_TcpEstablishedTimeout 172800 `
    -ConnectionTrackingSpecification_UdpStreamTimeout 90 `
    -ConnectionTrackingSpecification_UdpTimeout 60
```

Beberapa antarmuka jaringan untuk instans Amazon EC2 Anda

Melampirkan beberapa antarmuka jaringan ke sebuah instance berguna ketika Anda membutuhkan yang berikut ini:

- Jaringan manajemen.
- Peralatan jaringan dan keamanan.
- Instans dual-homed dengan beban kerja di subnet yang berbeda atau. VPCs
- Solusi anggaran rendah dan ketersediaan tinggi.

Jaringan manajemen

Ikhtisar berikut menjelaskan jaringan manajemen yang dibuat menggunakan beberapa antarmuka jaringan.

Kriteria

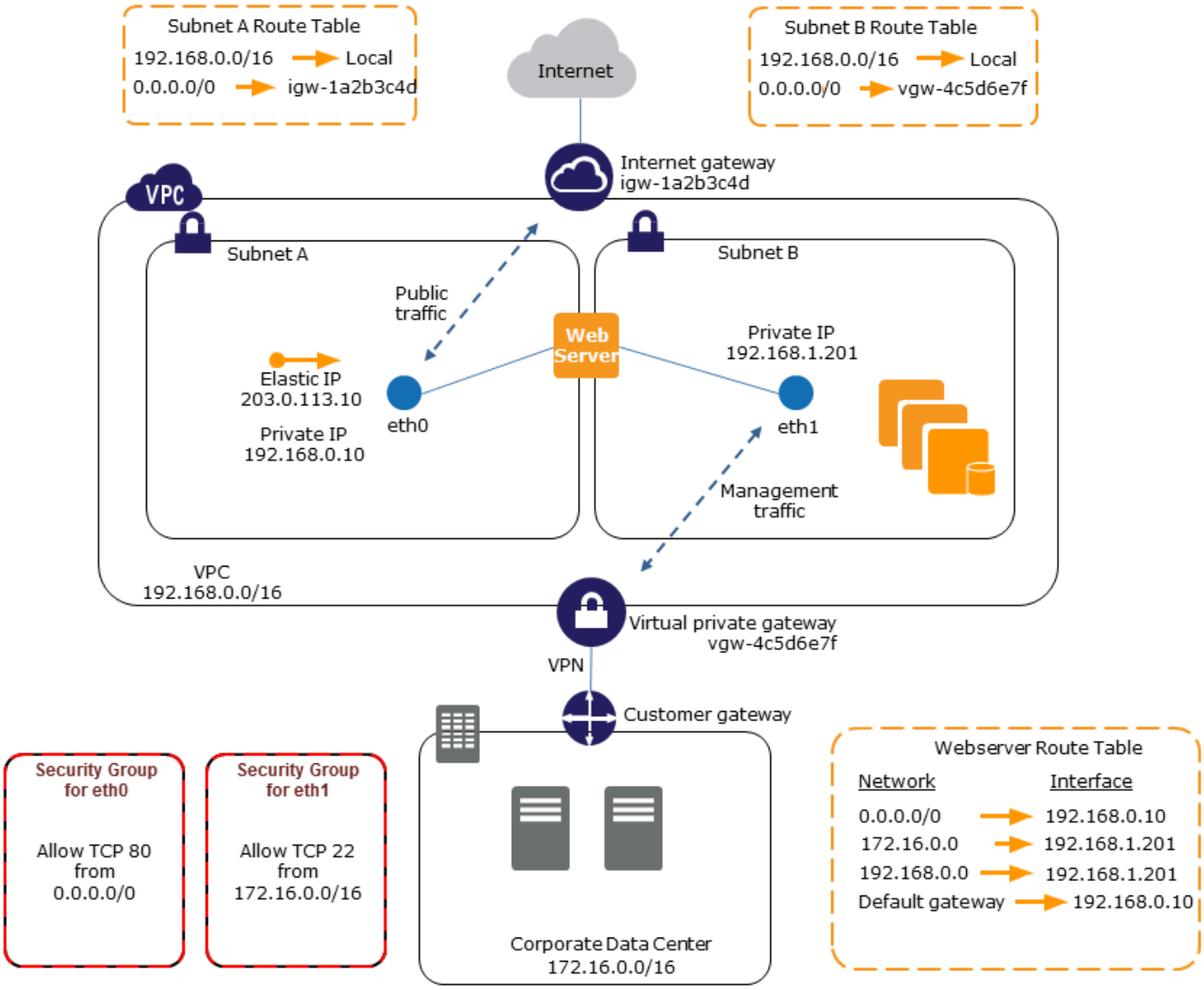
- Antarmuka jaringan utama pada instance (misalnya,eth0) menangani lalu lintas publik.
- Antarmuka jaringan sekunder pada instance (misalnya,eth1) menangani lalu lintas manajemen backend. Ini terhubung ke subnet terpisah yang memiliki kontrol akses yang lebih ketat, dan terletak di dalam Availability Zone yang sama dengan antarmuka jaringan utama.

Pengaturan

- Antarmuka jaringan primer, yang mungkin atau mungkin tidak berada di belakang penyeimbang beban, memiliki grup keamanan terkait yang memungkinkan akses ke server dari internet. Misalnya, izinkan port TCP 80 dan 443 dari 0.0.0.0/0 atau dari penyeimbang beban.
- Antarmuka jaringan sekunder memiliki grup keamanan terkait yang memungkinkan akses SSH saja, dimulai dari salah satu lokasi berikut:
  - Rentang alamat IP yang diizinkan, baik di dalam VPC, atau dari internet.

- Subnet pribadi dalam Availability Zone yang sama dengan antarmuka jaringan utama.
- Virtual private gateway.

> **Note**
>
> Untuk memastikan kemampuan failover, pertimbangkan untuk menggunakan private sekunder IPv4 untuk lalu lintas masuk pada antarmuka jaringan. Jika terjadi kegagalan instans, Anda dapat memindahkan IPv4 alamat pribadi and/or sekunder antarmuka ke instance siaga.



Peralatan jaringan dan keamanan

Beberapa peralatan jaringan dan keamanan, seperti penyeimbang beban, server network address translation (NAT), dan server proksi lebih suka dikonfigurasi dengan beberapa antarmuka jaringan. Anda dapat membuat dan memasang antarmuka jaringan sekunder ke instans yang menjalankan tipe aplikasi ini dan mengonfigurasi antarmuka tambahan dengan alamat IP publik dan privatnya sendiri, grup keamanan, dan pemeriksaan sumber/tujuan.

Instans dual-homed dengan beban kerja di subnet yang berbeda

Anda dapat menempatkan antarmuka jaringan di setiap server web Anda yang terhubung ke jaringan tingkat menengah tempat server aplikasi berada. Server aplikasi juga bisa menjadi dual-homed ke jaringan backend (subnet) tempat server basis data berada. Alih-alih merutekan paket jaringan melalui instans dual-homed, setiap instans dual-homed menerima dan memproses permintaan di front end, memulai koneksi ke backend, dan kemudian mengirim permintaan ke server di jaringan backend.

Instans dual-homed dengan beban kerja berbeda di akun yang sama VPCs

Anda dapat meluncurkan instans EC2 dalam satu VPC dan melampirkan ENI sekunder dari VPC yang berbeda, selama antarmuka jaringan berada di Availability Zone yang sama dengan instance. Ini memungkinkan Anda membuat instance multi-homed VPCs dengan konfigurasi jaringan dan keamanan yang berbeda. Anda tidak dapat membuat instance multi-homed VPCs di akun yang berbeda. AWS

Anda dapat menggunakan instance dual-homed VPCs di seluruh kasus penggunaan berikut:

- Atasi tumpang tindih CIDR antara dua VPCs yang tidak dapat diintip bersama: Anda dapat memanfaatkan CIDR sekunder dalam VPC dan mengizinkan instance untuk berkomunikasi di dua rentang IP yang tidak tumpang tindih.
- Connect multiple in a single account: Aktifkan komunikasi antar sumber daya individual yang biasanya dipisahkan oleh VPCs batas-batas VPC.

Solusi anggaran rendah dan ketersediaan tinggi

Jika salah satu instans Anda yang melayani fungsi tertentu gagal, antarmuka jaringannya dapat dilampirkan ke instans pengganti atau hot standby yang telah dikonfigurasi sebelumnya untuk peran yang sama guna memulihkan layanan dengan cepat. Misalnya, Anda dapat menggunakan antarmuka jaringan sebagai antarmuka jaringan primer atau sekunder ke layanan penting seperti instans basis data atau instans NAT. Jika instans gagal, Anda (atau lebih mungkin, kode yang berjalan atas nama Anda) dapat memasang antarmuka jaringan ke instans hot standby. Karena antarmuka mempertahankan alamat IP privatnya, alamat IP Elastis, dan alamat MAC, lalu lintas jaringan mulai mengalir ke instans siaga segera setelah Anda memasang antarmuka jaringan ke instans pengganti. Pengguna mengalami kehilangan konektivitas singkat antara waktu instans gagal dan waktu saat antarmuka jaringan dilampirkan ke instans standby, tetapi tidak ada perubahan pada tabel rute VPC atau server DNS Anda yang diperlukan.

Antarmuka jaringan yang dikelola pemohon

Antarmuka jaringan yang dikelola pemohon adalah antarmuka jaringan yang dibuat di VPC Layanan AWS Anda atas nama Anda. Antarmuka jaringan dikaitkan dengan sumber daya untuk layanan lain, seperti instans DB dari Amazon RDS, gateway NAT, atau titik akhir VPC antarmuka dari. AWS PrivateLink

Pertimbangan-pertimbangan

- Anda dapat melihat antarmuka jaringan yang dikelola pemohon di akun Anda. Anda dapat menambah atau menghapus tanda, tetapi Anda tidak dapat mengubah properti lain dari antarmuka jaringan yang dikelola pemohon.
- Anda tidak dapat melepaskan antarmuka jaringan yang dikelola pemohon.
- Saat Anda menghapus sumber daya yang terkait dengan antarmuka jaringan yang dikelola pemohon, antarmuka jaringan Layanan AWS terlepas dan menghapusnya. Jika layanan melepaskan antarmuka jaringan tetapi tidak menghapusnya, Anda dapat menghapus antarmuka jaringan yang terpisah.

Console

Untuk melihat antarmuka jaringan yang dikelola pemohon

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Jaringan & Keamanan, Antarmuka Jaringan.
3. Pilih ID antarmuka jaringan untuk membuka halaman detailnya.
4. Berikut ini adalah bidang kunci yang dapat Anda gunakan untuk menentukan tujuan antarmuka jaringan:
   - Deskripsi: Deskripsi yang disediakan oleh AWS layanan yang menciptakan antarmuka. Misalnya, “VPC Endpoint Interface vpce 089f2123488812123”.
   - Requester-managed: Menunjukkan apakah antarmuka jaringan dikelola oleh. AWS
   - ID Pemohon: Alias atau ID AWS akun dari prinsipal atau layanan yang membuat antarmuka jaringan. Jika Anda membuat antarmuka jaringan, ini adalah Akun AWS ID Anda. Jika tidak, pengguna utama atau layanan lain menciptakannya.

AWS CLI

Untuk melihat antarmuka jaringan yang dikelola pemohon

Gunakan perintah describe-network-interfaces sebagai berikut.

```
aws ec2 describe-network-interfaces \
    --filters "Name=requester-managed,Values=true" \
    --query "NetworkInterfaces[*].[Description, InterfaceType]" \
    --output table
```

Berikut ini adalah contoh output yang menunjukkan bidang kunci yang dapat Anda gunakan untuk menentukan tujuan antarmuka jaringan: `Description` dan `InterfaceType`.

```
-------------------------------------------------------------------------------
|                          DescribeNetworkInterfaces                          |
+---------------------------------------------------+-------------------------+
|  VPC Endpoint Interface: vpce-0f00567fa8477a1e6   |  interface              |
|  VPC Endpoint Interface vpce-0d8ddce4be80e4474    |  interface              |
|  VPC Endpoint Interface vpce-078221a1e27d1ea5b    |  vpc_endpoint           |
|  Resource Gateway Interface rgw-0bba03f3d56060135 |  interface              |
|  VPC Endpoint Interface: vpce-0cc199f605eaeace7   |  interface              |
|  VPC Endpoint Interface vpce-019b90d6f16d4f958    |  interface              |
+---------------------------------------------------+-------------------------+
```

PowerShell

Untuk melihat antarmuka jaringan yang dikelola pemohon

Gunakan Get-EC2NetworkInterfacecmdlet sebagai berikut.

```
Get-EC2NetworkInterface -Filter @{Name="requester-managed"; Values="true"} | Select
 Description, InterfaceType
```

Berikut ini adalah contoh output yang menunjukkan bidang kunci yang dapat Anda gunakan untuk menentukan tujuan antarmuka jaringan: `Description` dan`InterfaceType`.

```
Description                                    InterfaceType
-----------                                    -------------
VPC Endpoint Interface: vpce-0f00567fa8477a1e6   interface
VPC Endpoint Interface vpce-0d8ddce4be80e4474    interface
```

```
VPC Endpoint Interface vpce-078221a1e27d1ea5b    vpc_endpoint
Resource Gateway Interface rgw-0bba03f3d56060135 interface
VPC Endpoint Interface: vpce-0cc199f605eaeace7   interface
VPC Endpoint Interface vpce-019b90d6f16d4f958    interface
```

Delegasi awalan untuk antarmuka jaringan Amazon EC2

Anda dapat menetapkan rentang pribadi IPv4 atau IPv6 CIDR, baik secara otomatis atau manual, ke antarmuka jaringan Anda. Dengan menetapkan prefiks, Anda menskalakan dan menyederhanakan manajemen aplikasi, termasuk aplikasi kontainer dan jaringan yang memerlukan beberapa alamat IP pada sebuah instans. Untuk informasi selengkapnya tentang IPv4 dan IPv6 alamat, lihatPengalamatan IP instans Amazon EC2.

Pilihan penetapan berikut tersedia:

- Penugasan otomatis — AWS memilih awalan dan menetapkannya ke antarmuka jaringan Anda. Jika subnet untuk antarmuka jaringan memiliki jenis reservasi CIDR subnet`prefix`, kami memilih awalan dari reservasi CIDR subnet. Jika tidak, kami memilihnya dari rentang CIDR subnet.
- Penugasan manual — Anda menentukan awalan dan AWS memverifikasi bahwa itu belum ditetapkan ke sumber daya lain sebelum menetapkannya ke antarmuka jaringan Anda.

Menetapkan prefiks memiliki manfaat sebagai berikut:

- Peningkatan alamat IP pada antarmuka jaringan — Ketika Anda menggunakan prefiks, Anda menetapkan blok alamat IP sebagai lawan dari alamat IP individual. Ini meningkatkan jumlah alamat IP untuk antarmuka jaringan.
- Manajemen VPC yang disederhanakan untuk kontainer — Dalam aplikasi kontainer, setiap kontainer memerlukan alamat IP yang unik. Menetapkan awalan ke instans menyederhanakan pengelolaan Anda VPCs, karena Anda dapat meluncurkan dan menghentikan container tanpa harus memanggil Amazon EC2 APIs untuk penetapan IP individual.

Daftar Isi

- Hal-hal mendasar
- Pertimbangan-pertimbangan
- Kelola awalan untuk antarmuka jaringan Anda
  - Tetapkan prefiks selama pembuatan antarmuka jaringan

- Tetapkan awalan ke antarmuka jaringan yang ada
- Hapus prefiks dari antarmuka jaringan Anda

Hal-hal mendasar

- Anda dapat menetapkan prefiks ke antarmuka jaringan baru atau yang sudah ada.
- Untuk menggunakan prefiks, Anda menetapkan prefiks ke antarmuka jaringan Anda, melampirkan antarmuka jaringan ke instans Anda, lalu mengonfigurasi sistem operasi Anda.
- Saat Anda memilih opsi untuk menentukan prefiks, prefiks harus memenuhi persyaratan berikut ini:
  - IPv4 Awalan yang dapat Anda tentukan adalah `/28`.
  - IPv6 Awalan yang dapat Anda tentukan adalah `/80`.
  - Prefiks ada di subnet CIDR antarmuka jaringan, dan tidak tumpang tindih dengan prefiks lain atau alamat IP yang ditetapkan ke sumber daya yang ada di subnet.
- Anda dapat menetapkan prefiks ke antarmuka jaringan primer atau sekunder.
- Anda dapat menetapkan alamat IP Elastis ke antarmuka jaringan yang memiliki prefiks yang ditetapkan untuk itu.
- Anda juga dapat menetapkan alamat IP Elastis ke bagian alamat IP dari prefiks yang ditetapkan.
- Kami menyelesaikan nama host DNS pribadi dari sebuah instance ke IPv4 alamat pribadi utama.
- Kami menetapkan setiap IPv4 alamat pribadi untuk antarmuka jaringan, termasuk yang dari awalan, menggunakan format berikut:
  - Wilayah `us-east-1`

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Wilayah Lainnya

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Pertimbangan-pertimbangan

Pertimbangkan hal berikut ini saat Anda menggunakan prefiks:

- Antarmuka jaringan dengan awalan didukung dengan instance berbasis Nitro.
- Awalan untuk antarmuka jaringan harus menggunakan IPv6 alamat atau alamat pribadi. IPv4

- Jumlah maksimum alamat IP yang dapat Anda tetapkan ke antarmuka jaringan tergantung pada tipe instans. Setiap prefiks yang Anda tetapkan ke antarmuka jaringan dihitung sebagai satu alamat IP. Misalnya, sebuah `c5.large` instance memiliki batas `10` IPv4 alamat per antarmuka jaringan. Setiap antarmuka jaringan untuk contoh ini memiliki IPv4 alamat utama. Jika antarmuka jaringan tidak memiliki IPv4 alamat sekunder, Anda dapat menetapkan hingga 9 awalan ke antarmuka jaringan. Untuk setiap IPv4 alamat tambahan yang Anda tetapkan ke antarmuka jaringan, Anda dapat menetapkan satu awalan kurang ke antarmuka jaringan. Untuk informasi selengkapnya, lihat Alamat IP maksimum per antarmuka jaringan.
- Awalan termasuk dalam source/destination cek.
- Anda harus mengonfigurasi sistem operasi Anda untuk bekerja dengan antarmuka jaringan dengan prefiks. Perhatikan hal-hal berikut:
  - Beberapa Amazon Linux AMIs berisi skrip tambahan yang diinstal oleh AWS, yang dikenal sebagai`ec2-net-utils`. Skrip ini secara opsional mengotomatiskan konfigurasi antarmuka jaringan Anda. Mereka hanya untuk digunakan di Amazon Linux.
  - Untuk kontainer, Anda dapat menggunakan Container Network Interface (CNI) untuk plug-in Kubernetes, atau `dockerd` jika Anda menggunakan Docker untuk mengelola kontainer Anda.

Kelola awalan untuk antarmuka jaringan Anda

Ketika Anda menetapkan awalan ke antarmuka jaringan, Anda dapat memilih apakah akan membiarkan kami secara otomatis menetapkan awalan atau Anda dapat menentukan awalan kustom. Jika Anda membiarkan kami secara otomatis menetapkan awalan dan subnet untuk antarmuka jaringan memiliki jenis reservasi CIDR subnet`prefix`, kami memilih awalan dari reservasi CIDR subnet. Jika tidak, kami memilihnya dari rentang CIDR subnet.

Tugas

- Tetapkan prefiks selama pembuatan antarmuka jaringan
- Tetapkan awalan ke antarmuka jaringan yang ada
- Hapus prefiks dari antarmuka jaringan Anda

Tetapkan prefiks selama pembuatan antarmuka jaringan

Anda dapat menetapkan awalan otomatis atau kustom saat membuat antarmuka jaringan.

Console

Untuk menetapkan prefiks otomatis selama pembuatan antarmuka jaringan

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih Buat antarmuka jaringan.
4. Masukkan deskripsi untuk antarmuka jaringan, pilih subnet untuk membuat antarmuka jaringan, dan konfigurasikan pribadi IPv4 dan IPv6 alamat.
5. Perluas Pengaturan lanjutan.
6. Untuk delegasi IPv4 awalan lakukan salah satu hal berikut:
   - Untuk menetapkan IPv4 awalan secara otomatis, pilih Tetapkan otomatis. Untuk Jumlah IPv4 awalan, masukkan jumlah awalan yang akan ditetapkan.
   - Untuk menetapkan IPv4 awalan tertentu, pilih Kustom. Pilih Tambahkan awalan baru dan masukkan awalan.
7. Untuk delegasi IPv6 awalan lakukan salah satu hal berikut:
   - Untuk menetapkan IPv6 awalan secara otomatis, pilih Tetapkan otomatis. Untuk Jumlah IPv6 awalan, masukkan jumlah awalan yang akan ditetapkan.
   - Untuk menetapkan IPv6 awalan tertentu, pilih Kustom. Pilih Tambahkan awalan baru dan masukkan awalan.

   > **Note**
   >
   > IPv6 delegasi awalan hanya muncul jika subnet yang dipilih diaktifkan untuk. IPv6
8. Pilih grup keamanan yang akan dikaitkan dengan antarmuka jaringan dan tetapkan tanda sumber daya jika diperlukan.
9. Pilih Buat antarmuka jaringan.

AWS CLI

Untuk menetapkan IPv4 awalan otomatis selama pembuatan antarmuka jaringan

Gunakan create-network-interfaceperintah dan atur `--ipv4-prefix-count` ke jumlah IPv4 awalan AWS untuk menetapkan. Dalam contoh berikut, AWS berikan satu IPv4 awalan.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 automatic example" \
    --ipv4-prefix-count 1
```

Untuk menetapkan IPv4 awalan tertentu selama pembuatan antarmuka jaringan

Gunakan create-network-interfaceperintah dan atur `--ipv4-prefixes` ke awalan. AWS memilih IPv4 alamat dari rentang ini. Dalam contoh berikut, prefiks CIDR adalah 10.0.0.208/28.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Untuk menetapkan IPv6 awalan otomatis selama pembuatan antarmuka jaringan

Gunakan create-network-interfaceperintah dan atur `--ipv6-prefix-count` ke jumlah IPv6 awalan AWS untuk menetapkan. Dalam contoh berikut, AWS berikan satu IPv6 awalan.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 automatic example" \
    --ipv6-prefix-count 1
```

Untuk menetapkan IPv6 awalan tertentu selama pembuatan antarmuka jaringan

Gunakan create-network-interfaceperintah dan atur `--ipv6-prefixes` ke awalan. AWS memilih IPv6 alamat dari rentang ini. Dalam contoh berikut, prefiks CIDR adalah 2600:1f13:fc2:a700:1768::/80.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

PowerShell

Untuk menetapkan IPv4 awalan otomatis selama pembuatan antarmuka jaringan

Gunakan New-EC2NetworkInterfacecmdlet dan atur `Ipv4PrefixCount` ke jumlah IPv4 awalan untuk ditetapkan. AWS Dalam contoh berikut, AWS berikan satu IPv4 awalan.

```
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv4 automatic example' `
    -Ipv4PrefixCount 1
```

Untuk menetapkan IPv4 awalan tertentu selama pembuatan antarmuka jaringan

Gunakan New-EC2NetworkInterfacecmdlet dan atur `Ipv4Prefix` ke awalan. AWS memilih IPv4 alamat dari rentang ini. Dalam contoh berikut, prefiks CIDR adalah 10.0.0.208/28.

```
Import-Module AWS.Tools.EC2
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv4 manual example' `
    -Ipv4Prefix (New-Object `
        -TypeName Amazon.EC2.Model.Ipv4PrefixSpecificationRequest `
        -Property @{Ipv4Prefix = '10.0.0.208/28'})
```

Untuk menetapkan IPv6 awalan otomatis selama pembuatan antarmuka jaringan

Gunakan New-EC2NetworkInterfacecmdlet dan atur `Ipv6PrefixCount` ke jumlah IPv6 awalan untuk ditetapkan. AWS Dalam contoh berikut, AWS berikan satu IPv6 awalan.

```
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv6 automatic example' `
    -Ipv6PrefixCount 1
```

Untuk menetapkan IPv6 awalan tertentu selama pembuatan antarmuka jaringan

Gunakan New-EC2NetworkInterfacecmdlet dan atur `Ipv6Prefixes` ke awalan.
AWS memilih IPv6 alamat dari rentang ini. Dalam contoh berikut, prefiks CIDR adalah 2600:1f13:fc2:a700:1768::/80.

```
Import-Module AWS.Tools.EC2
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
```

```
    -Description 'IPv6 manual example' `
    -Ipv6Prefix (New-Object `
        -TypeName Amazon.EC2.Model.Ipv6PrefixSpecificationRequest `
        -Property @{Ipv6Prefix = '2600:1f13:fc2:a700:1768::/80'})
```

Tetapkan awalan ke antarmuka jaringan yang ada

Anda dapat menetapkan awalan otomatis atau kustom ke antarmuka jaringan yang ada.

Console

Untuk menetapkan prefiks otomatis ke antarmuka jaringan yang ada

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih antarmuka jaringan yang akan menetapkan prefiks, dan pilih Tindakan, Kelola prefiks.
4. Untuk delegasi IPv4 awalan lakukan salah satu hal berikut:
   - Untuk menetapkan IPv4 awalan secara otomatis, pilih Tetapkan otomatis. Untuk Jumlah IPv4 awalan, masukkan jumlah awalan yang akan ditetapkan.
   - Untuk menetapkan IPv4 awalan tertentu, pilih Kustom. Pilih Tambahkan awalan baru dan masukkan awalan.
5. Untuk delegasi IPv6 awalan lakukan salah satu hal berikut:
   - Untuk menetapkan IPv6 awalan secara otomatis, pilih Tetapkan otomatis. Untuk Jumlah IPv6 awalan, masukkan jumlah awalan yang akan ditetapkan.
   - Untuk menetapkan IPv6 awalan tertentu, pilih Kustom. Pilih Tambahkan awalan baru dan masukkan awalan.

   > **Note**
   >
   > IPv6 delegasi awalan hanya muncul jika subnet yang dipilih diaktifkan untuk. IPv6

6. Pilih Simpan.

AWS CLI

Gunakan perintah assign-ipv6-address untuk menetapkan awalan dan perintah untuk menetapkan IPv6 awalan ke antarmuka jaringan yang ada assign-private-ip-addresses. IPv4

Untuk menetapkan IPv4 awalan otomatis ke antarmuka jaringan yang ada

Gunakan assign-private-ip-addressesperintah dan atur `--ipv4-prefix-count` ke jumlah IPv4 awalan AWS untuk menetapkan. Dalam contoh berikut, AWS berikan satu IPv4 awalan.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefix-count 1
```

Untuk menetapkan IPv4 awalan tertentu ke antarmuka jaringan yang ada

Gunakan assign-private-ip-addressesperintah dan atur `--ipv4-prefixes` ke awalan. AWS memilih IPv4 alamat dari rentang ini. Dalam contoh berikut, prefiks CIDR adalah 10.0.0.208/28.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefixes 10.0.0.208/28
```

Untuk menetapkan IPv6 awalan otomatis ke antarmuka jaringan yang ada

Gunakan perintah assign-ipv6-address dan atur `--ipv6-prefix-count` ke jumlah awalan untuk ditetapkan. IPv6 AWS Dalam contoh berikut, AWS berikan satu IPv6 awalan.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefix-count 1
```

Untuk menetapkan IPv6 awalan tertentu ke antarmuka jaringan yang ada

Gunakan perintah assign-ipv6-address dan atur ke awalan. `--ipv6-prefixes`
AWS memilih IPv6 alamat dari rentang ini. Dalam contoh berikut, prefiks CIDR adalah 2600:1f13:fc2:a700:18bb::/80.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

PowerShell

Untuk menetapkan IPv4 awalan otomatis ke antarmuka jaringan yang ada

Gunakan Register-EC2PrivateIpAddresscmdlet dan atur `Ipv4PrefixCount` ke jumlah IPv4 awalan untuk ditetapkan. AWS Dalam contoh berikut, AWS berikan satu IPv4 awalan.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4PrefixCount 1
```

Untuk menetapkan IPv4 awalan tertentu ke antarmuka jaringan yang ada

Gunakan Register-EC2PrivateIpAddresscmdlet dan atur `Ipv4Prefix` ke awalan. AWS memilih IPv4 alamat dari rentang ini. Dalam contoh berikut, prefiks CIDR adalah 10.0.0.208/28.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4Prefix '10.0.0.208/28'
```

Untuk menetapkan IPv6 awalan otomatis ke antarmuka jaringan yang ada

Gunakan AddressList cmdlet Register-EC2Ipv6 dan atur `Ipv6PrefixCount` ke jumlah IPv4 awalan untuk ditetapkan. AWS Dalam contoh berikut, AWS berikan satu IPv6 awalan.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6PrefixCount 1
```

Untuk menetapkan IPv6 awalan tertentu ke antarmuka jaringan yang ada

Gunakan AddressList cmdlet Register-EC2Ipv6 dan atur `Ipv6Prefix` ke awalan. AWS memilih IPv6 alamat dari rentang ini. Dalam contoh berikut, prefiks CIDR adalah 2600:1f13:fc2:a700:18bb::/80.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6Prefix '2600:1f13:fc2:a700:18bb::/80'
```

Hapus prefiks dari antarmuka jaringan Anda

Anda dapat menghapus awalan dari antarmuka jaringan yang ada.

Console

Untuk menghapus prefiks dari antarmuka jaringan

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih antarmuka jaringan.
4. Pilih Tindakan, Kelola awalan.
5. Untuk delegasi IPv4 awalan, untuk menghapus awalan tertentu, pilih Unassign di sebelah awalan yang akan dihapus. Untuk menghapus semua awalan, pilih Jangan tetapkan.
6. Untuk delegasi IPv6 awalan, untuk menghapus awalan tertentu, pilih Unassign di sebelah awalan yang akan dihapus. Untuk menghapus semua awalan, pilih Jangan tetapkan.

   > **Note**
   >
   > IPv6 delegasi awalan hanya muncul jika subnet yang dipilih diaktifkan untuk. IPv6

7. Pilih Simpan.

AWS CLI

Anda dapat menggunakan perintah unassign-ipv6-address untuk menghapus awalan dan perintah untuk menghapus IPv6 awalan dari antarmuka jaringan yang ada unassign-private-ip-addresses. IPv4

Untuk menghapus IPv4 awalan dari antarmuka jaringan

Gunakan unassign-private-ip-addressesperintah dan atur `--ipv4-prefix` ke awalan CIDR untuk menghapus.

```
aws ec2 unassign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefixes 10.0.0.176/28
```

Untuk menghapus IPv6 awalan dari antarmuka jaringan

Gunakan perintah unassign-ipv6-address dan atur `--ipv6-prefix` ke awalan CIDR untuk menghapus.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

PowerShell

Untuk menghapus IPv4 awalan dari antarmuka jaringan

Gunakan Unregister-EC2PrivateIpAddresscmdlet dan atur `Ipv4Prefix` ke awalan CIDR untuk menghapus.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4Prefix '10.0.0.208/28'
```

Untuk menghapus IPv6 awalan dari antarmuka jaringan

Gunakan AddressList cmdlet Unregister-EC2Ipv6 dan atur `Ipv6Prefix` ke awalan CIDR untuk menghapus.

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6Prefix '2600:1f13:fc2:a700:18bb::/80'
```

Menghapus antarmuka jaringan

Menghapus antarmuka jaringan melepaskan semua atribut yang terkait dengan antarmuka dan melepaskan semua alamat IP privat atau alamat IP Elastis untuk digunakan oleh instans lain.

Anda tidak dapat menghapus antarmuka jaringan yang sedang digunakan. Pertama, Anda harus lepaskan antarmuka jaringan.

Console

Untuk menghapus antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan.
3. Pilih kotak centang untuk antarmuka jaringan, dan kemudian pilih Tindakan, Hapus.

4. Saat diminta konfirmasi, pilih Hapus.

AWS CLI

Untuk menghapus antarmuka jaringan

Gunakan perintah berikut delete-network-interface.

```
aws ec2 delete-network-interface --network-interface-id eni-1234567890abcdef0
```

PowerShell

Untuk menghapus antarmuka jaringan

Gunakan Remove-EC2NetworkInterfacecmdlet.

```
Remove-EC2NetworkInterface -NetworkInterfaceId eni-1234567890abcdef0
```

Bandwidth jaringan EC2 instans Amazon

Spesifikasi bandwidth instans berlaku untuk lalu lintas masuk dan keluar untuk instans. Misalnya, jika sebuah instance menentukan bandwidth hingga 10 Gbps, itu berarti ia memiliki bandwidth hingga 10 Gbps untuk lalu lintas masuk dan, secara bersamaan, hingga 10 Gbps untuk lalu lintas keluar. Bandwidth jaringan yang tersedia untuk sebuah EC2 instance tergantung pada beberapa faktor, sebagai berikut.

Lalu lintas multi-aliran

Bandwidth untuk lalu lintas multi-aliran dibatasi hingga 50% dari bandwidth yang tersedia untuk lalu lintas yang melewati gateway internet atau gateway lokal untuk contoh dengan 32 atau lebih vCPUs, atau 5 Gbps, mana yang lebih besar. Untuk contoh dengan kurang dari 32 vCPUs, bandwidth dibatasi hingga 5 Gbps.

Lalu lintas alur tunggal

Bandwidth untuk lalu lintas aliran tunggal dibatasi hingga 5 Gbps ketika instance tidak berada dalam grup penempatan cluster yang sama. Untuk mengurangi latensi dan meningkatkan bandwidth alur tunggal, cobalah lakukan salah satu hal berikut:

- Gunakan grup penempatan klaster untuk mencapai bandwidth hingga 10 Gbps untuk instans dalam grup penempatan yang sama.
- Siapkan beberapa jalur antara dua titik akhir untuk mencapai bandwidth yang lebih tinggi dengan Multipath TCP (MPTCP).
- Konfigurasikan ENA Express untuk instans yang memenuhi syarat dalam Availability Zone yang sama untuk mencapai hingga 25 Gbps di antara instans tersebut.

> **Note**
>
> Aliran tunggal dianggap sebagai aliran TCP atau UDP 5-tuple yang unik. Untuk protokol lain yang mengikuti header IP, seperti `GRE` atau`IPsec`, 3 tuple IP sumber, IP tujuan, dan protokol berikutnya digunakan untuk menentukan aliran.

Bandwidth instans yang tersedia

Bandwidth jaringan yang tersedia dari sebuah instance tergantung pada jumlah v CPUs yang dimilikinya. Misalnya, sebuah `m5.8xlarge` instance memiliki bandwidth jaringan 32 v CPUs dan 10 Gbps, dan sebuah `m5.16xlarge` instance memiliki bandwidth jaringan 64 v CPUs dan 20 Gbps. Namun, instans mungkin tidak mencapai bandwidth ini; misalnya, jika melebihi perizinan jaringan pada tingkat instans, seperti paket per detik atau jumlah koneksi yang dilacak. Berapa banyak bandwidth yang tersedia yang dapat digunakan lalu lintas tergantung pada jumlah v CPUs dan tujuan. Misalnya, sebuah `m5.16xlarge` instance memiliki 64 vCPUs, sehingga lalu lintas ke instance lain di Wilayah dapat memanfaatkan bandwidth penuh yang tersedia (20 Gbps). Namun, lalu lintas yang melewati gateway internet atau gateway lokal hanya dapat memanfaatkan 50% dari bandwidth yang tersedia (10 Gbps).

Biasanya, instance dengan 16 v CPUs atau kurang (ukuran `4xlarge` dan lebih kecil) didokumentasikan memiliki “hingga” bandwidth tertentu; misalnya, “hingga 10 Gbps”. Instans ini memiliki bandwidth acuan. Untuk memenuhi permintaan tambahan, mereka dapat menggunakan mekanisme kredit I/O jaringan untuk melampaui bandwidth dasar mereka. Instans dapat menggunakan lonjakan bandwidth untuk waktu yang terbatas, biasanya dari 5 hingga 60 menit, tergantung pada ukuran instans.

Sebuah instance menerima jumlah maksimum I/O kredit jaringan saat peluncuran. Jika instance menghabiskan I/O kredit jaringannya, ia kembali ke bandwidth dasarnya. Sebuah instance yang berjalan menghasilkan I/O kredit jaringan setiap kali menggunakan bandwidth jaringan lebih sedikit

daripada bandwidth dasarnya. Instans yang dihentikan tidak mendapatkan I/O kredit jaringan. Lonjakan instans adalah upaya terbaik, bahkan ketika instans memiliki kredit yang tersedia, karena lonjakan bandwidth adalah sumber daya bersama.

Ada bucket I/O kredit jaringan terpisah untuk lalu lintas masuk dan keluar.

Performa jaringan dasar dan lonjakan

Panduan Jenis EC2 Instans Amazon menjelaskan performa jaringan untuk setiap jenis instans, ditambah bandwidth jaringan dasar yang tersedia untuk instans yang dapat menggunakan bandwidth burst. Untuk informasi selengkapnya, lihat berikut ini:

- Spesifikasi jaringan — Tujuan umum
- Spesifikasi jaringan — Komputasi dioptimalkan
- Spesifikasi jaringan - Memori dioptimalkan
- Spesifikasi jaringan - Penyimpanan dioptimalkan
- Spesifikasi jaringan — Komputasi yang dipercepat
- Spesifikasi jaringan — Komputasi kinerja tinggi
- Spesifikasi jaringan — Generasi sebelumnya

Atau, Anda dapat menggunakan alat baris perintah untuk mendapatkan informasi ini. EC2 Konsol Amazon tidak menampilkan bandwidth jaringan dasar dari jenis instans.

AWS CLI

Anda dapat menggunakan describe-instance-typesperintah untuk menampilkan informasi tentang jenis instance. Contoh berikut menampilkan informasi performa jaringan untuk semua instans C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance,
 NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps] | sort_by(@,&[2])" \
    --output table
```

Berikut ini adalah output contoh. Jika output Anda tidak memiliki bandwidth dasar, perbarui ke versi terbaru. AWS CLI

```
-------------------------------------------
```

```
|           DescribeInstanceTypes           |
+--------------+--------------------+-------+
|  c5.large    |  Up to 10 Gigabit  |  0.75 |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25 |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5  |
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0  |
|  c5.9xlarge  |  12 Gigabit        |  12.0 |
|  c5.12xlarge |  12 Gigabit        |  12.0 |
|  c5.18xlarge |  25 Gigabit        |  25.0 |
|  c5.24xlarge |  25 Gigabit        |  25.0 |
|  c5.metal    |  25 Gigabit        |  25.0 |
+--------------+--------------------+-------+
```

PowerShell

Anda dapat menggunakan Get-EC2InstanceType PowerShell perintah untuk menampilkan informasi tentang jenis instance. Contoh berikut menampilkan informasi performa jaringan untuk semua instans C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
    Select-Object `
    InstanceType,
    @{Name = 'NetworkPerformance'; Expression =
 {($_.Networkinfo.NetworkCards.NetworkPerformance)}},
    @{Name = 'BaselineBandwidthInGbps'; Expression =
 {($_.Networkinfo.NetworkCards.BaselineBandwidthInGbps)}} | `
Format-Table -AutoSize
```

Berikut ini adalah output contoh.

```
InstanceType NetworkPerformance BaselineBandwidthInGbps
------------ ------------------ ----------------------
c5.4xlarge   Up to 10 Gigabit                     5.00
c5.xlarge    Up to 10 Gigabit                     1.25
c5.12xlarge  12 Gigabit                          12.00
c5.9xlarge   12 Gigabit                          12.00
c5.24xlarge  25 Gigabit                          25.00
c5.metal     25 Gigabit                          25.00
c5.2xlarge   Up to 10 Gigabit                     2.50
c5.large     Up to 10 Gigabit                     0.75
c5.18xlarge  25 Gigabit                          25.00
```

EC2 konfigurasi pembobotan bandwidth contoh

Beberapa jenis instance mendukung pembobotan bandwidth yang dapat dikonfigurasi, di mana Anda dapat memilih pembobotan bandwidth dasar yang mendukung pemrosesan jaringan atau operasi EBS. Pengaturan default untuk bandwidth dasar ditentukan oleh jenis instans Anda. Anda dapat mengonfigurasi pembobotan bandwidth selama peluncuran, atau memodifikasi pengaturan instans Anda dengan preferensi pembobotan berikut:

- default — Opsi ini menggunakan konfigurasi bandwidth standar untuk jenis instans Anda.
- vpc-1 — Opsi ini meningkatkan bandwidth dasar yang tersedia untuk jaringan dan mengurangi bandwidth dasar untuk operasi EBS.
- ebs-1 — Opsi ini meningkatkan bandwidth dasar yang tersedia untuk operasi EBS, dan mengurangi bandwidth dasar untuk jaringan.

Pertimbangan pembobotan bandwidth

Berikut ini adalah beberapa pertimbangan yang dapat memengaruhi strategi pembobotan bandwidth Anda.

- Pengaturan preferensi pembobotan bandwidth hanya memengaruhi spesifikasi bandwidth. Spesifikasi paket jaringan per detik (PPS) dan input/output operasi EBS per detik (IOPS) tidak berubah.
- Spesifikasi bandwidth gabungan antara jaringan dan EBS tidak berubah. Ketika Anda memilih konfigurasi pembobotan bandwidth, bandwidth dasar yang tersedia untuk opsi yang dipilih meningkat, dan bandwidth dasar untuk opsi yang tersisa dikurangi dengan jumlah absolut yang sama. Untuk semua instance kecuali instans Flex, bandwidth burst yang tersedia tetap sama untuk opsi yang Anda pilih, dan dikurangi untuk opsi yang tersisa. Untuk instans Flex hingga 4xlarge, bandwidth burst tetap tidak berubah. Untuk instance Flex 8xlarge dan lebih besar, bandwidth burst meningkat dengan jumlah yang sama dengan bandwidth dasar.
- Penting untuk memahami bagaimana perubahan alokasi bandwidth dapat memengaruhi I/O kinerja untuk EBS. Untuk EC2 contoh yang memiliki `vpc-1` konfigurasi (peningkatan bandwidth jaringan), Anda mungkin mengalami IOPS yang lebih rendah untuk volume EBS jika Anda mencapai batas bandwidth EBS sebelum mencapai batas IOPS. Ini lebih terlihat dengan I/O ukuran yang lebih besar.

Misalnya, pada jenis instans yang biasanya mendukung 240.000 IOPS dengan I/O ukuran 16 KiB, jika Anda memilih `vpc-1` pembobotan, itu mungkin mengurangi IOPS yang dapat dicapai karena batas bandwidth dasar EBS yang disesuaikan.

Saat merencanakan beban kerja Anda, pertimbangkan I/O ukuran dan pola Anda. I/O Ukuran yang lebih kecil cenderung tidak terpengaruh oleh keterbatasan bandwidth, sementara I/O ukuran yang lebih besar atau beban kerja berurutan mungkin melihat lebih banyak dampak dari perubahan bandwidth. Selalu uji beban kerja spesifik Anda untuk memastikan kinerja optimal dengan konfigurasi yang Anda pilih.

- Spesifikasi bandwidth multi-aliran jaringan untuk lalu lintas yang melewati gateway internet atau gateway lokal disesuaikan dengan 50% dari bandwidth dasar dari opsi yang dikonfigurasi atau 5 Gbps, jika berlaku. Untuk informasi selengkapnya, lihat Bandwidth jaringan EC2 instans Amazon.

  Contoh berikut didasarkan pada jenis instance yang memiliki bandwidth dasar default 40 Gbps, dan bandwidth batas default 20 Gbps. Jika Anda memilih pembobotan `vpc-1` bandwidth untuk contoh ini, bandwidth dasar tertimbang berubah menjadi 50 Gbps, dan bandwidth perbatasan berubah menjadi 25 Gbps.
- Fitur ini tersedia di semua wilayah komersial, selaras dengan ketersediaan EC2 instans dan dukungan.
- Fitur ini tidak menambahkan biaya tambahan ke EC2 instans Anda.

Jenis instans yang didukung untuk pembobotan bandwidth

Jenis instans dalam keluarga instance berikut mendukung pembobotan bandwidth yang dapat dikonfigurasi.

- Tujuan umum: m8a, m8g, m8gd, m8i, m8id, m8i-flex
- Komputasi dioptimalkan: C8a, C8g, C8gd, C8i, C8id, C8i-flex
- Memori dioptimalkan: R8a, R8g, R8gd, R8i, R8id, R8i-flex, X8g, X8AEDZ, X8i

Periksa pengaturan bandwidth saat ini

Untuk melihat pengaturan bandwidth saat ini untuk instans Anda, pilih salah satu tab untuk instruksi.

Console

Untuk mendapatkan pengaturan bandwidth untuk sebuah instance

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih contoh yang ingin Anda periksa dari daftar, dan arahkan ke tab Jaringan. Pengaturan Anda saat ini ditampilkan di bidang bandwidth yang Dikonfigurasi. Amazon EC2 menggunakan pengaturan default untuk jenis instans Anda jika bandwidth tidak disetel ke nilai tertentu.

AWS CLI

Untuk mendapatkan pengaturan bandwidth untuk sebuah instance

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].NetworkPerformanceOptions.BandwidthWeighting
 \
    --output text
```

Berikut ini adalah output contoh.

```
default
```

Contoh ini mencantumkan semua instance Anda yang memiliki preferensi pembobotan bandwidth yang disetel kevpc-1, untuk bandwidth jaringan yang lebih tinggi.

```
aws ec2 describe-instances \
    --filters "Name=network-performance-options.bandwidth-weighting,Values=vpc-1" \
    --query Reservations[].Instances[].InstanceId \
    --output text
```

PowerShell

Untuk mendapatkan pengaturan bandwidth untuk sebuah instance

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance `
    -
InstanceId i-1234567890abcdef0).Instances.NetworkPerformanceOptions.BandwidthWeighting.Value
```

Berikut ini adalah output contoh.

```
default
```

Contoh ini mencantumkan semua instance Anda yang memiliki preferensi pembobotan bandwidth yang disetel kevpc-1, untuk bandwidth jaringan yang lebih tinggi.

```
(Get-EC2Instance `
    -Filter @{Name="network-performance-options.bandwidth-
weighting";Values="vpc-1"}).Instances.InstanceId
```

Konfigurasikan pembobotan bandwidth untuk instans Anda

Anda dapat mengonfigurasi pembobotan bandwidth baik saat peluncuran atau dengan memodifikasi instance yang ada dari EC2 konsol, atau API/SDKs CLI.

Konfigurasikan pembobotan bandwidth saat Anda meluncurkan instance

Untuk mengonfigurasi pengaturan bandwidth saat Anda meluncurkan instance, pilih salah satu tab untuk instruksi.

Anda juga dapat menentukan pembobotan bandwidth dalam template peluncuran. Untuk membuat template peluncuran, lihatBuat template peluncuran Amazon EC2. Parameter yang akan disetel berada di lokasi yang sama seperti untuk meluncurkan instance langsung dari konsol. Perluas bagian Detail lanjutan, dan atur konfigurasi bandwidth Instance.

Untuk meluncurkan instance dengan template peluncuran Anda, lihatLuncurkan instans EC2 menggunakan template peluncuran.

Console

Untuk meluncurkan instance dengan pembobotan bandwidth yang dapat dikonfigurasi

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.

3. Pilih Luncurkan Instans. Ini membuka dialog Launch an instance. Ada beberapa cara tambahan yang bisa Anda dapatkan ke dialog peluncuran, tergantung pada preferensi Anda. Misalnya, Anda dapat meluncurkan instance langsung dari AMI atau dari EC2 dasbor Amazon itu sendiri.
4. Amazon Machine Image (AMI) yang Anda luncurkan harus didasarkan pada `Arm` arsitektur. Banyak gambar Mulai Cepat mendukung keduanya `x86` dan `Arm` arsitektur, Setelah Anda memilih sistem operasi untuk instance Anda, pilih `Arm` opsi dari daftar Arsitektur.
5. Jenis instance harus menjadi salah satu Tipe instans yang didukung untuk fitur ini.
6. Saat memperluas bagian Detail lanjutan, Anda dapat menggulir ke bawah untuk menemukan pengaturan konfigurasi bandwidth Instance. Pilih opsi konfigurasi bandwidth untuk instans Anda.
7. Konfigurasikan semua pengaturan lain untuk instance Anda seperti biasa, dan pilih Launch instance.

AWS CLI

Untuk meluncurkan instance dengan pembobotan bandwidth yang dapat dikonfigurasi

Gunakan perintah run-instance dengan opsi berikut untuk meluncurkan instance yang dikonfigurasi untuk pembobotan bandwidth jaringan yang lebih tinggi.

```
--network-performance-options BandwidthWeighting=vpc-1
```

Gunakan perintah run-instance dengan opsi berikut untuk meluncurkan instance yang dikonfigurasi untuk pembobotan bandwidth EBS yang lebih tinggi.

```
--network-performance-options BandwidthWeighting=ebs-1
```

PowerShell

Untuk meluncurkan instance dengan pembobotan bandwidth yang dapat dikonfigurasi

Gunakan New-EC2Instancecmdlet dengan parameter berikut untuk meluncurkan instance yang dikonfigurasi untuk pembobotan bandwidth jaringan yang lebih tinggi.

```
-NetworkPerformanceOptions_BandwidthWeighting vpc-1
```

Gunakan New-EC2Instancecmdlet dengan parameter berikut untuk meluncurkan instance yang dikonfigurasi untuk pembobotan bandwidth EBS yang lebih tinggi.

```
-NetworkPerformanceOptions_BandwidthWeighting ebs-1
```

Perbarui pembobotan bandwidth untuk instance yang ada

Untuk memperbarui pembobotan bandwidth untuk instance yang ada, instance Anda harus dalam `Stopped` status.

Console

Untuk memperbarui pembobotan bandwidth

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih contoh yang ingin Anda perbarui dari daftar.
4. Sebelum Anda mengubah konfigurasi bandwidth, instans Anda harus dalam `Stopped` keadaan. Jika instance Anda sedang berjalan, pilih Stop instance dari menu status Instance.
5. Pilih Kelola bandwidth dari menu Actions > Networking. Ini membuka dialog Kelola bandwidth.

   > **Note**
   >
   > Jika jenis instans Anda tidak mendukung konfigurasi untuk pembobotan bandwidth, item menu tersebut dinonaktifkan.

6. Pilih opsi untuk memperbarui instans Anda, dan pilih Ubah untuk menyimpan pengaturan Anda.

AWS CLI

Untuk memperbarui pembobotan bandwidth

Gunakan perintah modify-instance-network-performance-options untuk mengonfigurasi pembobotan bandwidth jaringan yang lebih tinggi untuk instance yang ditentukan.

```
aws ec2 modify-instance-network-performance-options \
```

```
    --instance-id i-1234567890abcdef0 \
    --bandwidth-weighting=vpc-1
```

Contoh berikut mengonfigurasi pembobotan bandwidth EBS yang lebih tinggi untuk instance yang ditentukan.

```
aws ec2 modify-instance-network-performance-options \
    --instance-id i-1234567890abcdef0 \
    --bandwidth-weighting=ebs-1
```

PowerShell

Untuk memperbarui pembobotan bandwidth

Gunakan Edit-EC2InstanceNetworkPerformanceOptioncmdlet untuk mengonfigurasi pembobotan bandwidth jaringan yang lebih tinggi untuk instance yang ditentukan.

```
Edit-EC2InstanceNetworkPerformanceOption `
    -InstanceId i-1234567890abcdef0 `
    -BandwidthWeighting vpc-1
```

Contoh berikut mengonfigurasi pembobotan bandwidth EBS yang lebih tinggi untuk instance yang ditentukan.

```
Edit-EC2InstanceNetworkPerformanceOption `
    -InstanceId i-1234567890abcdef0 `
    -BandwidthWeighting ebs-1
```

Kinerja jaringan

Tabel berikut menunjukkan kinerja jaringan, dalam Gbps, yang dapat dicapai dengan`default`,`vpc-1`, dan `ebs-1` konfigurasi.

Tipe instans	**`default`** (Garis dasar/Burst)	**`vpc-1`** (Garis dasar/Burst)	**`ebs-1`** (Garis dasar/Burst)
c8a.sedang	0,52/12,5	0,65/12,5	0,438/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8a.large	0,937/12,5	1.172/12,5	0,774/10.0
c8a.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
c8a.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
c8a.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
c8a.8xlarge	15.0	18.75	12,5
c8a.12xlarge	22.5	28.125	18.75
c8a.16xlarge	30.0	37,5	25.0
c8a.24xlarge	40.0	50.0	32.5
c8a.48xlarge	75.0	93,75	60.0
c8a.metal-24xl	40.0	50.0	32.5
c8a.metal-48xl	75.0	93,75	60.0
c8g.sedang	0,52/12,5	0,65/12,5	0,441/10.0
c8g.large	0,937/12,5	1.171/12,5	0,779/10.0
c8g.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
c8g.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
c8g.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
c8g.8xlarge	15.0	18.75	12,5
c8g.12xlarge	22.5	28.125	18.75
c8g.16xlarge	30.0	37,5	25.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8g.24xlarge	40.0	50.0	32.5
c8g.48xlarge	50.0	62.5	40.0
c8g.logam-24xl	40.0	50.0	32.5
c8g.logam-48xl	50.0	62.5	40.0
c8gd.sedang	0,52/12,5	0,65/12,5	0,441/10.0
c8gd.large	0,937/12,5	1.171/12,5	0,779/10.0
c8gd.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
c8gd.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
c8gd.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
c8gd.8xlarge	15.0	18.75	12,5
c8gd.12xlarge	22.5	28.125	18.75
c8gd.16xlarge	30.0	37,5	25.0
c8gd.24xlarge	40.0	50.0	32.5
c8gd.48xlarge	50.0	62.5	40.0
c8gd.metal-24xl	40.0	50.0	32.5
c8gd.metal-48xl	50.0	62.5	40.0
c8i.large	0,937/12,5	1.172/12,5	0,774/10.0
c8i.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
c8i.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8i.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
c8i.8xlarge	15.0	18.75	12,5
c8i.12xlarge	22.5	28.125	18.75
c8i.16xlarge	30.0	37,5	25.0
c8i.24xlarge	40.0	50.0	32.5
c8i.32xlarge	50.0	62.5	40.0
c8i.48xlarge	75.0	93,75	60.0
c8i.96xlarge	100.0	125.0	80.0
c8i.logam-48xl	75.0	93,75	60.0
c8i.logam-96xl	100.0	125.0	80.0
c8id.large	0,937/12,5	1.172/12,5	0,774/10.0
c8id.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
c8id.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
c8id.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
c8id.8xlarge	15.0	18.75	12,5
c8id.12xlarge	22.5	28.125	18.75
c8id.16xlarge	30.0	37,5	25.0
c8id.24xlarge	40.0	50.0	32.5
c8id.32xlarge	50.0	62.5	40.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8id.48xlarge	75.0	93,75	60.0
c8id.96xlarge	100.0	125.0	80.0
c8id.metal-48xl	75.0	93,75	60.0
c8id.metal-96xl	100.0	125.0	80.0
c8i-flex.large	0,468/12,5	0,585/12,5	0,389/10.0
c8i-flex.xlarge	0,937/12,5	1.172/12,5	0,779/10.0
c8i-flex.2xlarge	1,875/15,0	2.344/15.0	1,562/12,5
c8i-flex.4xlarge	3,75/15,0	4.688/15.0	3.125/12,5
c8i-flex.8xlarge	7,5/15,0	9.375/18.75	6.25/12,5
c8i-flex.12xlarge	11.25/22.5	14.063/28.125	9.375/18.75
c8i-flex.16xlarge	15.0/30.0	18.75/37,5	12,5/25.0
m8a.sedang	0,52/12,5	0,65/12,5	0,438/10.0
m8a.large	0,937/12,5	1.172/12,5	0,774/10.0
m8a.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
m8a.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
m8a.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
m8a.8xlarge	15.0	18.75	12,5
m8a.12xlarge	22.5	28.125	18.75
m8a.16xlarge	30.0	37,5	25.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
m8a.24xlarge	40.0	50.0	32.5
m8a.48xlarge	75.0	93,75	60.0
m8a.metal-24xl	40.0	50.0	32.5
m8a.logam-48xl	75.0	93,75	60.0
m8g.sedang	0,52/12,5	0,65/12,5	0,441/10.0
m8g.large	0,937/12,5	1.171/12,5	0,779/10.0
m8g.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
m8g.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
m8g.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
m8g.8xlarge	15.0	18.75	12,5
m8g.12xlarge	22.5	28.125	18.75
m8g.16xlarge	30.0	37,5	25.0
m8g.24xlarge	40.0	50.0	32.5
m8g.48xlarge	50.0	62.5	40.0
m8g.logam-24xl	40.0	50.0	32.5
m8g.logam-48xl	50.0	62.5	40.0
m8gd.sedang	0,52/12,5	0,65/12,5	0,441/10.0
m8gd.large	0,937/12,5	1.171/12,5	0,779/10.0
m8gd.xlarge	1.875/12,5	2.344/12,5	1,562/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
m8gd.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
m8gd.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
m8gd.8xlarge	15.0	18.75	12,5
m8gd.12xlarge	22.5	28.125	18.75
m8gd.16xlarge	30.0	37,5	25.0
m8gd.24xlarge	40.0	50.0	32.5
m8gd.48xlarge	50.0	62.5	40.0
m8gd.metal-24xl	40.0	50.0	32.5
m8gd.metal-48xl	50.0	62.5	40.0
m8i.large	0,937/12,5	1.172/12,5	0,774/10.0
m8i.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
m8i.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
m8i.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
m8i.8xlarge	15.0	18.75	12,5
m8i.12xlarge	22.5	28.125	18.75
m8i.16xlarge	30.0	37,5	25.0
m8i.24xlarge	40.0	50.0	32.5
m8i.32xlarge	50.0	62.5	40.0
m8i.48xlarge	75.0	93,75	60.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
m8i.96xlarge	100.0	125.0	80.0
m8i.logam-48xl	75.0	93,75	60.0
m8i.logam-96xl	100.0	125.0	80.0
m8id.large	0,937/12,5	1.172/12,5	0,774/10.0
m8id.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
m8id.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
m8id.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
m8id.8xlarge	15.0	18.75	12,5
m8id.12xlarge	22.5	28.125	18.75
m8id.16xlarge	30.0	37,5	25.0
m8id.24xlarge	40.0	50.0	32.5
m8id.32xlarge	50.0	62.5	40.0
m8id.48xlarge	75.0	93,75	60.0
m8id.96xlarge	100.0	125.0	80.0
m8id.metal-48xl	75.0	93,75	60.0
m8id.metal-96xl	100.0	125.0	80.0
m8i-flex.large	0,468/12,5	0,585/12,5	0,389/10.0
m8i-flex.xlarge	0,937/12,5	1.172/12,5	0,779/10.0
m8i-flex.2xlarge	1,875/15,0	2.344/15.0	1,562/12,5

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
m8i-flex.4xlarge	3,75/15,0	4.688/15.0	3.125/12,5
m8i-flex.8xlarge	7,5/15,0	9.375/18.75	6.25/12,5
m8i-flex.12xlarge	11.25/22.5	14.063/28.125	9.375/18.75
m8i-flex.16xlarge	15.0/30.0	18.75/37,5	12,5/25.0
r8a.sedang	0,52/12,5	0,65/12,5	0,438/10.0
r8a.large	0,937/12,5	1.172/12,5	0,774/10.0
r8a.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
r8a.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
r8a.4xlarge	7,5/15,0	9,375/15.0	6.25/12,5
r8a.8xlarge	15.0	18.75	12,5
r8a.12xlarge	22.5	28.125	18.75
r8a.16xlarge	30.0	37,5	25.0
r8a.24xlarge	40.0	50.0	32.5
r8a.48xlarge	75.0	93,75	60.0
r8a.metal-24xl	40.0	50.0	32.5
r8a.metal-48xl	75.0	93,75	60.0
r8g.sedang	0,52/12,5	0,65/12,5	0,441/10.0
r8g.besar	0,937/12,5	1.171/12,5	0,779/10.0
r8g.xlarge	1.875/12,5	2.344/12,5	1,562/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
r8g.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
r8g.4xlarge	7,5/15,0	9,375/15.0	6.25/12,5
r8g.8xlarge	15.0	18.75	12,5
r8g.12xlarge	22.5	28.125	18.75
r8g.16xlarge	30.0	37,5	25.0
r8g.24xlarge	40.0	50.0	32.5
r8g.48xlarge	50.0	62.5	40.0
r8g.logam-24xl	40.0	50.0	32.5
r8g.logam-48xl	50.0	62.5	40.0
r8gd.sedang	0,52/12,5	0,65/12,5	0,441/10.0
r8gd.large	0,937/12,5	1.171/12,5	0,779/10.0
r8gd.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
r8gd.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
r8gd.4xlarge	7,5/15,0	9,375/15.0	6.25/12,5
r8gd.8xlarge	15.0	18.75	12,5
r8gd.12xlarge	22.5	28.125	18.75
r8gd.16xlarge	30.0	37,5	25.0
r8gd.24xlarge	40.0	50.0	32.5
r8gd.48xlarge	50.0	62.5	40.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
r8gd.metal-24xl	40.0	50.0	32.5
r8gd.metal-48xl	50.0	62.5	40.0
r8i.besar	0,937/12,5	1.172/12,5	0,774/10.0
r8i.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
r8i.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
r8i.4xlarge	7,5/15,0	9,375/15.0	6.25/12,5
r8i.8xlarge	15.0	18.75	12,5
r8i.12xlarge	22.5	28.125	18.75
r8i.16xlarge	30.0	37,5	25.0
r8i.24xlarge	40.0	50.0	32.5
r8i.32xlarge	50.0	62.5	40.0
r8i.48xlarge	75.0	93,75	60.0
r8i.96xlarge	100.0	125.0	80.0
r8i.logam-48xl	75.0	93,75	60.0
r8i.logam-96xl	100.0	125.0	80.0
r8id.large	0,937/12,5	1.172/12,5	0,774/10.0
r8id.xlarge	1.875/12,5	2.344/12,5	1,562/10.0
r8id.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
r8id.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
r8id.8xlarge	15.0	18.75	12,5
r8id.12xlarge	22.5	28.125	18.75
r8id.16xlarge	30.0	37,5	25.0
r8id.24xlarge	40.0	50.0	32.5
r8id.32xlarge	50.0	62.5	40.0
r8id.48xlarge	75.0	93,75	60.0
r8id.96xlarge	100.0	125.0	80.0
r8id.metal-48xl	75.0	93,75	60.0
r8id.metal-96xl	100.0	125.0	80.0
r8i-flex.large	0,468/12,5	0,585/12,5	0,389/10.0
r8i-flex.xlarge	0,937/12,5	1.172/12,5	0,779/10.0
r8i-flex.2xlarge	1,875/15,0	2.344/15.0	1,562/12,5
r8i-flex.4xlarge	3,75/15,0	4.688/15.0	3.125/12,5
r8i-flex.8xlarge	7,5/15,0	9.375/18.75	6.25/12,5
r8i-flex.12xlarge	11.25/22.5	14.063/28.125	9.375/18.75
r8i-flex.16xlarge	15.0/30.0	18.75/37,5	12,5/25.0
x8g.sedang	0,52/12,5	0,65/12,5	0,441/10.0
x8g.large	0,937/12,5	1.171/12,5	0,779/10.0
x8g.xlarge	1.875/12,5	2.344/12,5	1,562/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
x8g.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
x8g.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
x8g.8xlarge	15.0	18.75	12,5
x8g.12xlarge	22.5	28.125	18.75
x8g.16xlarge	30.0	37,5	25.0
x8g.24xlarge	40.0	50.0	32.5
x8g.48xlarge	50.0	62.5	40.0
x8g.logam-24xl	40.0	50.0	32.5
x8g.logam-48xl	50.0	62.5	40.0
x8aedz.large	1,562/18.75	1.953/18.75	1.249/15.0
x8aedz.xlarge	3.125/18.75	3.907/18.75	2.5/15.0
x8aedz.3xlarge	9.375/18.75	11.719/18.75	7,5/15,0
x8aedz.6xlarge	18.75	23.438	15.0
x8aedz.12xlarge	37,5	46.875	30.0
x8aedz.24xlarge	75.0	93,75	60.0
x8aedz.metal-12xl	37,5	46.875	30.0
x8aedz.metal-24xl	75.0	93,75	60.0
x8i.large	0,937/12,5	1.172/12,5	0,774/10.0
x8i.xlarge	1.875/12,5	2.344/12,5	1,562/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
x8i.2xlarge	3,75/15,0	4.688/15.0	3.125/12,5
x8i.4xlarge	7,5/15,0	9,375/15,0	6.25/12,5
x8i.8xlarge	15.0	18.75	12,5
x8i.12xlarge	22.5	28.125	18.75
x8i.16xlarge	30.0	37,5	25.0
x8i.24xlarge	40.0	50.0	32.5
x8i.32xlarge	50.0	62.5	40.0
x8i.48xlarge	75.0	93,75	60.0
x8i.64xlarge	80.0	100.0	62.5
x8i.96xlarge	100.0	125.0	80.0
x8i.logam-48xl	75.0	93,75	60.0
x8i.logam-96xl	100.0	125.0	80.0

Performa Amazon EBS

Tabel berikut menunjukkan kinerja Amazon EBS, dalam Gbps, yang dapat dicapai dengan`default`,`vpc-1`, dan `ebs-1` konfigurasi.

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8a.sedang	0,325/10.0	0,195/6.25	0,407/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8a.large	0,65/10.0	0,415/6.25	0,813/10.0
c8a.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
c8a.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
c8a.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8a.8xlarge	10.0	6.25	12,5
c8a.12xlarge	15.0	9.375	18.75
c8a.16xlarge	20.0	12,5	25.0
c8a.24xlarge	30.0	20.0	37,5
c8a.48xlarge	60.0	41,25	75.0
c8a.metal-24xl	30.0	20.0	37,5
c8a.metal-48xl	60.0	41,25	75.0
c8g.sedang	0,315/10.0	0,185/6.25	0,394/10.0
c8g.large	0,63/10.0	0,396/6.25	0,788/10.0
c8g.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
c8g.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
c8g.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8g.8xlarge	10.0	6.25	12,5
c8g.12xlarge	15.0	9.375	18.75
c8g.16xlarge	20.0	12,5	25.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8g.24xlarge	30.0	20.0	37,5
c8g.48xlarge	40.0	27.5	50.0
c8g.logam-24xl	30.0	20.0	37,5
c8g.logam-48xl	40.0	27.5	50.0
c8gd.sedang	0,315/10.0	0,185/6.25	0,394/10.0
c8gd.large	0,63/10.0	0,396/6.25	0,788/10.0
c8gd.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
c8gd.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
c8gd.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8gd.8xlarge	10.0	6.25	12,5
c8gd.12xlarge	15.0	9.375	18.75
c8gd.16xlarge	20.0	12,5	25.0
c8gd.24xlarge	30.0	20.0	37,5
c8gd.48xlarge	40.0	27.5	50.0
c8gd.metal-24xl	30.0	20.0	37,5
c8gd.metal-48xl	40.0	27.5	50.0
c8i.large	0,65/10.0	0,415/6.25	0,813/10.0
c8i.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
c8i.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8i.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8i.8xlarge	10.0	6.25	12,5
c8i.12xlarge	15.0	9.375	18.75
c8i.16xlarge	20.0	12,5	25.0
c8i.24xlarge	30.0	20.0	37,5
c8i.32xlarge	40.0	27.5	50.0
c8i.48xlarge	60.0	41,25	75.0
c8i.96xlarge	80.0	55,0	100.0
c8i.logam-48xl	60.0	41,25	75.0
c8i.logam-96xl	80.0	55,0	100.0
c8id.large	0,65/10.0	0,415/6.25	0,813/10.0
c8id.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
c8id.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
c8id.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8id.8xlarge	10.0	6.25	12,5
c8id.12xlarge	15.0	9.375	18.75
c8id.16xlarge	20.0	12,5	25.0
c8id.24xlarge	30.0	20.0	37,5
c8id.32xlarge	40.0	27.5	50.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
c8id.48xlarge	60.0	41,25	75.0
c8id.96xlarge	80.0	55,0	100.0
c8id.metal-48xl	60.0	41,25	75.0
c8id.metal-96xl	80.0	55,0	100.0
c8i-flex.large	0,315/10.0	0,198/6.25	0,394/10.0
c8i-flex.xlarge	0,63/10.0	0,395/6.25	0,788/10.0
c8i-flex.2xlarge	1.25/10.0	0,781/6.25	1,563/10.0
c8i-flex.4xlarge	2.5/10.0	1,562/6.25	3.125/10.0
c8i-flex.8xlarge	5.0/10.0	3.125/6.25	6.25/12,5
c8i-flex.12xlarge	7,5/15,0	4.687/9.375	9.375/18.75
c8i-flex.16xlarge	10.0/20.0	6.25/12,5	12,5/25.0
m8a.sedang	0,325/10.0	0,195/6.25	0,407/10.0
m8a.large	0,65/10.0	0,415/6.25	0,813/10.0
m8a.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
m8a.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
m8a.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8a.8xlarge	10.0	6.25	12,5
m8a.12xlarge	15.0	9.375	18.75
m8a.16xlarge	20.0	12,5	25.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
m8a.24xlarge	30.0	20.0	37,5
m8a.48xlarge	60.0	41,25	75.0
m8a.metal-24xl	30.0	20.0	37,5
m8a.logam-48xl	60.0	41,25	75.0
m8g.sedang	0,315/10.0	0,185/6.25	0,394/10.0
m8g.large	0,63/10.0	0,396/6.25	0,788/10.0
m8g.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
m8g.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
m8g.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8g.8xlarge	10.0	6.25	12,5
m8g.12xlarge	15.0	9.375	18.75
m8g.16xlarge	20.0	12,5	25.0
m8g.24xlarge	30.0	20.0	37,5
m8g.48xlarge	40.0	27.5	50.0
m8g.logam-24xl	30.0	20.0	37,5
m8g.logam-48xl	40.0	27.5	50.0
m8gd.sedang	0,315/10.0	0,185/6.25	0,394/10.0
m8gd.large	0,63/10.0	0,396/6.25	0,788/10.0
m8gd.xlarge	1.25/10.0	0,781/6.25	1,563/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
m8gd.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
m8gd.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8gd.8xlarge	10.0	6.25	12,5
m8gd.12xlarge	15.0	9.375	18.75
m8gd.16xlarge	20.0	12,5	25.0
m8gd.24xlarge	30.0	20.0	37,5
m8gd.48xlarge	40.0	27.5	50.0
m8gd.metal-24xl	30.0	20.0	37,5
m8gd.metal-48xl	40.0	27.5	50.0
m8i.large	0,65/10.0	0,415/6.25	0,813/10.0
m8i.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
m8i.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
m8i.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8i.8xlarge	10.0	6.25	12,5
m8i.12xlarge	15.0	9.375	18.75
m8i.16xlarge	20.0	12,5	25.0
m8i.24xlarge	30.0	20.0	37,5
m8i.32xlarge	40.0	27.5	50.0
m8i.48xlarge	60.0	41,25	75.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
m8i.96xlarge	80.0	55,0	100.0
m8i.logam-48xl	60.0	41,25	75.0
m8i.logam-96xl	80.0	55,0	100.0
m8id.large	0,65/10.0	0,415/6.25	0,813/10.0
m8id.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
m8id.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
m8id.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8id.8xlarge	10.0	6.25	12,5
m8id.12xlarge	15.0	9.375	18.75
m8id.16xlarge	20.0	12,5	25.0
m8id.24xlarge	30.0	20.0	37,5
m8id.32xlarge	40.0	27.5	50.0
m8id.48xlarge	60.0	41,25	75.0
m8id.96xlarge	80.0	55,0	100.0
m8id.metal-48xl	60.0	41,25	75.0
m8id.metal-96xl	80.0	55,0	100.0
m8i-flex.large	0,315/10.0	0,198/6.25	0,394/10.0
m8i-flex.xlarge	0,63/10.0	0,395/6.25	0,788/10.0
m8i-flex.2xlarge	1.25/10.0	0,781/6.25	1,563/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
m8i-flex.4xlarge	2.5/10.0	1,562/6.25	3.125/10.0
m8i-flex.8xlarge	5.0/10.0	3.125/6.25	6.25/12,5
m8i-flex.12xlarge	7,5/15,0	4.687/9.375	9.375/18.75
m8i-flex.16xlarge	10.0/20.0	6.25/12,5	12,5/25.0
r8a.sedang	0,325/10.0	0,195/6.25	0,407/10.0
r8a.large	0,65/10.0	0,415/6.25	0,813/10.0
r8a.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
r8a.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
r8a.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8a.8xlarge	10.0	6.25	12,5
r8a.12xlarge	15.0	9.375	18.75
r8a.16xlarge	20.0	12,5	25.0
r8a.24xlarge	30.0	20.0	37,5
r8a.48xlarge	60.0	41,25	75.0
r8a.metal-24xl	30.0	20.0	37,5
r8a.metal-48xl	60.0	41,25	75.0
r8g.sedang	0,315/10.0	0,185/6.25	0,394/10.0
r8g.besar	0,63/10.0	0,396/6.25	0,788/10.0
r8g.xlarge	1.25/10.0	0,781/6.25	1,563/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
r8g.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
r8g.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8g.8xlarge	10.0	6.25	12,5
r8g.12xlarge	15.0	9.375	18.75
r8g.16xlarge	20.0	12,5	25.0
r8g.24xlarge	30.0	20.0	37,5
r8g.48xlarge	40.0	27.5	50.0
r8g.logam-24xl	30.0	20.0	37,5
r8g.logam-48xl	40.0	27.5	50.0
r8gd.sedang	0,315/10.0	0,185/6.25	0,394/10.0
r8gd.large	0,63/10.0	0,396/6.25	0,788/10.0
r8gd.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
r8gd.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
r8gd.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8gd.8xlarge	10.0	6.25	12,5
r8gd.12xlarge	15.0	9.375	18.75
r8gd.16xlarge	20.0	12,5	25.0
r8gd.24xlarge	30.0	20.0	37,5
r8gd.48xlarge	40.0	27.5	50.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
r8gd.metal-24xl	30.0	20.0	37,5
r8gd.metal-48xl	40.0	27.5	50.0
r8i.besar	0,65/10.0	0,415/6.25	0,813/10.0
r8i.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
r8i.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
r8i.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8i.8xlarge	10.0	6.25	12,5
r8i.12xlarge	15.0	9.375	18.75
r8i.16xlarge	20.0	12,5	25.0
r8i.24xlarge	30.0	20.0	37,5
r8i.32xlarge	40.0	27.5	50.0
r8i.48xlarge	60.0	41,25	75.0
r8i.96xlarge	80.0	55,0	100.0
r8i.logam-48xl	60.0	41,25	75.0
r8i.logam-96xl	80.0	55,0	100.0
r8id.large	0,65/10.0	0,415/6.25	0,813/10.0
r8id.xlarge	1.25/10.0	0,781/6.25	1,563/10.0
r8id.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
r8id.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
r8id.8xlarge	10.0	6.25	12,5
r8id.12xlarge	15.0	9.375	18.75
r8id.16xlarge	20.0	12,5	25.0
r8id.24xlarge	30.0	20.0	37,5
r8id.32xlarge	40.0	27.5	50.0
r8id.48xlarge	60.0	41,25	75.0
r8id.96xlarge	80.0	55,0	100.0
r8id.metal-48xl	60.0	41,25	75.0
r8id.metal-96xl	80.0	55,0	100.0
r8i-flex.large	0,315/10.0	0,198/6.25	0,394/10.0
r8i-flex.xlarge	0,63/10.0	0,395/6.25	0,788/10.0
r8i-flex.2xlarge	1.25/10.0	0,781/6.25	1,563/10.0
r8i-flex.4xlarge	2.5/10.0	1,562/6.25	3.125/10.0
r8i-flex.8xlarge	5.0/10.0	3.125/6.25	6.25/12,5
r8i-flex.12xlarge	7,5/15,0	4.687/9.375	9.375/18.75
r8i-flex.16xlarge	10.0/20.0	6.25/12,5	12,5/25.0
x8g.sedang	0,315/10.0	0,185/6.25	0,394/10.0
x8g.large	0,63/10.0	0,396/6.25	0,788/10.0
x8g.xlarge	1.25/10.0	0,781/6.25	1,563/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
x8g.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
x8g.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
x8g.8xlarge	10.0	6.25	12,5
x8g.12xlarge	15.0	9.375	18.75
x8g.16xlarge	20.0	12,5	25.0
x8g.24xlarge	30.0	20.0	37,5
x8g.48xlarge	40.0	27.5	50.0
x8g.logam-24xl	30.0	20.0	37,5
x8g.logam-48xl	40.0	27.5	50.0
x8aedz.large	1,25/15,0	0.859/10.312	1,563/15,0
x8aedz.xlarge	2.5/15.0	1.718/10.312	3.125/15.0
x8aedz.3xlarge	7,5/15,0	5.156/10.312	9,375/15.0
x8aedz.6xlarge	15.0	10.312	18.75
x8aedz.12xlarge	30.0	20.625	37,5
x8aedz.24xlarge	60.0	41,25	75.0
x8aedz.metal-12xl	30.0	20.625	37,5
x8aedz.metal-24xl	60.0	41,25	75.0
x8i.large	0,65/10.0	0,415/6.25	0,813/10.0
x8i.xlarge	1.25/10.0	0,781/6.25	1,563/10.0

Tipe instans	**default** (Garis dasar/Burst)	**vpc-1** (Garis dasar/Burst)	**ebs-1** (Garis dasar/Burst)
x8i.2xlarge	2.5/10.0	1,562/6.25	3.125/10.0
x8i.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
x8i.8xlarge	10.0	6.25	12,5
x8i.12xlarge	15.0	9.375	18.75
x8i.16xlarge	20.0	12,5	25.0
x8i.24xlarge	30.0	20.0	37,5
x8i.32xlarge	40.0	27.5	50.0
x8i.48xlarge	60.0	41,25	75.0
x8i.64xlarge	70.0	50.0	87.5
x8i.96xlarge	80.0	55,0	100.0
x8i.logam-48xl	60.0	41,25	75.0
x8i.logam-96xl	80.0	55,0	100.0

Memantau bandwidth instans

Anda dapat menggunakan CloudWatch metrik untuk memantau bandwidth jaringan instance dan paket yang dikirim dan diterima. Anda dapat menggunakan metrik kinerja jaringan yang disediakan oleh driver Elastic Network Adapter (ENA) untuk memantau kapan lalu lintas melebihi tunjangan jaringan yang EC2 ditentukan Amazon pada tingkat instans.

Anda dapat mengonfigurasi apakah Amazon EC2 mengirimkan data metrik untuk instans CloudWatch menggunakan periode satu menit atau periode lima menit. Ada kemungkinan bahwa metrik kinerja jaringan akan menunjukkan bahwa tunjangan terlampaui dan paket dijatuhkan sementara metrik CloudWatch instance tidak. Ini dapat terjadi ketika instance memiliki lonjakan

pendek dalam permintaan sumber daya jaringan (dikenal sebagai microburst), tetapi CloudWatch metriknya tidak cukup terperinci untuk mencerminkan lonjakan mikrodetik ini.

Pelajari selengkapnya

- Metrik instans
- Pantau kinerja jaringan

Jaringan yang disempurnakan di EC2 instans Amazon

Jaringan yang disempurnakan menggunakan I/O virtualisasi root tunggal (SR-IOV) untuk memberikan kemampuan jaringan berkinerja tinggi pada jenis instans yang didukung. SR-IOV adalah metode virtualisasi perangkat yang memberikan I/O kinerja yang lebih tinggi dan pemanfaatan CPU yang lebih rendah jika dibandingkan dengan antarmuka jaringan virtual tradisional. Jaringan yang disempurnakan memberikan bandwidth yang lebih tinggi, kinerja paket per detik (PPS) yang lebih tinggi, dan latensi yang lebih rendah secara konsisten antar instance. Tidak ada biaya tambahan karena menggunakan jaringan yang ditingkatkan.

Untuk informasi tentang kecepatan jaringan yang didukung untuk setiap jenis instans, lihat Jenis EC2 Instans Amazon.

Anda dapat mengaktifkan jaringan yang ditingkatkan menggunakan salah satu dari mekanisme berikut:

Adaptor Jaringan Elastis (ENA)

Adaptor Jaringan Elastis (ENA) mendukung kecepatan jaringan hingga 100 Gbps untuk tipe instans yang didukung.

Semua instans berbasis NITRO menggunakan ENA untuk meningkatkan jaringan. Selain itu, instance berbasis Xen berikut menggunakan ENA: H1, I3, G3,, P2, P3, P3dn`m4.16xlarge`, dan R4.

Untuk informasi selengkapnya, lihat Aktifkan jaringan yang disempurnakan dengan ENA pada instans EC2 Anda.

Antarmuka Virtual Function (VF) Intel 82599

Antarmuka Virtual Function Intel 82599 mendukung kecepatan jaringan hingga 10 Gbps untuk tipe instans yang didukung.

Tipe instans berikut menggunakan antarmuka Intel 82599 VF untuk jaringan yang ditingkatkan: C3, C4, D2, I2, M4 (tidak termasuk m4.16xlarge), dan R3.

Untuk informasi selengkapnya, lihat Jaringan yang disempurnakan dengan antarmuka Intel 82599 VF.

Konten

- Aktifkan jaringan yang disempurnakan dengan ENA pada instans EC2 Anda
- Tingkatkan kinerja jaringan antar instans EC2 dengan ENA Express
- Jaringan yang disempurnakan dengan antarmuka Intel 82599 VF
- Pantau kinerja jaringan untuk pengaturan ENA pada instans EC2 Anda
- Meningkatkan latensi jaringan untuk instance berbasis EC2 Linux
- Pertimbangan sistem nitro untuk penyetelan kinerja
- Optimalkan kinerja jaringan pada instance EC2 Windows

Aktifkan jaringan yang disempurnakan dengan ENA pada instans EC2 Anda

Amazon EC2 memberikan kemampuan jaringan yang ditingkatkan melalui Adaptor Jaringan Elastis (ENA). Untuk menggunakan jaringan yang disempurnakan, Anda harus menggunakan AMI yang menyertakan driver ENA yang diperlukan atau menginstalnya secara manual. Kemudian Anda dapat mengaktifkan dukungan ENA pada instans Anda.

Untuk meninjau catatan rilis atau petunjuk penginstalan driver ENA, lihat tab yang cocok dengan platform sistem operasi instans Anda.

Linux

Anda dapat meninjau dokumentasi berikut di GitHub:

- Tinjau catatan rilis driver kernel ENA Linux pada GitHub.
- Untuk ikhtisar driver kernel ENA Linux yang menyertakan petunjuk penginstalan, lihat Driver kernel Linux untuk keluarga Elastic Network Adapter (ENA) GitHub.

Windows

Anda dapat meninjau dokumentasi berikut dari bagian Kelola driver perangkat pada panduan ini:

- Lacak rilis versi driver ENA Windows.
- Instal driver ENA pada instans EC2 Windows.

Untuk instance berbasis Nitro, kemampuan jaringan yang ditingkatkan bervariasi menurut versi Nitro yang diimplementasikan oleh tipe instans.

Untuk meninjau spesifikasi jaringan untuk instans Anda, pilih tautan keluarga instance untuk jenis instans Anda. Jika Anda tidak yakin keluarga instans mana yang berlaku, lihat Konvensi penamaan di panduan Jenis Instans Amazon EC2.

- Spesifikasi jaringan untuk instans komputasi yang dipercepat
- Spesifikasi jaringan untuk menghitung instans yang dioptimalkan
- Spesifikasi jaringan untuk contoh tujuan umum
- Spesifikasi jaringan untuk instans komputasi berkinerja tinggi
- Spesifikasi jaringan untuk instance yang dioptimalkan memori
- Spesifikasi jaringan untuk instans penyimpanan yang dioptimalkan

Daftar Isi

- Prasyarat untuk meningkatkan jaringan dengan ENA
- Menguji apakah jaringan yang ditingkatkan diaktifkan
- Mengaktifkan jaringan yang ditingkatkan pada instans Anda
- Antrian ENA
- Memecahkan masalah driver kernel ENA di Linux
- Memecahkan masalah driver Windows Adaptor Jaringan Elastis

Prasyarat untuk meningkatkan jaringan dengan ENA

Untuk mempersiapkan jaringan yang ditingkatkan menggunakan ENA, siapkan instans Anda sebagai berikut:

- Luncurkan instance berbasis Nitro.
- Pastikan instans tersebut memiliki konektivitas internet.
- Jika memiliki data penting pada instans yang ingin Anda pertahankan, Anda harus melakukan back up data tersebut sekarang dengan membuat AMI dari instans Anda. Memperbarui driver kernel

ENA dan mengaktifkan `enaSupport` atribut mungkin membuat instance atau sistem operasi yang tidak kompatibel tidak dapat dijangkau. Jika Anda memiliki back up terbaru, data Anda akan tetap disimpan jika hal ini terjadi.

- Instans Linux — Luncurkan instance menggunakan versi kernel Linux yang didukung dan distribusi yang didukung, sehingga jaringan yang ditingkatkan ENA diaktifkan untuk instans Anda secara otomatis. Untuk informasi selengkapnya, lihat Catatan Rilis ENA Linux Kernel Driver.
- Instans Windows - Jika instance menjalankan Windows Server 2008 R2 SP1, pastikan itu memiliki pembaruan dukungan penandatanganan kode SHA-2.
- Gunakan AWS CloudShelldari Konsol Manajemen AWS, atau instal dan konfigurasikan AWS CLIatau AWS Tools for Windows PowerShelldi komputer mana pun yang Anda pilih, sebaiknya desktop atau laptop lokal Anda. Untuk informasi selengkapnya, lihat Akses Amazon EC2 atau Panduan Pengguna AWS CloudShell. Jaringan yang ditingkatkan tidak dapat dikelola dari konsol Amazon EC2.

Menguji apakah jaringan yang ditingkatkan diaktifkan

Anda dapat menguji apakah jaringan yang disempurnakan diaktifkan dalam instans Anda atau Anda AMIs.

Atribut contoh

Periksa nilai atribut `enaSupport` instance.

AWS CLI

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].EnaSupport"
```

Jika jaringan yang ditingkatkan diaktifkan, outputnya adalah sebagai berikut.

```
[
    true
]
```

PowerShell

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.EnaSupport
```

Jika jaringan yang ditingkatkan diaktifkan, outputnya adalah sebagai berikut.

```
True
```

Atribut gambar

Periksa nilai atribut `enaSupport` gambar.

AWS CLI

Gunakan perintah describe-images.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query "Images[].EnaSupport"
```

Jika jaringan yang ditingkatkan diaktifkan, outputnya adalah sebagai berikut.

```
[
    true
]
```

PowerShell

Gunakan Get-EC2Imagecmdlet.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).EnaSupport
```

Jika jaringan yang ditingkatkan diaktifkan, outputnya adalah sebagai berikut.

```
True
```

Driver antarmuka jaringan Linux

Gunakan perintah berikut untuk memverifikasi bahwa driver `ena` kernel sedang digunakan pada antarmuka tertentu, menggantikan nama antarmuka yang ingin Anda periksa. Jika Anda menggunakan antarmuka tunggal (default), ini adalah `eth0`. Jika distribusi Linux Anda mendukung nama jaringan yang dapat diprediksi, ini bisa menjadi nama seperti`ens5`. Untuk informasi lebih lanjut, perluas bagian untuk RHEL, SUSE, dan CentOS di. Mengaktifkan jaringan yang ditingkatkan pada instans Anda

Dalam contoh berikut, driver `ena` kernel tidak dimuat, karena driver yang terdaftar adalah`vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Dalam contoh ini, driver `ena` kernel dimuat dan pada versi minimum yang direkomendasikan. Instans ini memiliki jaringan yang ditingkatkan, yang dikonfigurasi dengan benar.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Mengaktifkan jaringan yang ditingkatkan pada instans Anda

Prosedur yang Anda gunakan tergantung pada sistem operasi instance.

Amazon Linux

AMIs Untuk Amazon Linux termasuk driver kernel yang diperlukan untuk meningkatkan jaringan dengan ENA diinstal dan memiliki dukungan ENA diaktifkan. Oleh karena itu, jika Anda meluncurkan instans dengan versi HVM dari Amazon Linux pada tipe instans yang didukung, jaringan yang ditingkatkan telah diaktifkan untuk instans Anda. Untuk informasi selengkapnya, lihat Menguji apakah jaringan yang ditingkatkan diaktifkan.

Ubuntu

Ubuntu HVM terbaru AMIs termasuk driver kernel yang diperlukan untuk meningkatkan jaringan dengan ENA diinstal dan memiliki dukungan ENA diaktifkan. Oleh karena itu, jika Anda meluncurkan instans dengan AMI HVM Ubuntu terbaru pada tipe instans yang didukung, jaringan yang ditingkatkan sudah diaktifkan untuk instans Anda. Untuk informasi selengkapnya, lihat Menguji apakah jaringan yang ditingkatkan diaktifkan.

Jika Anda meluncurkan instans menggunakan AMI lama dan jaringan yang ditingkatkan belum diaktifkan, Anda dapat menginstal paket kernel `linux-aws` untuk mendapatkan driver jaringan terbaru yang ditingkatkan dan mengupdate atribut yang diperlukan.

Untuk menginstal paket kernel **`linux-aws`** (Ubuntu 16.04 atau yang lebih baru)

Ubuntu 16.04 dan 18.04 dikirimkan dengan kernel kustom Ubuntu (paket kernel `linux-aws`). Untuk menggunakan kernel yang berbeda, hubungi Dukungan.

Untuk menginstal paket kernel **`linux-aws`** (Ubuntu Trusty 14.04)

1. Connect ke instans Anda.
2. Perbarui cache paket dan paket.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Jika selama proses pembaruan Anda diminta untuk menginstal `grub`, gunakan `/dev/xvda` untuk menginstal `grub`, lalu pilih untuk mempertahankan versi `/boot/grub/menu.lst` saat ini.

3. [Instans yang didukung EBS] Dari komputer lokal Anda, hentikan instans menggunakan konsol Amazon EC2 atau salah satu perintah berikut stop-instances:AWS CLI() atau () Stop-EC2Instance.AWS Tools for Windows PowerShell

   [Instans yang didukung penyimpanan instans] Anda tidak dapat menghentikan instans untuk memodifikasi atribut. Sebagai gantinya, lanjutkan ke prosedur ini: Untuk mengaktifkan jaringan yang ditingkatkan di Ubuntu (instans yang didukung penyimpanan instans).

4. Dari komputer lokal Anda, aktifkan atribut jaringan yang ditingkatkan menggunakan salah satu dari perintah berikut ini:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-support
     ```

   - Edit-EC2InstanceAttribute(Alat untuk Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
     ```

5. (Opsional) Buat AMI dari instans, seperti yang dijelaskan di Buat AMI yang didukung Amazon EBS-Backed. AMI mewarisi atribut `enaSupport` jaringan yang ditingkatkan dari instans. Oleh karena itu, Anda dapat menggunakan AMI ini untuk meluncurkan instans lain dengan jaringan yang ditingkatkan diaktifkan secara default.
6. Dari komputer lokal Anda, mulai instance menggunakan konsol Amazon EC2 atau salah satu perintah berikut: start-instances(AWS CLI) atau Start-EC2Instance(AWS Tools for Windows PowerShell).

Untuk mengaktifkan jaringan yang ditingkatkan di Ubuntu (instans yang didukung penyimpanan instans)

Ikuti prosedur sebelumnya hingga langkah tempat Anda menghentikan instans. Buat AMI baru seperti yang dijelaskan di Buat AMI yang didukung Amazon S3, pastikan untuk mengaktifkan atribut jaringan yang ditingkatkan saat Anda mendaftarkan AMI.

- register-image (AWS CLI)

  ```
  aws ec2 register-image --ena-support ...
  ```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

RHEL, SUSE, CentOS

Yang terbaru AMIs untuk Red Hat Enterprise Linux, SUSE Linux Enterprise Server, dan CentOS termasuk driver kernel yang diperlukan untuk meningkatkan jaringan dengan ENA dan memiliki dukungan ENA diaktifkan. Oleh karena itu, jika Anda meluncurkan instans dengan AMI terbaru pada tipe instans yang didukung, jaringan yang ditingkatkan telah diaktifkan untuk instans Anda. Untuk informasi selengkapnya, lihat Menguji apakah jaringan yang ditingkatkan diaktifkan.

Prosedur berikut menyediakan langkah-langkah umum untuk mengaktifkan jaringan yang ditingkatkan pada distribusi Linux selain Amazon Linux AMI atau Ubuntu. Untuk informasi selengkapnya, seperti sintaksis terperinci untuk perintah, lokasi file, atau paket dan dukungan alat, lihat dokumentasi untuk distribusi Linux Anda.

Untuk mengaktifkan jaringan yang ditingkatkan di Linux

1. Terhubung ke instans Anda.
2. Kloning kode sumber untuk driver `ena` kernel pada instance Anda dari GitHub athttps://github.com/amzn/amzn-drivers. (SUSE Linux Enterprise Server 12 SP2 dan yang lebih baru menyertakan ENA 2.02 secara default, jadi Anda tidak diharuskan mengunduh dan mengkompilasi driver ENA. Untuk SUSE Linux Enterprise Server 12 SP2 dan yang lebih baru, Anda harus mengajukan permintaan untuk menambahkan versi driver yang Anda inginkan ke kernel stok).

   ```
   git clone https://github.com/amzn/amzn-drivers
   ```
3. Kompilasi dan instal driver `ena` kernel pada instance Anda. Langkah-langkah ini bergantung pada distribusi Linux. Untuk informasi selengkapnya tentang kompilasi driver kernel di Red Hat Enterprise Linux, lihat Bagaimana cara menginstal driver ENS terbaru untuk dukungan jaringan yang ditingkatkan pada instans Amazon EC2 yang menjalankan RHEL?
4. Jalankan sudo depmod perintah untuk memperbarui dependensi driver kernel.
5. `initramfs`Perbarui instans Anda untuk memastikan bahwa driver kernel baru dimuat pada saat boot. Misalnya, jika distribusi Anda mendukung dracut, Anda dapat menggunakan perintah berikut.

```
dracut -f -v
```

6. Tentukan apakah sistem Anda menggunakan nama antarmuka jaringan yang dapat diprediksi secara default. Sistem yang menggunakan systemd atau udev versi 197 atau lebih tinggi dapat mengganti nama perangkat Ethernet dan tidak menjamin bahwa satu antarmuka jaringan akan dinamai `eth0`. Perilaku ini dapat menyebabkan masalah saat terhubung ke instans Anda. Untuk informasi lebih lanjut dan untuk melihat opsi konfigurasi lainnya, lihat Nama Antarmuka Jaringan yang Dapat Diprediksi di situs web freedesktop.org.

   a. Anda dapat memeriksa versi systemd atau udev pada sistem berbasis RPM dengan perintah berikut.

   ```
   rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

   Dalam contoh Red Hat Enterprise Linux 7 di atas, versi systemd adalah 208, jadi nama antarmuka jaringan yang dapat diprediksi harus dinonaktifkan.

   b. Nonaktifkan nama antarmuka jaringan yang dapat diprediksi dengan menambahkan opsi `net.ifnames=0` ke baris `GRUB_CMDLINE_LINUX` di `/etc/default/grub`.

   ```
   sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
   grub
   ```

   c. Buat ulang file konfigurasi grub.

   ```
   sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. [Instans yang didukung EBS] Dari komputer lokal Anda, hentikan instans menggunakan konsol Amazon EC2 atau salah satu dari perintah berikut: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell).

   [Instans yang didukung penyimpanan instans] Anda tidak dapat menghentikan instans untuk memodifikasi atribut. Sebagai gantinya, lanjutkan ke prosedur ini: Untuk mengaktifkan jaringan yang ditingkatkan di Linux (instans yang didukung penyimpanan instans).

8. Dari komputer lokal Anda, aktifkan atribut `enaSupport` jaringan yang ditingkatkan menggunakan salah satu dari perintah berikut ini:

   - modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-support
```

- Edit-EC2InstanceAttribute(Alat untuk Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
```

9. (Opsional) Buat AMI dari instans, seperti yang dijelaskan di Buat AMI yang didukung Amazon EBS-Backed. AMI mewarisi atribut `enaSupport` jaringan yang ditingkatkan dari instans. Oleh karena itu, Anda dapat menggunakan AMI ini untuk meluncurkan instans lain dengan jaringan yang ditingkatkan diaktifkan secara default.

   Jika sistem operasi instans Anda berisi file `/etc/udev/rules.d/70-persistent-net.rules`, Anda harus menghapusnya sebelum membuat AMI. File ini berisi alamat MAC untuk adaptor Ethernet dari instans asli. Jika instans lain melakukan booting dengan file ini, sistem operasi tersebut `eth0` tidak akan dapat menemukan perangkat dan mungkin gagal, yang menyebabkan masalah booting. File ini dibuat ulang pada siklus boot berikutnya, dan setiap instans yang diluncurkan dari AMI membuat versi file mereka sendiri.
10. Dari komputer lokal Anda, mulai instance menggunakan konsol Amazon EC2 atau salah satu perintah berikut: start-instances(AWS CLI) atau Start-EC2Instance(AWS Tools for Windows PowerShell).
11. (Opsional) Hubungkan ke instans Anda dan verifikasi bahwa driver kernel diinstal.

    Jika Anda tidak dapat terhubung ke instans Anda setelah mengaktifkan jaringan yang ditingkatkan, lihat Memecahkan masalah driver kernel ENA di Linux.

Untuk mengaktifkan jaringan yang ditingkatkan di Linux (instans yang didukung penyimpanan instans)

Ikuti prosedur sebelumnya hingga langkah tempat Anda menghentikan instans. Buat AMI baru seperti yang dijelaskan di Buat AMI yang didukung Amazon S3, pastikan untuk mengaktifkan atribut jaringan yang ditingkatkan saat Anda mendaftarkan AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu dengan DKMS

Metode ini hanya untuk tujuan pengujian dan umpan balik. Metode ini tidak dimaksudkan untuk digunakan dengan penerapan produksi. Untuk penerapan produksi, lihat Ubuntu.

> **Important**
>
> Menggunakan DKMS membatalkan perjanjian dukungan untuk langganan Anda. Ini tidak boleh digunakan untuk penerapan produksi.

Untuk mengaktifkan jaringan yang ditingkatkan dengan ENA di Ubuntu (instans yang didukung EBS)

1. Ikuti langkah 1 dan 2 dalam Ubuntu.
2. Instal `build-essential` paket untuk mengkompilasi driver kernel dan `dkms` paket sehingga driver `ena` kernel Anda dibangun kembali setiap kali kernel Anda diperbarui.

   ```
   ubuntu:~$ sudo apt-get install -y build-essential dkms
   ```
3. Kloning sumber untuk driver `ena` kernel pada instance Anda dari GitHub athttps://github.com/amzn/amzn-drivers.

   ```
   ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
   ```
4. Pindahkan paket `amzn-drivers` ke direktori `/usr/src/` sehingga DKMS dapat menemukannya dan membangunnya untuk setiap pembaruan kernel. Tambahkan nomor versi (Anda dapat menemukan nomor versi saat ini di catatan rilis) dari kode sumber ke nama direktori. Misalnya, versi `1.0.0` ditunjukkan pada contoh berikut.

   ```
   ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
   ```
5. Buat file konfigurasi DKMS menggunakan nilai berikut, dengan menggantikan versi `ena`.

   Buat mengajukan.

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

Edit file dan tambahkan nilai berikut.

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Tambahkan, bangun, dan instal driver `ena` kernel pada instance Anda menggunakan DKMS.

   Tambahkan driver kernel ke DKMS.

   ```
   ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
   ```

   Bangun driver kernel menggunakan dkms perintah.

   ```
   ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
   ```

   Instal driver kernel menggunakandkms.

   ```
   ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
   ```

7. Bangun kembali `initramfs` sehingga driver kernel yang benar dimuat saat boot.

   ```
   ubuntu:~$ sudo update-initramfs -u -k all
   ```

8. Verifikasi bahwa driver `ena` kernel diinstal menggunakan perintah modinfo ena dari. Menguji apakah jaringan yang ditingkatkan diaktifkan

   ```
   ubuntu:~$ modinfo ena
   filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
   version:  1.0.0
   ```

```
license:  GPL
description: Elastic Network Adapter (ENA)
author:   Amazon.com, Inc. or its affiliates
srcversion:  9693C876C54CA64AE48F0CA
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:    3.13.0-74-generic SMP mod_unload modversions
parm:     debug:Debug level (0=none,...,16=all) (int)
parm:     push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
    0 - Automatically choose according to device capability (default)
    1 - Don't push anything to device memory
    3 - Push descriptors and header buffer to device memory (int)
parm:     enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:     enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:     numa_node_override_array:Numa node override map
(array of int)
parm:     numa_node_override:Enable/Disable numa node override (0=disable)
(int)
```

9. Lanjutkan dengan Langkah 3 di Ubuntu.

Mengaktifkan jaringan yang ditingkatkan di Windows

Jika Anda meluncurkan instans dan instans tersebut belum mengaktifkan jaringan yang ditingkatkan, Anda harus mengunduh dan menginstal driver adaptor jaringan yang diperlukan pada instans Anda, lalu menyetel atribut instans `enaSupport` untuk mengaktifkan jaringan yang ditingkatkan.

Untuk mengaktifkan jaringan yang ditingkatkan

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.
2. [Hanya Windows Server 2016 dan 2019] Jalankan PowerShell skrip EC2 Peluncuran berikut untuk mengonfigurasi instance setelah driver diinstal.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

3. Dari instans, instal driver sebagai berikut:

a. Unduh driver terbaru ke instans.

b. Ekstrak arsip zip.

c. Instal driver dengan menjalankan `install.ps1` PowerShell skrip.

> **Note**
>
> Jika Anda mendapatkan kesalahan kebijakan eksekusi, atur kebijakan ke `Unrestricted` (secara default kebijakan ini diatur ke `Restricted` atau `RemoteSigned`). Di baris perintah, jalankan`Set-ExecutionPolicy -ExecutionPolicy Unrestricted`, lalu jalankan `install.ps1` PowerShell skrip lagi.

4. Dari komputer lokal Anda, hentikan instans menggunakan konsol Amazon EC2 atau salah satu perintah berikut: stop-instances(AWS CLI) atau Stop-EC2Instance(AWS Tools for Windows PowerShell).

5. Aktifkan dukungan ENA pada instans Anda sebagai berikut:

   a. Dari komputer lokal Anda, periksa atribut dukungan ENA instans EC2 pada instans Anda dengan menjalankan salah satu perintah berikut. Jika atribut tersebut tidak diaktifkan, output akan menjadi "[]" atau kosong. `EnaSupport` diatur ke `false` secara default.

   - describe-instances (AWS CLI)

     ```
     aws ec2 describe-instances --instance-ids i-1234567890abcdef0 --query
      "Reservations[].Instances[].EnaSupport"
     ```

   - Get-EC2Instance(Alat untuk Windows PowerShell)

     ```
     (Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.EnaSupport
     ```

   b. Untuk mengaktifkan dukungan ENA, jalankan salah satu dari perintah berikut ini:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-
     support
     ```

   - Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
```

Jika Anda mengalami masalah saat memulai ulang instans, Anda juga dapat menonaktifkan dukungan ENA menggunakan salah satu dari perintah berikut:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --no-ena-support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $false
```

c. Verifikasi bahwa atribut telah diatur ke `true` menggunakan describe-instances atau Get-EC2Instance seperti yang ditunjukkan sebelumnya. Anda seharusnya sekarang melihat output berikut:

```
[
 true
]
```

6. Dari komputer lokal Anda, mulai instance menggunakan konsol Amazon EC2 atau salah satu perintah berikut: start-instances(AWS CLI) atau Start-EC2Instance(AWS Tools for Windows PowerShell).
7. Pada instans ini, validasi bahwa driver ENA diinstal dan diaktifkan sebagai berikut:
   a. Klik kanan ikon jaringan dan pilih Buka Pusat Jaringan dan Berbagi.
   b. Pilih adaptor Ethernet (misalnya, Ethernet 2).
   c. Pilih Detail. Untuk Detail Koneksi Jaringan, periksa apakah Deskripsi adalah Amazon Elastic Network Adapter.
8. (Opsional) Buat AMI dari instans. AMI mewarisi atribut `enaSupport` dari instans tersebut. Oleh karena itu, Anda dapat menggunakan AMI ini untuk meluncurkan instans lain dengan ENA yang diaktifkan secara default.

Antrian ENA

Antrian ENA dialokasikan ke antarmuka jaringan dengan batas statis default berdasarkan jenis dan ukuran instance. Pada jenis instans yang didukung, Anda dapat mengalokasikan antrian ini secara dinamis di seluruh Elastic Network Interfaces (). ENIs Meskipun jumlah antrian total per instance bergantung pada jenis dan ukurannya, Anda dapat mengonfigurasi beberapa ENIs dengan antrian ENA hingga Anda memenuhi jumlah antrian maksimum untuk ENI dan instance.

Alokasi antrian ENA yang fleksibel mengoptimalkan distribusi sumber daya, memungkinkan pemanfaatan vCPU maksimum. Beban kerja kinerja jaringan yang tinggi biasanya memerlukan beberapa antrian ENA. Anda dapat menyempurnakan kinerja jaringan dan paket per detik (PPS) dengan menyesuaikan jumlah antrian sesuai dengan kebutuhan beban kerja spesifik Anda. Misalnya, aplikasi intensif jaringan mungkin memerlukan lebih banyak antrian dibandingkan dengan aplikasi intensif CPU.

Topik

- Instans-instans yang didukung
- Ubah jumlah antrian

Instans-instans yang didukung

Contoh berikut mendukung alokasi dinamis beberapa antrian ENA.

Tujuan umum

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
	M6i		
`m6i.large`	2	2	6
`m6i.xlarge`	4	4	16
`m6i.2xlarge`	8	8	32
`m6i.4xlarge`	8	16	64

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
m6i.8xlarge	8	32	64
m6i.12xlarge	8	32	64
m6i.16xlarge	8	32	120
m6i.24xlarge	8	32	120
m6i.32xlarge	8	32	120
M6id			
m6id.large	2	2	6
m6id.xlarge	4	4	16
m6id.2xlarge	8	8	32
m6id.4xlarge	8	16	64
m6id.8xlarge	8	32	64
m6id.12xlarge	8	32	64
m6id.16xlarge	8	32	120
m6id.24xlarge	8	32	120
m6id.32xlarge	8	32	120
M6idn			
m6idn.large	2	2	6
m6idn.xlarge	4	4	16
m6idn.2xlarge	8	8	32

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
m6idn.4xlarge	8	16	64
m6idn.8xlarge	16	32	128
m6idn.12xlarge	16	32	128
m6idn.16xlarge	16	32	240
m6idn.24xlarge	32	32	480
m6idn.32xlarge	32	32	512 *
M6in			
m6in.large	2	2	6
m6in.xlarge	4	4	16
m6in.2xlarge	8	8	32
m6in.4xlarge	8	16	64
m6in.8xlarge	16	32	128
m6in.12xlarge	16	32	128
m6in.16xlarge	16	32	240
m6in.24xlarge	32	32	480
m6in.32xlarge	32	32	512 *
M8a			
m8a.medium	1	1	3
m8a.large	2	2	6

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
m8a.xlarge	4	4	16
m8a.2xlarge	8	8	32
m8a.4xlarge	8	16	64
m8a.8xlarge	8	32	128
m8a.12xlarge	16	64	192
m8a.16xlarge	16	64	256
m8a.24xlarge	16	128	384
m8a.48xlarge	32	128	768
m8a.metal-24xl	16	128	384
m8a.metal-48xl	32	128	768
M8azn			
m8azn.medium	1	1	3
m8azn.large	2	2	8
m8azn.xlarge	4	4	16
m8azn.3xlarge	4	16	48
m8azn.6xlarge	8	32	96
m8azn.12xlarge	8	64	192
m8azn.24xlarge	16	128	384
m8azn.metal-12xl	8	64	192

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
m8azn.metal-24xl	16	128	384
M8GB			
m8gb.medium	1	1	2
m8gb.large	2	2	6
m8gb.xlarge	4	4	16
m8gb.2xlarge	8	8	32
m8gb.4xlarge	8	16	64
m8gb.8xlarge	8	32	128
m8gb.12xlarge	16	64	192
m8gb.16xlarge	16	64	256
m8gb.24xlarge	16	128	384
m8gb.48xlarge	32	128	768 *
m8gb.metal-24xl	32	128	768
m8gb.metal-48xl	32	128	768 *
M8gn			
m8gn.medium	1	1	2
m8gn.large	2	2	6
m8gn.xlarge	4	4	16
m8gn.2xlarge	8	8	32

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
m8gn.4xlarge	8	16	64
m8gn.8xlarge	8	32	128
m8gn.12xlarge	16	64	192
m8gn.16xlarge	16	64	256
m8gn.24xlarge	16	128	384
m8gn.48xlarge	32	128	768 *
m8gn.metal-24xl	32	128	768
m8gn.metal-48xl	32	128	768 *
M8i			
m8i.large	2	2	6
m8i.xlarge	4	4	16
m8i.2xlarge	8	8	32
m8i.4xlarge	8	16	64
m8i.8xlarge	8	32	128
m8i.12xlarge	16	64	192
m8i.16xlarge	16	64	256
m8i.24xlarge	16	128	384
m8i.32xlarge	16	128	512
m8i.48xlarge	32	128	768

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
m8i.96xlarge	32	128	1536
m8i.metal-48xl	32	128	768
m8i.metal-96xl	32	128	1536
M8id			
m8id.large	2	2	6
m8id.xlarge	4	4	16
m8id.2xlarge	8	8	32
m8id.4xlarge	8	16	64
m8id.8xlarge	8	32	128
m8id.12xlarge	16	64	192
m8id.16xlarge	16	64	256
m8id.24xlarge	16	128	384
m8id.32xlarge	16	128	512
m8id.48xlarge	32	128	768
m8id.96xlarge	32	128	1536
m8id.metal-48xl	32	128	768
m8id.metal-96xl	32	128	1536
M8i-Flex			
m8i-flex.large	1	1	3

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
m8i-flex.xlarge	2	2	8
m8i-flex.2xlarge	4	4	16
m8i-flex.4xlarge	4	8	32
m8i-flex.8xlarge	4	16	64
m8i-flex.12xlarge	8	32	96
m8i-flex.16xlarge	8	32	128

> **Note**
>
> * Jenis contoh ini memiliki beberapa kartu jaringan. Jenis contoh lainnya memiliki kartu jaringan tunggal. Untuk informasi selengkapnya, lihat Kartu jaringan.

Komputasi yang dioptimalkan

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
	C6i		
c6i.large	2	2	6
c6i.xlarge	4	4	16
c6i.2xlarge	8	8	32
c6i.4xlarge	8	16	64
c6i.8xlarge	8	32	64

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
c6i.12xlarge	8	32	64
c6i.16xlarge	8	32	120
c6i.24xlarge	8	32	120
c6i.32xlarge	8	32	120
C6id			
c6id.large	2	2	6
c6id.xlarge	4	4	16
c6id.2xlarge	8	8	32
c6id.4xlarge	8	16	64
c6id.8xlarge	8	32	64
c6id.12xlarge	8	32	64
c6id.16xlarge	8	32	120
c6id.24xlarge	8	32	120
c6id.32xlarge	8	32	120
C6in			
c6in.large	2	2	6
c6in.xlarge	4	4	16
c6in.2xlarge	8	8	32
c6in.4xlarge	8	16	64

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
c6in.8xlarge	16	32	128
c6in.12xlarge	16	32	128
c6in.16xlarge	16	32	240
c6in.24xlarge	32	32	480
c6in.32xlarge	32	32	512 *
C8a			
c8a.medium	1	1	3
c8a.large	2	2	6
c8a.xlarge	4	4	16
c8a.2xlarge	8	8	32
c8a.4xlarge	8	16	64
c8a.8xlarge	8	32	128
c8a.12xlarge	16	64	192
c8a.16xlarge	16	64	256
c8a.24xlarge	16	128	384
c8a.48xlarge	32	128	768
c8a.metal-24xl	16	128	384
c8a.metal-48xl	32	128	768
C8GB			

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
c8gb.medium	1	1	2
c8gb.large	2	2	6
c8gb.xlarge	4	4	16
c8gb.2xlarge	8	8	32
c8gb.4xlarge	8	16	64
c8gb.8xlarge	8	32	128
c8gb.12xlarge	16	64	192
c8gb.16xlarge	16	64	256
c8gb.24xlarge	16	128	384
c8gb.48xlarge	32	128	768 *
c8gb.metal-24xl	32	128	768
c8gb.metal-48xl	32	128	768 *
	C8gn		
c8gn.medium	1	1	2
c8gn.large	2	2	6
c8gn.xlarge	4	4	16
c8gn.2xlarge	8	8	32
c8gn.4xlarge	8	16	64
c8gn.8xlarge	8	32	128

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
c8gn.12xlarge	16	64	192
c8gn.16xlarge	16	64	256
c8gn.24xlarge	16	128	384
c8gn.48xlarge	32	128	768 *
c8gn.metal-24xl	32	128	768
c8gn.metal-48xl	32	128	768 *
C8i			
c8i.large	2	2	6
c8i.xlarge	4	4	16
c8i.2xlarge	8	8	32
c8i.4xlarge	8	16	64
c8i.8xlarge	8	32	128
c8i.12xlarge	16	64	192
c8i.16xlarge	16	64	256
c8i.24xlarge	16	128	384
c8i.32xlarge	16	128	512
c8i.48xlarge	32	128	768
c8i.96xlarge	32	128	1536
c8i.metal-48xl	32	128	768

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
c8i.metal-96xl	32	128	1536
C8id			
c8id.large	2	2	6
c8id.xlarge	4	4	16
c8id.2xlarge	8	8	32
c8id.4xlarge	8	16	64
c8id.8xlarge	8	32	128
c8id.12xlarge	16	64	192
c8id.16xlarge	16	64	256
c8id.24xlarge	16	128	384
c8id.32xlarge	16	128	512
c8id.48xlarge	32	128	768
c8id.96xlarge	32	128	1536
c8id.metal-48xl	32	128	768
c8id.metal-96xl	32	128	1536
C8i-Flex			
c8i-flex.large	1	1	3
c8i-flex.xlarge	2	2	8
c8i-flex.2xlarge	4	4	16

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
c8i-flex.4xlarge	4	8	32
c8i-flex.8xlarge	4	16	64
c8i-flex.12xlarge	8	32	96
c8i-flex.16xlarge	8	32	128

> **Note**
>
> * Jenis contoh ini memiliki beberapa kartu jaringan. Jenis contoh lainnya memiliki kartu jaringan tunggal. Untuk informasi selengkapnya, lihat Kartu jaringan.

Memori yang dioptimalkan

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
	R6i		
r6i.large	2	2	6
r6i.xlarge	4	4	16
r6i.2xlarge	8	8	32
r6i.4xlarge	8	16	64
r6i.8xlarge	8	32	64
r6i.12xlarge	8	32	64
r6i.16xlarge	8	32	120

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
r6i.24xlarge	8	32	120
r6i.32xlarge	8	32	120
R6id			
r6id.large	2	2	6
r6id.xlarge	4	4	16
r6id.2xlarge	8	8	32
r6id.4xlarge	8	16	64
r6id.8xlarge	8	32	64
r6id.12xlarge	8	32	64
r6id.16xlarge	8	32	120
r6id.24xlarge	8	32	120
r6id.32xlarge	8	32	120
R6idn			
r6idn.large	2	2	6
r6idn.xlarge	4	4	16
r6idn.2xlarge	8	8	32
r6idn.4xlarge	8	16	64
r6idn.8xlarge	16	32	128
r6idn.12xlarge	16	32	128

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
r6idn.16xlarge	16	32	240
r6idn.24xlarge	32	32	480
r6idn.32xlarge	32	32	512 *
R6in			
r6in.large	2	2	6
r6in.xlarge	4	4	16
r6in.2xlarge	8	8	32
r6in.4xlarge	8	16	64
r6in.8xlarge	16	32	128
r6in.12xlarge	16	32	128
r6in.16xlarge	16	32	240
r6in.24xlarge	32	32	480
r6in.32xlarge	32	32	512 *
R8a			
r8a.medium	1	1	3
r8a.large	2	2	6
r8a.xlarge	4	4	16
r8a.2xlarge	8	8	32
r8a.4xlarge	8	16	64

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
r8a.8xlarge	8	32	128
r8a.12xlarge	16	64	192
r8a.16xlarge	16	64	256
r8a.24xlarge	16	128	384
r8a.48xlarge	32	128	768
r8a.metal-24xl	16	128	384
r8a.metal-48xl	32	128	768
R8GB			
r8gb.medium	1	1	2
r8gb.large	2	2	6
r8gb.xlarge	4	4	16
r8gb.2xlarge	8	8	32
r8gb.4xlarge	8	16	64
r8gb.8xlarge	8	32	128
r8gb.12xlarge	16	64	192
r8gb.16xlarge	16	64	256
r8gb.24xlarge	16	128	384
r8gb.48xlarge	32	128	768 *
r8gb.metal-24xl	32	128	768

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
r8gb.metal-48xl	32	128	768 *
R8gn			
r8gn.medium	1	1	2
r8gn.large	2	2	6
r8gn.xlarge	4	4	16
r8gn.2xlarge	8	8	32
r8gn.4xlarge	8	16	64
r8gn.8xlarge	8	32	128
r8gn.12xlarge	16	64	192
r8gn.16xlarge	16	64	256
r8gn.24xlarge	16	128	384
r8gn.48xlarge	32	128	768 *
r8gn.metal-24xl	32	128	768
r8gn.metal-48xl	32	128	768 *
R8i			
r8i.large	2	2	6
r8i.xlarge	4	4	16
r8i.2xlarge	8	8	32
r8i.4xlarge	8	16	64

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
r8i.8xlarge	8	32	128
r8i.12xlarge	16	64	192
r8i.16xlarge	16	64	256
r8i.24xlarge	16	128	384
r8i.32xlarge	16	128	512
r8i.48xlarge	32	128	768
r8i.96xlarge	32	128	1536
r8i.metal-48xl	32	128	768
r8i.metal-96xl	32	128	1536
R8id			
r8id.large	2	2	6
r8id.xlarge	4	4	16
r8id.2xlarge	8	8	32
r8id.4xlarge	8	16	64
r8id.8xlarge	8	32	128
r8id.12xlarge	16	64	192
r8id.16xlarge	16	64	256
r8id.24xlarge	16	128	384
r8id.32xlarge	16	128	512

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
r8id.48xlarge	32	128	768
r8id.96xlarge	32	128	1536
r8id.metal-48xl	32	128	768
r8id.metal-96xl	32	128	1536
R8i-Flex			
r8i-flex.large	1	1	3
r8i-flex.xlarge	2	2	8
r8i-flex.2xlarge	4	4	16
r8i-flex.4xlarge	4	8	32
r8i-flex.8xlarge	4	16	64
r8i-flex.12xlarge	8	32	96
r8i-flex.16xlarge	8	32	128
X8AEDZ			
x8aedz.large	2	2	8
x8aedz.xlarge	4	4	16
x8aedz.3xlarge	4	16	48
x8aedz.6xlarge	8	32	96
x8aedz.12xlarge	8	64	192
x8aedz.24xlarge	16	128	384

Tipe instans	Antrian ENA default per antarmuka	Antrian ENA maksimum per antarmuka	Antrian ENA maksimum per instance
x8aedz.metal-12xl	8	64	192
x8aedz.metal-24xl	16	128	384
	X8i		
x8i.large	2	2	6
x8i.xlarge	4	4	16
x8i.2xlarge	8	8	32
x8i.4xlarge	8	16	64
x8i.8xlarge	8	32	128
x8i.12xlarge	16	64	192
x8i.16xlarge	16	64	256
x8i.24xlarge	16	128	384
x8i.32xlarge	16	128	512
x8i.48xlarge	32	128	768
x8i.64xlarge	32	128	1024
x8i.96xlarge	32	128	1536
x8i.metal-48xl	32	128	768
x8i.metal-96xl	32	128	1536

> **Note**
>
> * Jenis contoh ini memiliki beberapa kartu jaringan. Jenis contoh lainnya memiliki kartu jaringan tunggal. Untuk informasi selengkapnya, lihat Kartu jaringan.

Ubah jumlah antrian

Anda dapat mengubah jumlah antrian ENA menggunakan Konsol Manajemen AWS atau. AWS CLI Dalam Konsol Manajemen AWS, konfigurasi antrian ENA tersedia di bawah setiap pengaturan antarmuka Jaringan.

Untuk mengubah jumlah antrian ENA menggunakan AWS CLI, gunakan salah satu dari perintah berikut. Sebelum memodifikasi jumlah antrian, gunakan perintah berikut untuk memeriksa jumlah antrian Anda saat ini.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

> **Note**
>
> - Instance Anda harus dihentikan sebelum memodifikasi jumlah antrian ENA.
> - Nilai antrian ENA harus berupa kekuatan 2, seperti, 1, 2, 4, 8, 16, 32, dll.
> - Jumlah antrian yang dialokasikan ke ENI tunggal mana pun tidak dapat melebihi jumlah v yang CPUs tersedia pada instans Anda.

attach-network-interface

Dalam contoh berikut, 32 antrian ENA dikonfigurasi pada ENI.

```
aws ec2 attach-network-interface \
  --network-interface-id eni-001aa1bb223cdd4e4 \
  --instance-id i-1234567890abcdef0 \
  --device-index 1 \
  --ena-queue-count 32
```

run-instances

Dalam contoh berikut, 2 antrian ENA masing-masing dikonfigurasi pada 3. ENIs

```
aws ec2 run-instances \
  --image-id ami-12ab3c30 \
  --instance-type c6i.large \
  --min-count 1 \
  --max-count 1 \
  --network-interfaces \
    "[{\"DeviceIndex\":0,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2},
      {\"DeviceIndex\":1,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2},
      {\"DeviceIndex\":2,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2}]"
```

modify-network-interface-attribute

Dalam contoh berikut, 32 antrian ENA dikonfigurasi pada ENI.

```
aws ec2 modify-network-interface-attribute \
--network-interface-id eni-1234567890abcdef0 \
--attachment AttachmentId=eni-attach-12345678,EnaQueueCount=32
```

Dalam contoh berikut, jumlah ENA diatur ulang ke nilai default.

```
aws ec2 modify-network-interface-attribute \
--network-interface-id eni-1234567890abcdef0 \
--attachment AttachmentId=eni-attach-12345678,DefaultEnaQueueCount=true
```

Memecahkan masalah driver kernel ENA di Linux

Adaptor Jaringan Elastis (ENA) dirancang untuk meningkatkan kesehatan sistem operasi dan mengurangi kemungkinan gangguan jangka panjang karena perilaku dan atau kegagalan perangkat keras yang tidak terduga. Arsitektur ENA menjaga kegagalan perangkat atau driver setransparan mungkin ke sistem. Topik ini memberikan informasi pemecahan masalah untuk ENA.

Jika Anda tidak dapat terhubung ke instans, mulailah dengan bagian Memecahkan masalah konektivitas.

Jika Anda mengalami penurunan kinerja setelah bermigrasi ke jenis instans generasi keenam, lihat artikel Apa yang harus saya lakukan sebelum saya memigrasikan EC2 instance saya ke instance generasi keenam untuk memastikan bahwa saya mendapatkan kinerja jaringan maksimum?

Jika Anda dapat menyambungkan ke instans, Anda dapat mengumpulkan informasi diagnostik dengan menggunakan deteksi kegagalan dan mekanisme pemulihan yang dibahas di bagian selanjutnya dari topik ini.

Daftar Isi

- Memecahkan masalah konektivitas
- Mekanisme keep-alive
- Mendaftarkan waktu habis baca
- Statistik
- Log error driver di syslog
- Pemberitahuan konfigurasi sub-optimal

Memecahkan masalah konektivitas

Jika Anda kehilangan konektivitas saat mengaktifkan jaringan yang ditingkatkan, modul `ena` mungkin tidak kompatibel dengan kernel yang sedang berjalan dari instans Anda. Ini dapat terjadi jika Anda menginstal modul untuk versi kernel tertentu (tanpa dkms, atau dengan file dkms.conf yang tidak dikonfigurasi dengan benar) lalu kernel instans Anda diperbarui. Jika kernel instans yang dimuat saat boot tidak memiliki modul `ena` yang diinstal dengan benar, instans Anda tidak akan mengenali adaptor jaringan dan instans Anda tidak dapat dijangkau.

Jika Anda mengaktifkan jaringan yang ditingkatkan untuk instans PV atau AMI, ini juga dapat membuat instans Anda tidak dapat dijangkau.

Jika instans Anda tidak dapat dijangkau setelah mengaktifkan jaringan yang ditingkatkan dengan ENA, Anda dapat menonaktifkan atribut `enaSupport` untuk instans Anda dan atribut itu akan kembali ke adaptor jaringan stok.

Untuk menonaktifkan jaringan yang ditingkatkan dengan ENA (instans yang didukung EBS)

1. Dari komputer lokal Anda, hentikan instance dengan menggunakan EC2 konsol Amazon, perintah stop-instance (AWS CLI), atau Stop-EC2Instancecmdlet ().AWS Tools for PowerShell
2. Dari komputer lokal Anda, nonaktifkan atribut jaringan yang disempurnakan dengan menggunakan modify-instance-attributeperintah dengan `--no-ena-support` opsi atau Edit-EC2InstanceAttributecmdlet dengan parameter. `-EnaSupport $false`
3. Dari komputer lokal Anda, mulai instance menggunakan EC2 konsol Amazon, perintah start-instance, atau cmdlet. Start-EC2Instance

4. (Opsional) Connect ke instans Anda dan coba instal ulang modul `ena` dengan versi kernel Anda saat ini, dengan mengikuti langkah-langkah di Aktifkan jaringan yang disempurnakan dengan ENA pada instans EC2 Anda.

Untuk menonaktifkan jaringan yang ditingkatkan dengan ENA (instans yang didukung penyimpanan instans)

1. Buat AMI baru seperti yang dijelaskan dalamBuat AMI yang didukung Amazon S3.
2. Saat Anda mendaftarkan AMI, pastikan untuk menyertakan `--no-ena-support` opsi dalam perintah stop-instance (AWS CLI) atau `-EnaSupport $false` parameter di cmdlet. Register-EC2Image

Mekanisme keep-alive

Perangkat ENA memposting peristiwa keep-alive dengan kecepatan tetap (biasanya sekali setiap detik). Driver ENA mengimplementasikan mekanisme watchdog, yang memeriksa keberadaan pesan keep-alive ini. Jika ada pesan atau beberapa pesan, watchdog disiapkan kembali, jika tidak driver menyimpulkan bahwa perangkat mengalami kegagalan dan kemudian melakukan hal berikut:

- Membuang statistik saat ini ke syslog
- Mereset perangkat ENA
- Mereset status driver ENA

Prosedur reset di atas dapat mengakibatkan kehilangan beberapa lalu lintas dalam waktu singkat (koneksi TCP harus dapat dipulihkan), tetapi seharusnya tidak mempengaruhi pengguna.

Perangkat ENA juga secara tidak langsung dapat meminta prosedur reset perangkat, misalnya dengan tidak mengirimkan pemberitahuan keep-alive, jika perangkat ENA mencapai status tidak diketahui setelah memuat konfigurasi yang tidak dapat dipulihkan.

Berikut ini adalah contoh prosedur reset:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
```

```
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Mendaftarkan waktu habis baca

Arsitektur ENA menyarankan penggunaan terbatas operasi pembacaan memori yang dipetakan I/O (MMIO). Daftar MMIO diakses oleh pengandar perangkat ENA hanya selama prosedur inisialisasi.

Jika log driver (tersedia dalam output dmesg) menunjukkan kegagalan operasi baca, ini mungkin disebabkan oleh driver yang tidak kompatibel atau tidak dikompilasi dengan benar, hardware yang sibuk, atau kegagalan hardware.

Entri log terputus-putus yang menunjukkan kegagalan pada operasi baca tidak boleh dianggap sebagai masalah; dalam kasus ini driver akan mencobanya kembali. Namun, urutan entri log yang berisi kegagalan pembacaan menunjukkan masalah driver atau hardware.

Di bawah ini adalah contoh entri log driver yang menunjukkan kegagalan operasi baca karena waktu habis:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistik

Jika Anda mengalami masalah latensi atau performa jaringan yang tidak memadai, Anda harus mengambil statistik perangkat dan memeriksanya. Statistik ini dapat diperoleh dengan menggunakan ethtool, seperti berikut ini.

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
 tx_timeout: 0
 suspend: 0
 resume: 0
 wd_expired: 0
 interface_up: 1
 interface_down: 0
 admin_q_pause: 0
 bw_in_allowance_exceeded: 0
 bw_out_allowance_exceeded: 0
 pps_allowance_exceeded: 0
 conntrack_allowance_available: 450878
 conntrack_allowance_exceeded: 0
 linklocal_allowance_exceeded: 0
 queue_0_tx_cnt: 4329
 queue_0_tx_bytes: 1075749
 queue_0_tx_queue_stop: 0
 ...
```

Parameter output perintah berikut dijelaskan di bawah ini:

`tx_timeout`: *N*

Berapa kali watchdog Netdev diaktifkan.

`suspend`: *N*

Jumlah berapa kali driver melakukan operasi penangguhan.

`resume`: *N*

Jumlah berapa kali driver melakukan operasi kelanjutan.

`wd_expired`: *N*

Berapa kali driver tersebut tidak menerima peristiwa keep-alive dalam tiga detik sebelumnya.

`interface_up`: *N*

Berapa kali antarmuka ENA dinaikkan.

`interface_down`: *N*

Berapa kali antarmuka ENA diturunkan.

`admin_q_pause`: *N*

Jumlah berapa kali antrean admin tidak ditemukan dalam status berjalan.

`bw_in_allowance_exceeded`: *N*

Jumlah paket antri atau dijatuhkan karena kumpulan bandwidth yang masuk melebihi maksimum untuk instans.

`bw_out_allowance_exceeded`: *N*

Jumlah paket antri atau dijatuhkan karena kumpulan bandwidth agregat yang keluar melebihi maksimum untuk instans.

`pps_allowance_exceeded`: *N*

Jumlah paket mengantri atau turun karena PPS dua arah melebihi maksimum untuk instance. *

`conntrack_allowance_available`: *N*

Jumlah koneksi yang dilacak yang dapat dibuat oleh instans sebelum menekan tunjangan Connections Tracked dari tipe instans tersebut. Hanya tersedia untuk instans berbasis Nitro. Tidak didukung dengan FreeBSD instans atau lingkungan DPDK.

`conntrack_allowance_exceeded`: *N*

Jumlah paket turun karena pelacakan koneksi melebihi maksimum untuk instans dan koneksi baru tidak dapat dibuat. Hal ini dapat mengakibatkan hilangnya paket untuk lalu lintas ke atau dari instans.

`linklocal_allowance_exceeded`: *N*

Jumlah paket turun karena PPS lalu lintas ke layanan proksi lokal melebihi batas maksimum untuk antarmuka jaringan. Hal ini memengaruhi lalu lintas ke layanan DNS Amazon, Layanan Metadata Instans, dan Layanan Sinkronisasi Waktu Amazon, tetapi tidak memengaruhi lalu lintas ke resolver DNS khusus.

`queue_`*N*`_tx_cnt`: *N*

Jumlah paket yang dikirimkan untuk antrean ini.

`queue_`*N*`_tx_bytes`: *N*

Jumlah bita yang dikirimkan untuk antrean ini.

`queue_`*N*`_tx_queue_stop`: *N*

Berapa kali antrian *N* itu penuh dan berhenti.

`queue_`*N*`_tx_queue_wakeup`: *N*

Berapa kali antrian *N* dilanjutkan setelah dihentikan.

`queue_`*N*`_tx_dma_mapping_err`: *N*

Jumlah kesalahan akses memori langsung. Jika nilai ini bukan 0, ini menunjukkan sumber daya sistem yang rendah.

`queue_`*N*`_tx_linearize`: *N*

Jumlah berapa kali linierisasi SKB dicoba untuk antrean.

`queue_`*N*`_tx_linearize_failed`: *N*

Jumlah berapa kali linierisasi SKB gagal untuk antrean ini.

`queue_`*N*`_tx_napi_comp`: *N*

Jumlah berapa kali handler `napi` memanggil `napi_complete` untuk antrean ini.

`queue_`*N*`_tx_tx_poll`: *N*

Jumlah berapa kali handler `napi` dijadwalkan untuk antrean ini.

`queue_N_tx_doorbells`: *N*

Jumlah doorbell transmisi untuk antrean ini.

`queue_N_tx_prepare_ctx_err`: *N*

Jumlah berapa kali `ena_com_prepare_tx` gagal untuk antrean ini.

`queue_N_tx_bad_req_id`: *N*

`req_id` tidak valid untuk antrean ini. `req_id` yang valid adalah nol, dikurangi `queue_size`, dikurangi 1.

`queue_N_tx_llq_buffer_copy`: *N*

Jumlah paket yang ukuran headernya lebih besar dari entri llq untuk antrean ini.

`queue_N_tx_missed_tx`: *N*

Jumlah paket yang tidak diselesaikan untuk antrean ini.

`queue_N_tx_unmask_interrupt`: *N*

Jumlah berapa kali interupsi tx dibuka untuk antrean ini.

`queue_N_rx_cnt`: *N*

Jumlah paket yang diterima untuk antrean ini.

`queue_N_rx_bytes`: *N*

Jumlah byte yang diterima untuk antrean ini.

`queue_N_rx_rx_copybreak_pkt`: *N*

Jumlah berapa kali antrean rx menerima paket yang kurang dari ukuran paket rx_copybreak untuk antrean ini.

`queue_N_rx_csum_good`: *N*

Jumlah berapa kali antrean rx menerima paket di mana checksum diperiksa dan benar untuk antrean ini.

`queue_N_rx_refil_partial`: *N*

Jumlah berapa kali driver tidak berhasil mengisi kembali bagian antrean rx yang kosong dengan buffer untuk antrean ini. Jika nilai ini bukan nol, ini menunjukkan sumber daya memori rendah.

`queue_N_rx_bad_csum`: *N*

Jumlah berapa kali antrean `rx` memiliki checksum buruk untuk antrean ini (hanya jika rx checksum offload didukung).

`queue_N_rx_page_alloc_fail`: *N*

Jumlah berapa kali alokasi halaman gagal untuk antrean ini. Jika nilai ini bukan nol, ini menunjukkan sumber daya memori rendah.

`queue_N_rx_skb_alloc_fail`: *N*

Jumlah berapa kali alokasi SKB gagal untuk antrean ini. Jika nilai ini bukan nol, ini menunjukkan sumber daya sistem yang rendah.

`queue_N_rx_dma_mapping_err`: *N*

Jumlah kesalahan akses memori langsung. Jika nilai ini bukan 0, ini menunjukkan sumber daya sistem yang rendah.

`queue_N_rx_bad_desc_num`: *N*

Terlalu banyak buffer per paket. Jika nilai ini bukan 0, ini menunjukkan penggunaan buffer yang sangat kecil.

`queue_N_rx_bad_req_id`: *N*

Req_id untuk antrean ini tidak valid. Req_id valid adalah dari [0, queue_size - 1].

`queue_N_rx_empty_rx_ring`: *N*

Jumlah berapa kali antrean rx kosong untuk antrean ini.

`queue_N_rx_csum_unchecked`: *N*

Jumlah berapa kali antrean rx menerima paket di mana checksum tidak diperiksa untuk antrean ini.

`queue_N_rx_xdp_aborted`: *N*

Jumlah berapa kali paket XDP diklasifikasikan sebagai XDP_ABORT.

`queue_N_rx_xdp_drop`: *N*

Jumlah berapa kali paket XDP diklasifikasikan sebagai XDP_DROP.

`queue_N_rx_xdp_pass`: *N*

Jumlah berapa kali paket XDP diklasifikasikan sebagai XDP_PASS.

`queue_N_rx_xdp_tx: N`

Jumlah berapa kali paket XDP diklasifikasikan sebagai XDP_TX.

`queue_N_rx_xdp_invalid: N`

Jumlah berapa kali kode pengembalian XDP untuk paket tidak valid.

`queue_N_rx_xdp_redirect: N`

Jumlah berapa kali paket XDP diklasifikasikan sebagai XDP_REDIRECT.

`queue_N_xdp_tx_cnt: N`

Jumlah paket yang dikirimkan untuk antrean ini.

`queue_N_xdp_tx_bytes: N`

Jumlah bita yang dikirimkan untuk antrean ini.

`queue_N_xdp_tx_queue_stop: N`

Jumlah berapa kali antrean ini penuh dan dihentikan.

`queue_N_xdp_tx_queue_wakeup: N`

Jumlah berapa kali antrean ini dilanjutkan setelah dihentikan.

`queue_N_xdp_tx_dma_mapping_err: N`

Jumlah kesalahan akses memori langsung. Jika nilai ini bukan 0, ini menunjukkan sumber daya sistem yang rendah.

`queue_N_xdp_tx_linearize: N`

Jumlah berapa kali linierisasi buffer XDP dicoba untuk antrean ini.

`queue_N_xdp_tx_linearize_failed: N`

Jumlah berapa kali linierisasi buffer XDP gagal untuk antrean ini.

`queue_N_xdp_tx_napi_comp: N`

Jumlah berapa kali handler napi memanggil napi_complete untuk antrean ini.

`queue_N_xdp_tx_tx_poll: N`

Jumlah berapa kali handler napi dijadwalkan untuk antrean ini.

`queue_N_xdp_tx_doorbells: N`

Jumlah doorbell transmisi untuk antrean ini.

`queue_N_xdp_tx_prepare_ctx_err: N`

Jumlah berapa kali ena_com_prepare_tx gagal untuk antrean ini. Nilai ini harus selalu nol; jika tidak, lihat log driver.

`queue_N_xdp_tx_bad_req_id: N`

Req_id untuk antrean ini tidak valid. Req_id valid adalah dari [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy: N`

Jumlah paket yang headernya disalin menggunakan buffer llq untuk antrean ini.

`queue_N_xdp_tx_missed_tx: N`

Jumlah berapa kali entri antrean tx melewatkan waktu tunggu penyelesaian untuk antrean ini.

`queue_N_xdp_tx_unmask_interrupt: N`

Jumlah berapa kali interupsi tx dibuka untuk antrean ini.

`ena_admin_q_aborted_cmd: N`

Jumlah perintah admin yang dibatalkan. Ini biasanya terjadi selama prosedur pemulihan otomatis.

`ena_admin_q_submitted_cmd: N`

Jumlah doorbell antrean admin.

`ena_admin_q_completed_cmd: N`

Jumlah penyelesaian antrean admin.

`ena_admin_q_out_of_space: N`

Berapa kali driver mencoba mengirim perintah admin baru, namun antrean penuh.

`ena_admin_q_no_completion: N`

Berapa kali driver tidak mendapatkan penyelesaian perintah dari admin.

Log error driver di syslog

Driver ENA menulis pesan log ke syslog selama boot sistem. Anda dapat memeriksa log ini untuk mencari error jika mengalami masalah. Di bawah ini adalah contoh informasi yang dicatat lognya oleh driver ENA di syslog selama boot sistem, bersama dengan beberapa penjelasan untuk pesan yang dipilih.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM:
 ena_com_validate_version] ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM:
 ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device
 watchdog is Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation
 is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM:
 ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
 is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM:
 ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
 configuration is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic
 Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted.
 Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family
 10
```

Error mana yang dapat saya abaikan?

Peringatan berikut yang mungkin muncul di log error sistem Anda dapat diabaikan untuk Elastic Network Adapter:

Set atribut host tidak didukung

> Atribut host tidak didukung untuk perangkat ini.

gagal untuk mengalokasikan buffer untuk antrean rx

> Ini adalah error yang dapat dipulihkan, dan ini menunjukkan bahwa mungkin ada masalah tekanan memori saat error terjadi.

Fitur *X* tidak didukung

Fitur yang direferensikan tidak didukung oleh Elastic Network Adapter. Nilai yang mungkin untuk *X* meliputi:

- 10: Konfigurasi fungsi RSS Hash tidak didukung untuk perangkat ini.
- 12: Konfigurasi tabel RSS Indirection tidak didukung untuk perangkat ini.
- 18: Konfigurasi Input Hash RSS tidak didukung untuk perangkat ini.
- 20: Moderasi interupsi tidak didukung untuk perangkat ini.
- 27: Driver Adaptor Jaringan Elastis tidak mendukung polling kemampuan Ethernet dari snmpd.

Gagal untuk mengonfigurasi AENQ

Elastic Network Adapter tidak mendukung konfigurasi AENQ.

Mencoba untuk mengatur peristiwa AENQ yang tidak didukung

Error ini menunjukkan upaya untuk mengatur grup peristiwa AENQ yang tidak didukung oleh Elastic Network Adapter.

Pemberitahuan konfigurasi sub-optimal

Perangkat ENA mendeteksi pengaturan konfigurasi sub-optimal di driver yang dapat Anda ubah. Perangkat memberi tahu driver ENA dan mencatat peringatan ke konsol. Contoh berikut menunjukkan format pesan peringatan.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

Daftar berikut menunjukkan detail kode notifikasi dan tindakan yang disarankan untuk temuan konfigurasi sub-optimal.

- Kode 1: ENA Express dengan konfigurasi LLQ lebar tidak disarankan

  ENA Ekspres ENI dikonfigurasi dengan LLQ lebar. Konfigurasi ini kurang optimal dan dapat memengaruhi performa ENA Ekspres. Kami menyarankan Anda menonaktifkan pengaturan LLQ yang luas saat Anda menggunakan ENA Express ENIs sebagai berikut.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

Untuk informasi selengkapnya tentang konfigurasi optimal untuk ENA Ekspres, lihat Tingkatkan kinerja jaringan antar instans EC2 dengan ENA Express.

- Kode 2: ENA Express ENI dengan kedalaman antrian Tx sub-optimal tidak disarankan

  ENA Ekspres ENI dikonfigurasi dengan kedalaman antrean Tx sub-optimal. Konfigurasi ini dapat memengaruhi performa ENA Ekspres. Kami menyarankan Anda memperbesar semua antrian Tx ke nilai maksimum untuk antarmuka jaringan saat Anda menggunakan ENA Express sebagai berikut. ENIs

  Anda dapat menjalankan ethtool perintah berikut untuk menyesuaikan ukuran LLQ. Untuk mempelajari lebih lanjut tentang cara mengontrol, menanyakan, dan mengaktifkan Wide-LLQ, lihat topik Large Low-Latency Queue (Large LLQ) dari driver kernel Linux untuk dokumentasi ENA di repositori Amazon Drivers. GitHub

  ```
  ethtool -g interface
  ```

  Atur antrian Tx Anda ke kedalaman maksimum:

  ```
  ethtool -G interface tx depth
  ```

  Untuk informasi selengkapnya tentang konfigurasi optimal untuk ENA Ekspres, lihat Tingkatkan kinerja jaringan antar instans EC2 dengan ENA Express.

- Kode 3: ENA dengan ukuran LLQ reguler dan lalu lintas paket Tx melebihi ukuran header maksimum yang didukung

  Secara default, ENA LLQ mendukung ukuran header paket Tx hingga 96 byte. Jika ukuran header paket lebih besar dari 96 byte, paket dijatuhkan. Untuk mengurangi masalah ini, kami menyarankan Anda mengaktifkan Wide-LLQ, yang meningkatkan ukuran header paket Tx yang didukung hingga maksimum 224 byte.

  Namun, saat Anda mengaktifkan Wide-LLQ, ukuran cincin Tx maksimum dikurangi dari 1000 menjadi 512 entri. Wide-LLQ diaktifkan secara default untuk semua jenis Nitro v4 dan instance yang lebih baru.

  - Jenis instans Nitro v4 memiliki ukuran cincin Wide-LLQ Tx maksimum default 512 entri, yang tidak dapat diubah.

- Jenis instans Nitro v5 memiliki ukuran cincin Wide-LLQ Tx default 512 entri, yang dapat Anda tingkatkan hingga 1000 entri.

Anda dapat menjalankan ethtool perintah berikut untuk menyesuaikan ukuran LLQ. Untuk mempelajari lebih lanjut tentang cara mengontrol, menanyakan, dan mengaktifkan Wide-LLQ, lihat topik Large Low-Latency Queue (Large LLQ) dari driver kernel Linux untuk dokumentasi ENA di repositori Amazon Drivers. GitHub

Temukan kedalaman maksimum untuk antrian Tx Anda:

```
ethtool -g interface
```

Atur antrian Tx Anda ke kedalaman maksimum:

```
ethtool -G interface tx depth
```

Memecahkan masalah driver Windows Adaptor Jaringan Elastis

Adaptor Jaringan Elastis (ENA) dirancang untuk meningkatkan kesehatan sistem operasi dan mengurangi perilaku atau kegagalan perangkat keras yang tidak terduga yang dapat mengganggu pengoperasian instans Windows Anda. Arsitektur ENA menjaga kegagalan perangkat atau driver setransparan mungkin ke sistem operasi.

Kumpulkan informasi diagnostik pada instans

Langkah-langkah untuk membuka alat sistem operasi (OS) Windows bervariasi, tergantung pada versi OS yang diinstal pada instans Anda. Di bagian berikut, kami menggunakan dialog Run untuk membuka alat, yang bekerja sama di semua versi OS. Namun, Anda dapat mengakses alat ini menggunakan metode apa pun yang Anda inginkan.

Akses dialog Jalankan

- Menggunakan kombinasi tombol logo Windows: `Windows + R`
- Menggunakan bilah pencarian:
  - Masukkan `run` ke bilah pencarian.
  - Pilih aplikasi Jalankan dari hasil pencarian.

Beberapa langkah memerlukan menu konteks untuk mengakses properti atau tindakan peka konteks. Ada beberapa cara untuk melakukan ini, tergantung pada versi OS dan perangkat keras Anda.

Akses menu konteks

- Menggunakan mouse Anda: klik kanan item untuk membuka menu konteksnya.
- Menggunakan keyboard Anda:
  - Tergantung pada versi OS Anda, gunakan `Shift` + `F10`, atau `Ctrl` + `Shift` + `F10`.
  - Jika Anda memiliki tombol konteks pada keyboard Anda (tiga garis horizontal dalam kotak), pilih item yang Anda inginkan dan kemudian tekan tombol konteks.

Jika Anda dapat terhubung ke instans Anda, gunakan teknik berikut untuk mengumpulkan informasi diagnostik untuk pemecahan masalah.

Periksa status perangkat ENA

Untuk memeriksa status driver ENA Windows Anda menggunakan Windows Device Manager, ikuti langkah-langkah berikut:

1. Buka dialog Jalankan menggunakan salah satu metode yang dijelaskan di bagian sebelumnya.
2. Untuk membuka Windows Device Manager, masukkan `devmgmt.msc` di kotak Jalankan.
3. Pilih OKE. Ini membuka jendela Device Manager.
4. Pilih panah di sebelah kiri Adaptor jaringan untuk memperluas daftar.
5. Pilih nama, atau buka menu konteks untuk Adaptor Jaringan Elastis Amazon, lalu pilih Properti. Ini membuka dialog Properti Adaptor Jaringan Elastis Amazon.
6. Verifikasi bahwa pesan di tab Umum mengatakan “Perangkat ini berfungsi dengan baik”.

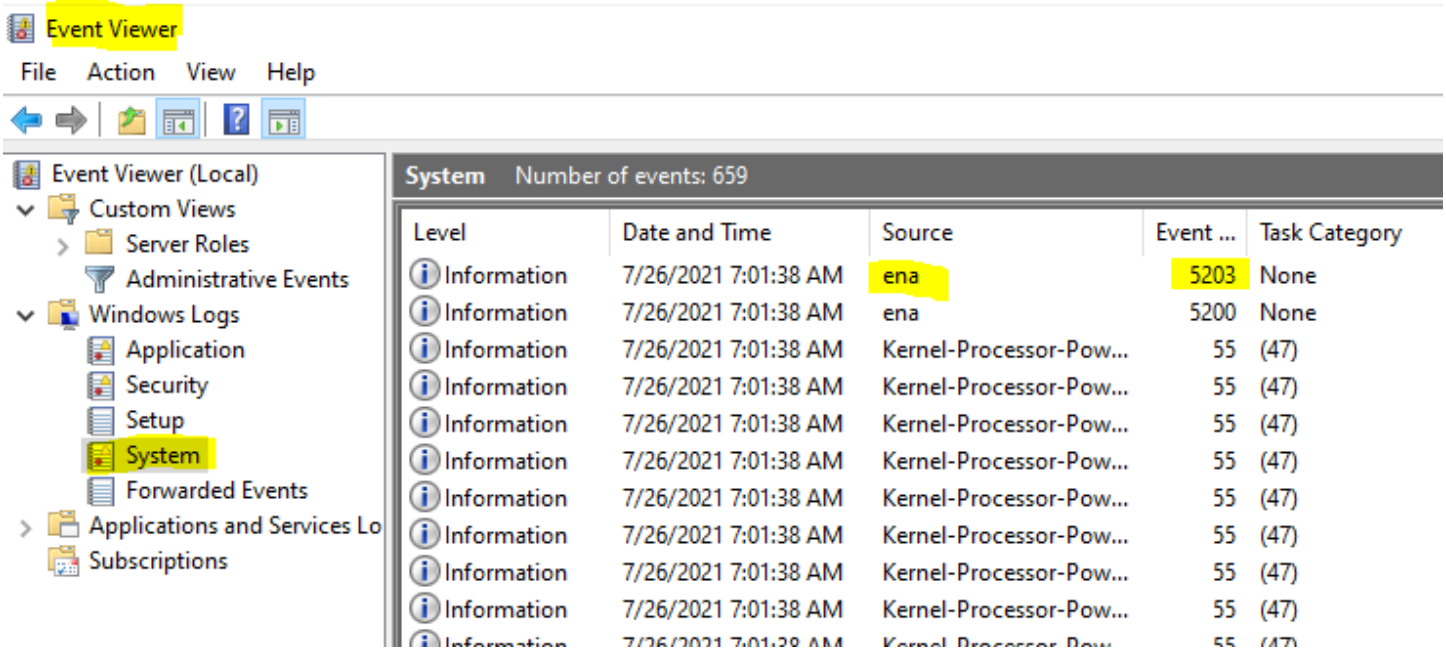
Selidiki pesan peristiwa driver

Untuk meninjau log peristiwa driver ENA Windows menggunakan Windows Event Viewer, ikuti langkah-langkah berikut:

1. Buka dialog Jalankan menggunakan salah satu metode yang dijelaskan di bagian sebelumnya.
2. Untuk membuka Windows Event Viewer, masukkan `eventvwr.msc` di kotak Jalankan.
3. Pilih OKE. Ini membuka jendela Event Viewer.
4. Perluas menu Windows Logs, lalu pilih System.

5. Di bawah Tindakan, di panel kanan atas, pilih Filter Log Saat Ini. Ini menampilkan dialog penyaringan.
6. Di kotak Sumber peristiwa, masukkan `ena`. Ini membatasi hasil untuk peristiwa yang dihasilkan oleh driver ENA Windows.
7. Pilih OKE. Ini menunjukkan hasil log peristiwa yang difilter di bagian detail jendela.
8. Untuk menelusuri detailnya, pilih pesan peristiwa dari daftar.

Contoh berikut menunjukkan peristiwa driver ENA dalam daftar peristiwa sistem Windows Event Viewer:



Ringkasan pesan peristiwa

Tabel berikut menunjukkan pesan peristiwa yang dihasilkan oleh driver ENA Windows.

Input

ID peristiwa	Deskripsi peristiwa driver ENA	Tipe
5001	Perangkat keras kehabisan sumber daya	Kesalahan
5002	Adaptor telah mendeteksi kesalahan perangkat keras	Kesalahan

ID peristiwa	Deskripsi peristiwa driver ENA	Tipe
5005	Adaptor telah habis waktu operasi NDIS yang tidak selesai tepat waktu	Kesalahan
5032	Adaptor gagal mengatur ulang perangkat	Kesalahan
5200	Adaptor telah diinisialisasi	Informasi
5201	Adaptor telah dihentikan	Informasi
5202	Adaptor telah dijeda	Informasi
5203	Adaptor telah dimulai ulang	Informasi
5204	Adaptor telah dimatikan	Informasi
5205	Adaptor telah diatur ulang	Kesalahan
5206	Adaptor telah dihapus secara mengejutkan	Kesalahan
5208	Rutin inisialisasi adaptor telah gagal	Kesalahan
5210	Adaptor telah mengalami dan berhasil memulihkan masalah internal	Kesalahan

Tinjau metrik performa

Driver ENA Windows menerbitkan metrik performa jaringan dari instans di mana metrik diaktifkan. Anda dapat melihat dan mengaktifkan metrik pada instans menggunakan aplikasi Monitor Performa asli. Untuk informasi selengkapnya tentang metrik yang diproduksi driver ENA Windows, lihat Pantau kinerja jaringan untuk pengaturan ENA pada instans EC2 Anda.

Pada contoh di mana metrik ENA diaktifkan, dan CloudWatch agen Amazon diinstal, CloudWatch mengumpulkan metrik yang terkait dengan penghitung di Windows Performance Monitor, serta

beberapa metrik lanjutan untuk ENA. Metrik ini dikumpulkan sebagai tambahan untuk metrik yang diaktifkan secara default di instans EC2. Untuk informasi selengkapnya tentang metrik, lihat Metrik yang dikumpulkan oleh CloudWatch agen di CloudWatch Panduan Pengguna Amazon.

> **Note**
>
> Metrik performa tersedia untuk driver ENA versi 2.4.0 dan yang lebih baru (juga untuk versi 2.2.3). Driver ENA versi 2.2.4 dibatalkan karena potensi penurunan performa pada instans EC2 generasi keenam. Kami menyarankan Anda melakukan peningkatan ke versi driver saat ini untuk memastikan bahwa Anda memiliki pembaruan terbaru.

Beberapa cara yang dapat Anda pakai untuk menggunakan metrik performa meliputi:

- Memecahkan masalah performa instans.
- Pilih ukuran instans yang tepat untuk beban kerja.
- Merencanakan kegiatan penskalaan secara proaktif.
- Benchmark aplikasi untuk menentukan apakah mereka memaksimalkan performa yang tersedia pada sebuah instans.

Tingkat penyegaran

Secara default, driver menyegarkan metrik menggunakan interval 1 detik. Namun, aplikasi yang mengambil metrik mungkin menggunakan interval yang berbeda untuk polling. Anda dapat mengubah interval penyegaran di Device Manager, menggunakan properti lanjutan untuk driver.

Untuk mengubah interval penyegaran metrik untuk driver ENA Windows, ikuti langkah-langkah berikut:

1. Buka dialog Jalankan menggunakan salah satu metode yang dijelaskan di bagian sebelumnya.
2. Untuk membuka Windows Device Manager, masukkan `devmgmt.msc` di kotak Jalankan.
3. Pilih OKE. Ini membuka jendela Device Manager.
4. Pilih panah di sebelah kiri Adaptor jaringan untuk memperluas daftar.
5. Pilih nama, atau buka menu konteks untuk Adaptor Jaringan Elastis Amazon, lalu pilih Properti. Ini membuka dialog Properti Adaptor Jaringan Elastis Amazon.
6. Buka tab Advanced di jendela pop-up.

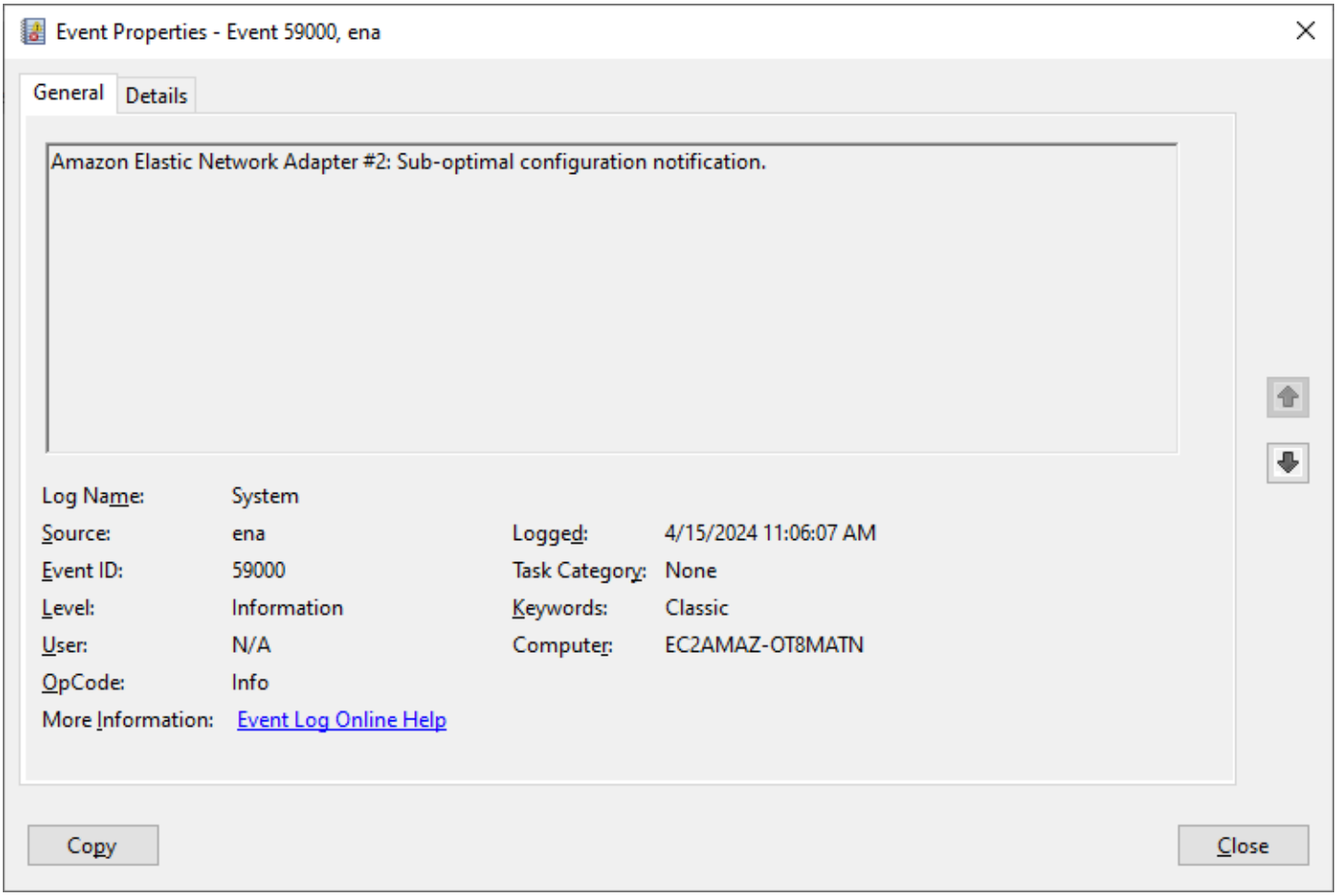
7. Dari daftar Properti, pilih Metrics Refresh Interval untuk mengubah nilai.
8. Setelah selesai, pilih OK.

Selidiki pemberitahuan konfigurasi sub-optimal

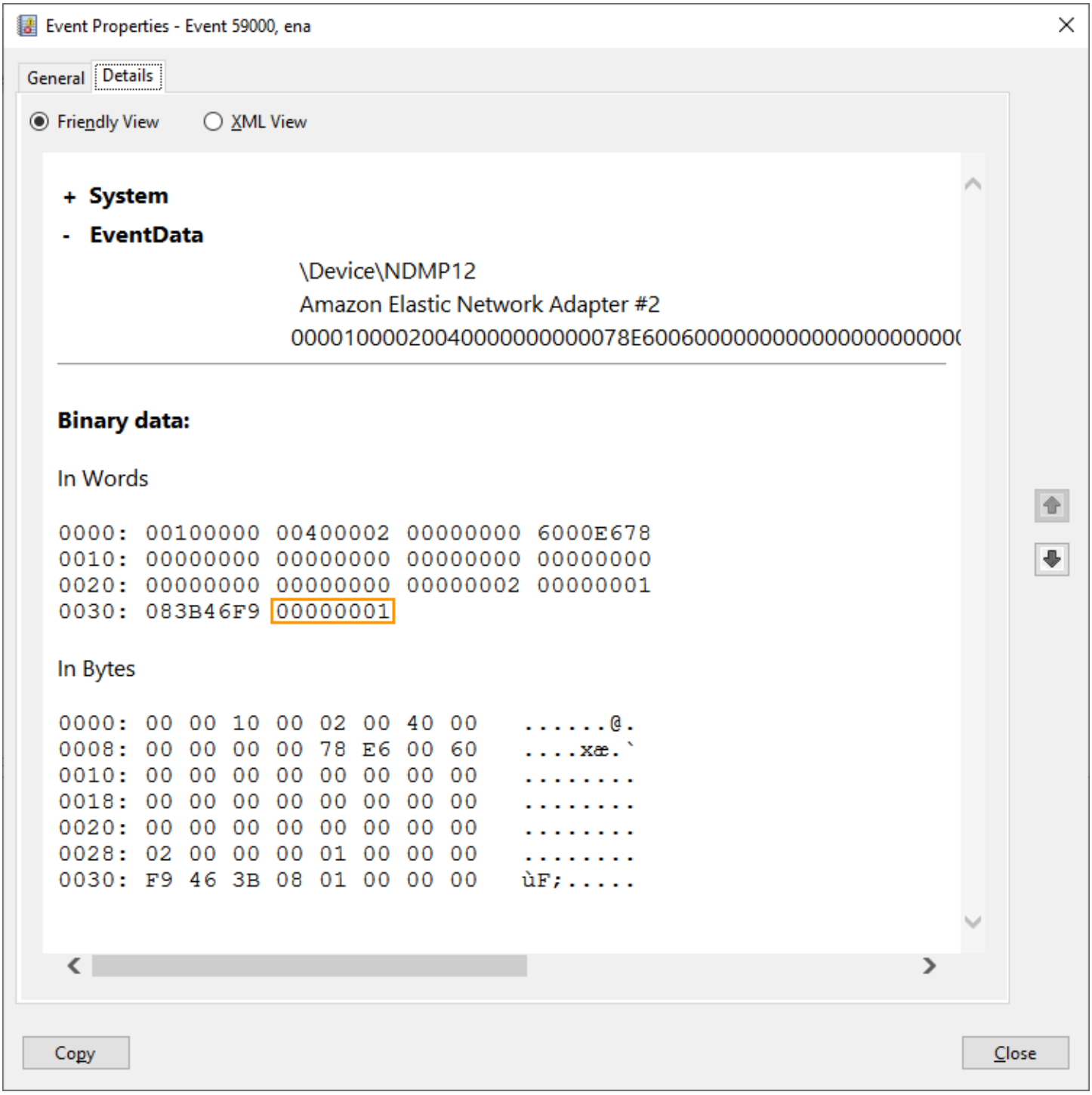
Perangkat ENA mendeteksi pengaturan konfigurasi sub-optimal di driver yang dapat Anda ubah. Perangkat memberi tahu driver ENA dan mencatat pemberitahuan acara. Untuk meninjau peristiwa sub-optimal di Windows Event Viewer

1. Buka dialog Jalankan menggunakan salah satu metode yang dijelaskan di bagian sebelumnya.
2. Untuk membuka Windows Event Viewer, masukkan `eventvwr.msc` di kotak Jalankan.
3. Pilih OKE. Ini membuka jendela Event Viewer.
4. Perluas menu Windows Logs, lalu pilih System.
5. Di bawah Tindakan, di panel kanan atas, pilih Filter Log Saat Ini. Ini menampilkan dialog penyaringan.
6. Di kotak Sumber peristiwa, masukkan `ena`. Ini membatasi hasil untuk peristiwa yang dihasilkan oleh driver ENA Windows.
7. Pilih OKE. Ini menunjukkan hasil log peristiwa yang difilter di bagian detail jendela.

Peristiwa dengan ID `5900`0 memberi tahu Anda tentang temuan konfigurasi yang kurang optimal. Klik kanan acara dan pilih Properti Acara untuk membuka tampilan detail, atau pilih Panel Pratinjau dari menu Tampilan untuk melihat detail yang sama.



Buka tab Detail untuk melihat kode acara. Di bagian Binary Data: In words, kata terakhir adalah kode.



Daftar berikut menunjukkan detail kode notifikasi dan tindakan yang disarankan untuk temuan konfigurasi sub-optimal.

- Kode**1**: ENA Ekspres dengan konfigurasi LLQ lebar tidak disarankan

ENA Ekspres ENI dikonfigurasi dengan LLQ lebar. Konfigurasi ini kurang optimal dan dapat memengaruhi performa ENA Ekspres. Kami menyarankan Anda menonaktifkan pengaturan LLQ yang luas saat Anda menggunakan ENA Express ENIs sebagai berikut.

1. Untuk membuka Windows Device Manager, masukkan `devmgmt.msc` di kotak Jalankan.
2. Pilih OKE. Ini membuka jendela Device Manager.
3. Pilih panah di sebelah kiri Adaptor jaringan untuk memperluas daftar.
4. Buka properti perangkat untuk file`Amazon Elastic Network Adapter`.
5. Dari sana, buka tab Advanced untuk membuat perubahan Anda.
6. Pilih properti LLQ Header Size Policy, dan atur nilainya. `Normal (128 Bytes)`
7. Pilih OK untuk menyimpan perubahan Anda.

- Kode**2**: ENA Ekspres ENI dengan kedalaman antrean Tx sub-optimal tidak disarankan

  ENA Ekspres ENI dikonfigurasi dengan kedalaman antrean Tx sub-optimal. Konfigurasi ini dapat memengaruhi performa ENA Ekspres. Kami menyarankan Anda memperbesar semua antrian Tx ke nilai maksimum untuk antarmuka jaringan saat Anda menggunakan ENA Express sebagai berikut. ENIs

  Ikuti langkah-langkah ini untuk memperbesar antrian Tx ke kedalaman maksimum:

  1. Untuk membuka Windows Device Manager, masukkan `devmgmt.msc` di kotak Jalankan.
  2. Pilih OKE. Ini membuka jendela Device Manager.
  3. Pilih panah di sebelah kiri Adaptor jaringan untuk memperluas daftar.
  4. Buka properti perangkat untuk file`Amazon Elastic Network Adapter`.
  5. Dari sana, buka tab Advanced untuk membuat perubahan Anda.
  6. Pilih properti Transmit Buffers, dan atur nilainya ke maksimum yang didukung.
  7. Pilih OK untuk menyimpan perubahan Anda.

Reset adaptor ENA

Proses reset dimulai ketika driver ENA Windows mendeteksi kesalahan pada adaptor, dan menandai adaptor sebagai tidak sehat. Driver tidak dapat mengatur ulang sendiri, jadi itu tergantung pada sistem operasi untuk memeriksa status kesehatan adaptor, dan memanggil pegangan reset untuk driver ENA Windows. Proses reset dapat mengakibatkan periode waktu singkat di mana kehilangan lalu lintas terjadi. Namun, koneksi TCP harus dapat pulih.

Adaptor ENA mungkin juga secara tidak langsung meminta prosedur reset perangkat, dengan gagal mengirim notifikasi keep-alive. Misalnya, jika adaptor ENA mencapai status tidak diketahui setelah memuat konfigurasi yang tidak dapat dipulihkan, mungkin berhenti mengirim notifikasi keep-alive.

Penyebab umum reset untuk adaptor ENA

- Pesan yang masih aktif tidak ada

  Adaptor ENA memposting peristiwa keep-alive dengan kecepatan tetap (biasanya sekali setiap detik). Driver ENA Windows mengimplementasikan mekanisme watchdog, yang secara berkala memeriksa keberadaan pesan keep-alive ini. Jika mendeteksi satu atau lebih pesan baru sejak terakhir kali diperiksa, itu mencatat hasil yang sukses. Jika tidak, pengemudi menyimpulkan bahwa perangkat mengalami kegagalan, dan memulai urutan reset.
- Paket terjebak dalam antrean transmisi

  Adaptor ENA memverifikasi bahwa paket mengalir melalui antrean transmisi seperti yang diharapkan. Driver ENA Windows mendeteksi jika paket macet, dan memulai urutan reset jika ada.
- Batas waktu baca untuk register Memory Mapped I/O (MMIO)

  Untuk membatasi operasi pembacaan memori yang dipetakan I/O (MMIO), driver ENA Windows mengakses register MMIO hanya selama proses inisialisasi dan reset. Jika driver mendeteksi batas waktu, dibutuhkan salah satu tindakan berikut, tergantung pada proses apa yang sedang berjalan:
  - Jika batas waktu terdeteksi selama inisialisasi, aliran gagal, yang mengakibatkan driver menampilkan tanda seru kuning oleh adaptor ENA di Windows Device Manager.
  - Jika batas waktu terdeteksi selama reset, alirannya gagal. OS kemudian memulai penghapusan kejutan adaptor ENA, dan memulihkannya dengan menghentikan dan memulai adaptor yang telah dihapus. Untuk informasi selengkapnya tentang penghapusan kejutan kartu antarmuka jaringan (NIC), lihat Menangani Penghapusan Kejutan NIC dalam dokumentasi Developer Perangkat Keras Microsoft Windows.

Skenario pemecahan masalah

Skenario berikut dapat membantu Anda memecahkan masalah yang mungkin Anda alami dengan driver ENA Windows. Kami menyarankan Anda memulai dengan meningkatkan driver ENA Anda, jika Anda tidak memiliki versi terbaru. Untuk menemukan driver terbaru untuk versi OS Windows Anda, lihat Lacak rilis versi driver ENA Windows.

Versi driver ENA yang tidak terduga diinstal

Deskripsi

Setelah Anda melalui langkah-langkah untuk menginstal versi tertentu dari driver ENA, Windows Device Manager menunjukkan bahwa Windows menginstal versi driver ENA yang berbeda.

Penyebab

Ketika Anda menjalankan instalasi untuk paket driver, Windows memberi peringkat semua paket driver yang valid untuk perangkat yang diberikan di Toko Driver lokal sebelum dimulai. Kemudian memilih paket dengan nilai peringkat terendah sebagai kecocokan terbaik. Ini bisa berbeda dari paket yang ingin Anda instal. Untuk informasi selengkapnya tentang proses pemilihan paket driver perangkat, lihat Cara Windows memilih paket driver untuk perangkat di situs web dokumentasi Microsoft.

Solusi

Untuk memastikan bahwa Windows menginstal versi paket driver yang Anda pilih, Anda dapat menghapus paket driver berperingkat lebih rendah dari Toko Driver dengan alat baris PUtil perintah Pn.

Ikuti langkah-langkah berikut ini untuk memperbarui driver ENA:

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.
2. Buka jendela properti Device Manager, seperti yang dijelaskan di Periksa status perangkat ENA bagian. Ini membuka tab Umum jendela Properti Adaptor Jaringan Elastis Amazon.
3. Buka tab Driver.
4. Pilih Perbarui Driver. Ini membuka kotak dialog Perbarui Driver Perangkat lunak – Adaptor Jaringan Elastis Amazon.
    a. Pada Bagaimana Anda ingin mencari perangkat lunak driver? halaman, pilih Jelajahi komputer saya untuk perangkat lunak driver.
    b. Pada halaman Jelajahi driver perangkat lunak di komputer Anda, pilih Biarkan saya memilih dari daftar driver perangkat di komputer saya, yang terletak di bawah bilah pencarian.
    c. Pada Pilih driver perangkat yang ingin Anda instal untuk halaman perangkat keras ini, pilih Have Disk....
    d. Di jendela Instal dari Disk, pilih Browse..., di sebelah lokasi file dari daftar dropdown.

e. Arahkan ke lokasi di mana Anda mengunduh paket driver ENA target. Pilih file bernama `ena.inf` dan pilih Buka.

f. Untuk memulai instalasi, pilih OK, lalu pilih Selanjutnnya.

5. Jika penginstal tidak secara otomatis me-reboot instance Anda, jalankan Restart-Computer PowerShell cmdlet.

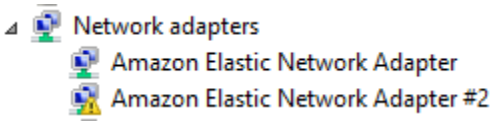
```
PS C:\> Restart-Computer
```

Peringatan perangkat untuk driver ENA

Deskripsi

Ikon adaptor ENA di bagian Adaptor Jaringan Manajer Perangkat menampilkan tanda peringatan (segitiga kuning dengan tanda seru di dalamnya).

Contoh berikut menunjukkan adaptor ENA dengan ikon peringatan di Windows Device Manager:



Penyebab

Peringatan perangkat ini umumnya disebabkan oleh masalah lingkungan, yang mungkin memerlukan lebih banyak penelitian, dan seringkali memerlukan proses eliminasi untuk menentukan penyebab yang mendasarinya. Untuk daftar lengkap kesalahan perangkat, lihat Pesan Kesalahan Pengelola Perangkat di dokumentasi Microsoft.

Solusi

Solusi untuk peringatan perangkat ini tergantung pada akar penyebabnya. Proses eliminasi yang dijelaskan di sini mencakup beberapa langkah dasar untuk membantu mengidentifikasi dan menyelesaikan masalah paling umum yang mungkin memiliki solusi sederhana. Analisis akar penyebab tambahan diperlukan ketika langkah-langkah ini tidak menyelesaikan masalah.

Ikuti langkah-langkah berikut untuk membantu mengidentifikasi dan menyelesaikan masalah umum:

1. Hentikan dan mulai perangkat

   Buka jendela properti Device Manager, seperti yang dijelaskan di Periksa status perangkat ENA bagian. Ini membuka tab Umum jendela Properti Adaptor Jaringan Elastis Amazon, di mana status Perangkat menampilkan kode kesalahan dan pesan singkat.

   a. Buka tab Driver.
   b. Pilih Nonaktifkan Perangkat, dan tanggapi Ya pada pesan peringatan yang ditampilkan.
   c. Pilih Aktifkan Perangkat.

2. Hentikan dan mulai instans EC2

   Jika adaptor masih menampilkan ikon peringatan di Device Manager, langkah selanjutnya adalah menghentikan dan memulai instans EC2. Ini meluncurkan kembali instans pada perangkat keras yang berbeda dalam banyak kasus.

3. Selidiki kemungkinan masalah sumber daya instans

   Jika Anda telah menghentikan dan memulai instans EC2 Anda, dan masalah tetap ada, ini mungkin menunjukkan masalah sumber daya pada instans Anda, seperti memori yang tidak mencukupi.

Batas waktu koneksi dengan reset adaptor (kode kesalahan 5007, 5205)

Deskripsi

Windows Event Viewer menunjukkan batas waktu adaptor dan mengatur ulang peristiwa yang terjadi dalam kombinasi untuk adaptor ENA. Pesan menyerupai contoh berikut:

- ID Peristiwa 5007: Adaptor Jaringan Elastis Amazon: Habis waktu selama operasi.
- ID Peristiwa 5205: Adaptor Jaringan Elastis Amazon: Atur ulang adaptor telah dimulai.

Atur ulang adaptor menyebabkan gangguan lalu lintas minimal. Bahkan ketika ada beberapa reset, itu tidak biasa bagi mereka untuk menyebabkan gangguan jaringan yang parah.

Penyebab

Urutan peristiwa ini menunjukkan bahwa driver ENA Windows memulai reset untuk adaptor ENA yang tidak responsif. Namun, mekanisme yang digunakan driver perangkat untuk mendeteksi masalah ini tunduk pada positif palsu akibat kelaparan CPU 0.

Solusi

Jika kombinasi kesalahan ini sering terjadi, periksa alokasi sumber daya Anda untuk melihat di mana penyesuaian mungkin bermanfaat.

1. Buka dialog Jalankan menggunakan salah satu metode yang dijelaskan di bagian sebelumnya.
2. Untuk membuka Windows Resource Monitor, masukkan `resmon` di kotak Jalankan.
3. Pilih OKE. Ini membuka jendela Resource Monitor.
4. Buka tab CPU. Grafik penggunaan per CPU ditampilkan di sepanjang sisi kanan jendela Resource Monitor.
5. Periksa tingkat penggunaan untuk CPU 0 untuk melihat apakah mereka terlalu tinggi.

Kami menyarankan Anda mengonfigurasi RSS untuk mengecualikan CPU 0 untuk adaptor ENA pada tipe instans yang lebih besar (lebih dari 16 vCPU). Untuk tipe instans yang lebih kecil, mengonfigurasi RSS dapat meningkatkan pengalaman, tetapi karena jumlah inti yang tersedia lebih rendah, pengujian diperlukan untuk memastikan bahwa membatasi inti CPU tidak berdampak negatif pada performa.

Gunakan perintah Set-NetAdapterRss untuk mengonfigurasi RSS untuk adaptor ENA Anda, seperti yang ditunjukkan dalam contoh berikut ini.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

Migrasi ke infrastruktur instans generasi keenam berdampak pada performa atau keterikatan

Deskripsi

Jika Anda bermigrasi ke instans EC2 generasi keenam, Anda mungkin mengalami penurunan performa atau kegagalan lampiran ENA jika Anda belum memperbarui versi driver ENA Windows Anda.

Penyebab

Tipe instans EC2 generasi keenam memerlukan versi minimum driver ENA Windows berikut, berdasarkan sistem operasi instans (OS).

Versi minimum

Versi Windows Server	Versi driver ENA
Windows Server 2008 R2	2.2.3 atau 2.4.0
Windows Server 2012 dan yang lebih baru	2.2.3 dan versi yang lebih baru
Stasiun Kerja Windows	2.2.3 dan versi yang lebih baru

Solusi

Sebelum Anda meningkatkan ke instans EC2 generasi keenam, pastikan AMI yang Anda luncurkan memiliki driver yang kompatibel berdasarkan OS instans seperti yang ditunjukkan pada tabel sebelumnya. Untuk informasi selengkapnya, lihat Apa yang harus saya lakukan sebelum memigrasikan instans EC2 saya ke instans generasi keenam untuk memastikan bahwa saya mendapatkan performa jaringan yang maksimal? di pusat AWS re:Post pengetahuan.

Performa suboptimal untuk antarmuka jaringan elastis

Deskripsi

Antarmuka ENA tidak berfungsi seperti yang diharapkan.

Penyebab

Analisis akar penyebab untuk masalah performa adalah proses eliminasi. Ada terlalu banyak variabel yang terlibat untuk menyebutkan penyebab umum.

Solusi

Langkah pertama dalam analisis akar penyebab Anda adalah meninjau informasi diagnostik untuk instans yang tidak berfungsi seperti yang diharapkan, untuk menentukan apakah ada kesalahan yang mungkin menyebabkan masalah. Untuk informasi selengkapnya, lihat bagian Kumpulkan informasi diagnostik pada instans.

Anda mungkin perlu memodifikasi sistem operasi default untuk mencapai performa jaringan maksimum pada instans dengan jaringan yang ditingkatkan. Beberapa pengoptimalan, seperti

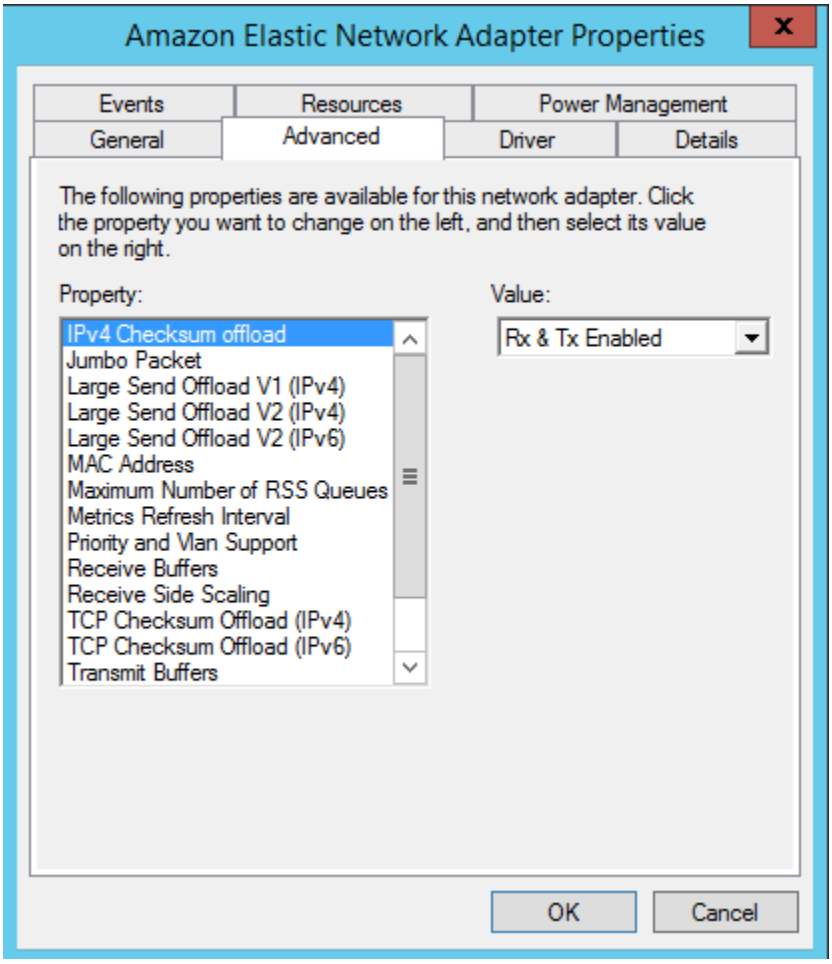
mengaktifkan pembongkaran checksum dan mengaktifkan RSS, dikonfigurasi secara default di Windows resmi. AMIs Untuk pengoptimalan lain yang dapat Anda terapkan ke adaptor ENA, lihat penyesuaian performa yang ditunjukkan di Penyesuaian performa adaptor ENA.

Kami menyarankan Anda melanjutkan dengan hati-hati, dan membatasi penyesuaian properti perangkat ke yang tercantum di bagian ini, atau perubahan spesifik yang direkomendasikan oleh tim AWS dukungan.

Untuk mengubah properti adaptor ENA, ikuti langkah-langkah ini:

1. Buka dialog Jalankan menggunakan salah satu metode yang dijelaskan di bagian sebelumnya.
2. Untuk membuka Windows Device Manager, masukkan `devmgmt.msc` di kotak Jalankan.
3. Pilih OKE. Ini membuka jendela Device Manager.
4. Pilih panah di sebelah kiri Adaptor jaringan untuk memperluas daftar.
5. Pilih nama, atau buka menu konteks untuk Adaptor Jaringan Elastis Amazon, lalu pilih Properti. Ini membuka dialog Properti Adaptor Jaringan Elastis Amazon.
6. Untuk membuat perubahan, buka tab Advanced.
7. Setelah selesai, pilih OKE untuk menyimpan perubahan Anda.

Contoh berikut menunjukkan properti adaptor ENA di Windows Device Manager:



Penyesuaian performa adaptor ENA

Tabel berikut mencakup properti yang dapat disesuaikan untuk meningkatkan performa antarmuka ENA.

Input

Properti	Deskripsi	Nilai default	Penyesuaian
Menerima Buffer	Mengontrol jumlah entri dalam perangkat lunak menerima antrean.	1024	Dapat ditingkatkan hingga maksimum 8192.
Terima Penskalaan Samping (RSS)	Memungkinkan distribusi pemrosesa	Enabled	Anda dapat menyebarkan beban

Properti	Deskripsi	Nilai default	Penyesuaian
	n penerimaan jaringan yang efisien CPUs di beberapa sistem multiprosesor.		di beberapa prosesor. Untuk mempelaja ri selengkapnya, lihat Optimalkan kinerja jaringan pada instance EC2 Windows.

Properti	Deskripsi	Nilai default	Penyesuaian
Jumlah Antrean RSS Maksimum	Mengatur jumlah maksimum antrean RSS yang diizinkan saat RSS diaktifkan.	32	Jumlah antrean RSS ditentukan selama inisialisasi pengemudi, dan mencakup batasan berikut (antara lain): • Batas antrean RSS ditetapkan oleh properti ini • Batas instans (jumlah vCPU) • Batas pembuatan perangkat keras (hingga 8 antrian RSS masuk ENAv1, dan hingga 32 antrian RSS) ENAv2 Anda dapat mengatur nilai dari 1-32, tergantung pada instans dan batas pembuatan perangkat keras Anda. Untuk mempelajari selengkapnya, lihat Optimalkan kinerja jaringan

Properti	Deskripsi	Nilai default	Penyesuaian
			pada instance EC2 Windows.
Paket jumbo	Memungkinkan penggunaan bingkai ethernet jumbo (lebih dari 1500 byte muatan).	Dinonaktifkan (ini membatasi muatan hingga 1500 byte atau kurang)	Nilai dapat diatur ke 9015, yang diterjemahkan ke 9001 byte payload. Ini adalah muatan maksimum untuk bingkai ethernet jumbo. Lihat Pertimbangan untuk menggunakan frame ethernet jumbo.

Pertimbangan untuk menggunakan frame ethernet jumbo

Bingkai jumbo memungkinkan lebih dari 1500 byte data dengan meningkatkan ukuran payload per paket, yang meningkatkan persentase paket yang bukan overhead paket. Diperlukan lebih sedikit paket untuk mengirimkan data yang dapat digunakan dalam jumlah sama. Namun, lalu lintas dibatasi hingga MTU maksimum 1500 dalam kasus berikut:

- Lalu lintas di luar AWS Wilayah tertentu untuk EC2 Classic.
- Lalu lintas di luar VPC tunggal.
- Lalu lintas melalui koneksi peering VPC antar wilayah.
- Lalu lintas melalui koneksi VPN.
- Lalu lintas melalui gateway internet.

> **Note**
>
> Paket lebih dari 1500 byte terfragmentasi. Jika Anda memiliki `Don't Fragment` bendera yang disetel di header IP, paket-paket ini dijatuhkan.
> Frame Jumbo harus digunakan dengan hati-hati untuk lalu lintas internet-bound atau setiap lalu lintas yang meninggalkan VPC. Paket difragmentasi oleh sistem menengah, yang

memperlambat lalu lintas ini. Untuk menggunakan bingkai jumbo di dalam VPC tanpa memengaruhi lalu lintas keluar yang meninggalkan VPC, coba salah satu opsi berikut:

- Konfigurasikan ukuran MTU berdasarkan rute.
- Gunakan beberapa antarmuka jaringan dengan ukuran MTU yang berbeda dan rute yang berbeda.

Kasus penggunaan yang disarankan untuk bingkai jumbo

Bingkai jumbo dapat berguna untuk lalu lintas di dalam dan di antaranya VPCs. Kami merekomendasikan penggunaan bingkai jumbo untuk kasus penggunaan berikut:

- Untuk instans yang ditempatkan di dalam grup penempatan klaster, bingkai jumbo membantu mencapai throughput jaringan semaksimum mungkin. Untuk informasi selengkapnya, lihat Grup penempatan untuk EC2 instans Amazon Anda.
- Anda dapat menggunakan bingkai jumbo untuk lalu lintas antara jaringan lokal Anda VPCs dan jaringan lokal Anda. Direct ConnectUntuk informasi selengkapnya tentang penggunaan Direct Connect, dan verifikasi kemampuan jumbo frame, lihat MTU untuk antarmuka virtual pribadi atau antarmuka virtual transit di Panduan Pengguna.Direct Connect
- Untuk informasi selengkapnya tentang ukuran MTU yang didukung untuk gateway transit, lihat Kuota untuk gateway transit Anda di Panduan Pengguna Gateway Transit Amazon VPC.

Tingkatkan kinerja jaringan antar instans EC2 dengan ENA Express

ENA Express didukung oleh teknologi AWS Scalable Reliable Datagram (SRD). SRD adalah protokol transportasi jaringan performa tinggi yang menggunakan perutean dinamis untuk meningkatkan throughput dan meminimalkan latensi ekor. Dengan ENA Express, Anda dapat berkomunikasi antara dua instans EC2 di Availability Zone yang sama.

Manfaat ENA Ekspres

- Meningkatkan bandwidth maksimum yang dapat digunakan aliran tunggal dari 5 Gbps hingga 25 Gbps dalam Availability Zone, hingga batas instans agregat.
- Mengurangi latensi ekor lalu lintas jaringan antara instans EC2, terutama selama periode beban jaringan yang tinggi.
- Mendeteksi dan menghindari jalur jaringan yang padat.

- Menangani beberapa tugas secara langsung di lapisan jaringan, seperti penataan ulang paket di ujung penerima, dan sebagian besar transmisi ulang yang diperlukan. Ini membebaskan lapisan aplikasi untuk pekerjaan lain.

> **Note**
>
> - Jika aplikasi Anda mengirim atau menerima volume paket yang tinggi per detik, dan perlu mengoptimalkan latensi sebagian besar waktu, terutama selama periode ketika tidak ada kemacetan di jaringan, Jaringan yang ditingkatkan mungkin lebih cocok untuk jaringan Anda.
> - Lalu lintas ENA Express tidak dapat dikirim di Zona Lokal.

Setelah Anda mengaktifkan ENA Express untuk lampiran antarmuka jaringan pada sebuah instance, instance pengirim memulai komunikasi dengan instance penerima, dan SRD mendeteksi apakah ENA Express beroperasi pada instance pengirim dan instance penerima. Jika ENA Ekspres beroperasi, komunikasi dapat menggunakan transmisi SRD. Jika ENA Ekspres tidak beroperasi, komunikasi kembali ke transmisi ENA standar.

Selama periode waktu ketika lalu lintas jaringan ringan, Anda mungkin melihat sedikit peningkatan latensi paket (puluhan mikrodetik) ketika paket menggunakan ENA Ekspres. Selama waktu tersebut, aplikasi yang memprioritaskan karakteristik performa jaringan tertentu dapat memperoleh manfaat dari ENA Ekspres sebagai berikut:

- Proses dapat memperoleh manfaat dari peningkatan bandwidth aliran tunggal maksimum dari 5 Gbps hingga 25 Gbps dalam Availability Zone yang sama, hingga batas instans agregat. Misalnya, jika tipe instans tertentu mendukung hingga 12,5 Gbps, bandwidth aliran tunggal juga dibatasi hingga 12,5 Gbps.
- Proses yang berjalan lebih lama akan mengalami pengurangan latensi ekor selama periode kemacetan jaringan.
- Proses dapat memperoleh manfaat dari distribusi yang lebih lancar dan lebih standar untuk waktu respons jaringan.

Topik

- Cara kerja ENA Ekspres

- Tipe instans yang didukung untuk ENA Ekspres
- Prasyarat untuk instance Linux
- Menyetel kinerja untuk pengaturan ENA Express pada instans Linux
- Tinjau pengaturan ENA Express untuk instans EC2 Anda
- Konfigurasikan pengaturan ENA Express untuk instans EC2 Anda

Cara kerja ENA Ekspres

ENA Express didukung oleh teknologi AWS Scalable Reliable Datagram (SRD). Ini mendistribusikan paket untuk setiap aliran jaringan di jalur AWS jaringan yang berbeda, dan secara dinamis menyesuaikan distribusi ketika mendeteksi tanda-tanda kemacetan. Ini juga mengelola penataan ulang paket di ujung penerima.

Untuk memastikan bahwa ENA Ekspres dapat mengelola lalu lintas jaringan sebagaimana dimaksud, mengirim dan menerima instans dan komunikasi di antara mereka harus memenuhi semua persyaratan berikut:

- Baik tipe instans pengiriman maupun penerimaan didukung. Lihat tabel Tipe instans yang didukung untuk ENA Ekspres untuk informasi selengkapnya.
- Instans pengiriman dan penerimaan harus memiliki ENA Ekspres yang dikonfigurasi. Jika ada perbedaan dalam konfigurasi, Anda dapat mengalami situasi di mana lalu lintas default ke transmisi ENA standar. Skenario berikut menunjukkan apa yang bisa terjadi.

  Skenario: Perbedaan konfigurasi

Instans	ENA Ekspres Diaktifkan	UDP menggunakan ENA Ekspres
Instans 1	Ya	Ya
Instans 2	Ya	Tidak

  Dalam hal ini, lalu lintas TCP antara dua instans dapat menggunakan ENA Ekspres, karena kedua instans telah mengaktifkannya. Namun, karena salah satu instans tidak menggunakan ENA Ekspres untuk lalu lintas UDP, komunikasi antara dua instans ini melalui UDP menggunakan transmisi ENA standar.

- Instance pengiriman dan penerimaan harus berjalan di Availability Zone yang sama.
- Jalur jaringan antara instans tidak boleh menyertakan kotak perangkat lunak perantara (middleware). ENA Ekspres saat ini tidak mendukung kotak perangkat lunak perantara (middleware).
- (Hanya instance Linux) Untuk memanfaatkan potensi bandwidth penuh, gunakan driver versi 2.2.9 atau lebih tinggi.
- (Hanya instance Linux) Untuk menghasilkan metrik, gunakan driver versi 2.8 atau lebih tinggi.

Jika ada persyaratan yang tidak terpenuhi, instance menggunakan TCP/UDP protokol standar tetapi tanpa SRD untuk berkomunikasi.

Untuk memastikan bahwa driver jaringan instans Anda dikonfigurasi untuk performa optimal, tinjau praktik terbaik yang disarankan untuk driver ENA. Praktik terbaik ini juga berlaku untuk ENA Ekspres. Untuk informasi selengkapnya, lihat Panduan Praktik Terbaik dan Pengoptimalan Kinerja Driver ENA Linux di GitHub situs web.

> **Note**
>
> Amazon EC2 mengacu pada hubungan antara instans dan antarmuka jaringan yang melekat padanya sebagai lampiran. Pengaturan ENA Ekspres berlaku untuk lampiran. Jika antarmuka jaringan terlepas dari instans, lampiran tidak ada lagi, dan pengaturan ENA Ekspres yang diterapkan padanya tidak lagi berlaku. Hal yang sama berlaku ketika sebuah instans diakhiri, bahkan jika antarmuka jaringan tetap ada.

Setelah mengaktifkan ENA Express untuk lampiran antarmuka jaringan pada instans pengirim dan instans penerima, Anda dapat menggunakan metrik ENA Express untuk membantu memastikan bahwa instans Anda memanfaatkan sepenuhnya peningkatan kinerja yang disediakan oleh teknologi SRD. Untuk informasi lebih lanjut tentang metrik ENA Ekspres, lihat Metrik untuk ENA Ekspres.

Tipe instans yang didukung untuk ENA Ekspres

Jenis contoh berikut mendukung ENA Express.

General purpose

Tipe instans	Arsitektur
m6a.12xlarge	x86_64
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m6idn.8xlarge	x86_64

Tipe instans	Arsitektur
m6idn.12xlarge	x86_64
m6idn.16xlarge	x86_64
m6idn.24xlarge	x86_64
m6idn.32xlarge	x86_64
m6idn.metal	x86_64
m6in.8xlarge	x86_64
m6in.12xlarge	x86_64
m6in.16xlarge	x86_64
m6in.24xlarge	x86_64
m6in.32xlarge	x86_64
m6in.metal	x86_64
m7a.12xlarge	x86_64
m7a.16xlarge	x86_64
m7a.24xlarge	x86_64
m7a.32xlarge	x86_64
m7a.48xlarge	x86_64
m7a.metal-48xl	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64

Tipe instans	Arsitektur
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64
m8a.16xlarge	x86_64
m8a.24xlarge	x86_64
m8a.48xlarge	x86_64
m8a.metal-24xl	x86_64
m8a.metal-48xl	x86_64
m8azn.12xlarge	x86_64
m8azn.24xlarge	x86_64
m8azn.metal-12xl	x86_64
m8azn.metal-24xl	x86_64
m8g.12xlarge	arm64
m8g.16xlarge	arm64

Tipe instans	Arsitektur
m8g.24xlarge	arm64
m8g.48xlarge	arm64
m8g.metal-24xl	arm64
m8g.metal-48xl	arm64
m8gb.8xlarge	arm64
m8gb.12xlarge	arm64
m8gb.16xlarge	arm64
m8gb.24xlarge	arm64
m8gb.48xlarge	arm64
m8gb.metal-24xl	arm64
m8gb.metal-48xl	arm64
m8gd.12xlarge	arm64
m8gd.16xlarge	arm64
m8gd.24xlarge	arm64
m8gd.48xlarge	arm64
m8gd.metal-24xl	arm64
m8gd.metal-48xl	arm64
m8gn.8xlarge	arm64
m8gn.12xlarge	arm64
m8gn.16xlarge	arm64

Tipe instans	Arsitektur
m8gn.24xlarge	arm64
m8gn.48xlarge	arm64
m8gn.metal-24xl	arm64
m8gn.metal-48xl	arm64
m8i.24xlarge	x86_64
m8i.32xlarge	x86_64
m8i.48xlarge	x86_64
m8i.96xlarge	x86_64
m8i.metal-48xl	x86_64
m8i.metal-96xl	x86_64
m8id.24xlarge	x86_64
m8id.32xlarge	x86_64
m8id.48xlarge	x86_64
m8id.96xlarge	x86_64
m8id.metal-48xl	x86_64
m8id.metal-96xl	x86_64

Compute optimized

Tipe instans	Arsitektur
c6a.12xlarge	x86_64

Tipe instans	Arsitektur
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64
c6a.metal	x86_64
c6gn.4xlarge	arm64
c6gn.8xlarge	arm64
c6gn.12xlarge	arm64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64

Tipe instans	Arsitektur
c6id.metal	x86_64
c6in.8xlarge	x86_64
c6in.12xlarge	x86_64
c6in.16xlarge	x86_64
c6in.24xlarge	x86_64
c6in.32xlarge	x86_64
c6in.metal	x86_64
c7a.12xlarge	x86_64
c7a.16xlarge	x86_64
c7a.24xlarge	x86_64
c7a.32xlarge	x86_64
c7a.48xlarge	x86_64
c7a.metal-48xl	x86_64
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64
c7gd.metal	arm64
c7gn.4xlarge	arm64

Tipe instans	Arsitektur
c7gn.8xlarge	arm64
c7gn.12xlarge	arm64
c7gn.16xlarge	arm64
c7gn.metal	arm64
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64
c8a.16xlarge	x86_64
c8a.24xlarge	x86_64
c8a.48xlarge	x86_64
c8a.metal-24xl	x86_64
c8a.metal-48xl	x86_64
c8g.12xlarge	arm64
c8g.16xlarge	arm64
c8g.24xlarge	arm64
c8g.48xlarge	arm64
c8g.metal-24xl	arm64

Tipe instans	Arsitektur
c8g.metal-48xl	arm64
c8gb.8xlarge	arm64
c8gb.12xlarge	arm64
c8gb.16xlarge	arm64
c8gb.24xlarge	arm64
c8gb.48xlarge	arm64
c8gb.metal-24xl	arm64
c8gb.metal-48xl	arm64
c8gd.12xlarge	arm64
c8gd.16xlarge	arm64
c8gd.24xlarge	arm64
c8gd.48xlarge	arm64
c8gd.metal-24xl	arm64
c8gd.metal-48xl	arm64
c8gn.8xlarge	arm64
c8gn.12xlarge	arm64
c8gn.16xlarge	arm64
c8gn.24xlarge	arm64
c8gn.48xlarge	arm64
c8gn.metal-24xl	arm64

Tipe instans	Arsitektur
c8gn.metal-48xl	arm64
c8i.24xlarge	x86_64
c8i.32xlarge	x86_64
c8i.48xlarge	x86_64
c8i.96xlarge	x86_64
c8i.metal-48xl	x86_64
c8i.metal-96xl	x86_64
c8id.24xlarge	x86_64
c8id.32xlarge	x86_64
c8id.48xlarge	x86_64
c8id.96xlarge	x86_64
c8id.metal-48xl	x86_64
c8id.metal-96xl	x86_64

Memory optimized

Tipe instans	Arsitektur
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64

Tipe instans	Arsitektur
r6a.48xlarge	x86_64
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r6idn.8xlarge	x86_64
r6idn.12xlarge	x86_64
r6idn.16xlarge	x86_64
r6idn.24xlarge	x86_64
r6idn.32xlarge	x86_64
r6idn.metal	x86_64

Tipe instans	Arsitektur
r6in.8xlarge	x86_64
r6in.12xlarge	x86_64
r6in.16xlarge	x86_64
r6in.24xlarge	x86_64
r6in.32xlarge	x86_64
r6in.metal	x86_64
r7a.12xlarge	x86_64
r7a.16xlarge	x86_64
r7a.24xlarge	x86_64
r7a.32xlarge	x86_64
r7a.48xlarge	x86_64
r7a.metal-48xl	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64
r7i.16xlarge	x86_64

Tipe instans	Arsitektur
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64
r7iz.8xlarge	x86_64
r7iz.12xlarge	x86_64
r7iz.16xlarge	x86_64
r7iz.32xlarge	x86_64
r7iz.metal-16xl	x86_64
r7iz.metal-32xl	x86_64
r8a.16xlarge	x86_64
r8a.24xlarge	x86_64
r8a.48xlarge	x86_64
r8a.metal-24xl	x86_64
r8a.metal-48xl	x86_64
r8g.12xlarge	arm64
r8g.16xlarge	arm64
r8g.24xlarge	arm64
r8g.48xlarge	arm64
r8g.metal-24xl	arm64

Tipe instans	Arsitektur
r8g.metal-48xl	arm64
r8gb.8xlarge	arm64
r8gb.12xlarge	arm64
r8gb.16xlarge	arm64
r8gb.24xlarge	arm64
r8gb.48xlarge	arm64
r8gb.metal-24xl	arm64
r8gb.metal-48xl	arm64
r8gd.12xlarge	arm64
r8gd.16xlarge	arm64
r8gd.24xlarge	arm64
r8gd.48xlarge	arm64
r8gd.metal-24xl	arm64
r8gd.metal-48xl	arm64
r8gn.8xlarge	arm64
r8gn.12xlarge	arm64
r8gn.16xlarge	arm64
r8gn.24xlarge	arm64
r8gn.48xlarge	arm64
r8gn.metal-24xl	arm64

Tipe instans	Arsitektur
r8gn.metal-48xl	arm64
r8i.24xlarge	x86_64
r8i.32xlarge	x86_64
r8i.48xlarge	x86_64
r8i.96xlarge	x86_64
r8i.metal-48xl	x86_64
r8i.metal-96xl	x86_64
r8id.24xlarge	x86_64
r8id.32xlarge	x86_64
r8id.48xlarge	x86_64
r8id.96xlarge	x86_64
r8id.metal-48xl	x86_64
r8id.metal-96xl	x86_64
u7i-6tb.112xlarge	x86_64
u7i-8tb.112xlarge	x86_64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
u7inh-32tb.480xlarge	x86_64

Tipe instans	Arsitektur
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64
x8g.12xlarge	arm64
x8g.16xlarge	arm64
x8g.24xlarge	arm64
x8g.48xlarge	arm64
x8g.metal-24xl	arm64
x8g.metal-48xl	arm64
x8aedz.24xlarge	x86_64
x8aedz.metal-24xl	x86_64
x8i.24xlarge	x86_64
x8i.32xlarge	x86_64
x8i.48xlarge	x86_64

Tipe instans	Arsitektur
x8i.64xlarge	x86_64
x8i.96xlarge	x86_64
x8i.metal-48xl	x86_64
x8i.metal-96xl	x86_64

Accelerated computing

Tipe instans	Arsitektur
g6.48xlarge	x86_64
g6e.12xlarge	x86_64
g6e.24xlarge	x86_64
g6e.48xlarge	x86_64
g7e.12xlarge	x86_64
g7e.24xlarge	x86_64
g7e.48xlarge	x86_64
p5.4xlarge	x86_64
p5.48xlarge	x86_64
p5e.48xlarge	x86_64
p5en.48xlarge	x86_64
p6-b200.48xlarge	x86_64
p6-b300.48xlarge	x86_64

Storage optimized

Tipe instans	Arsitektur
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64
i7i.12xlarge	x86_64
i7i.16xlarge	x86_64
i7i.24xlarge	x86_64
i7i.48xlarge	x86_64
i7i.metal-24xl	x86_64
i7i.metal-48xl	x86_64
i7ie.12xlarge	x86_64
i7ie.18xlarge	x86_64
i7ie.24xlarge	x86_64
i7ie.48xlarge	x86_64

Tipe instans	Arsitektur
i7ie.metal-24xl	x86_64
i7ie.metal-48xl	x86_64
i8g.12xlarge	arm64
i8g.16xlarge	arm64
i8g.24xlarge	arm64
i8g.48xlarge	arm64
i8g.metal-24xl	arm64
i8g.metal-48xl	arm64
i8ge.12xlarge	arm64
i8ge.18xlarge	arm64
i8ge.24xlarge	arm64
i8ge.48xlarge	arm64
i8ge.metal-24xl	arm64
i8ge.metal-48xl	arm64
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Prasyarat untuk instance Linux

Untuk memastikan bahwa ENA Express dapat beroperasi secara efektif, perbarui pengaturan untuk instance Linux Anda sebagai berikut.

- Jika instans Anda menggunakan bingkai jumbo, jalankan perintah berikut untuk menyetel unit transmisi maksimum (MTU) ke 8900

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Tingkatkan ukuran cincin penerima (Rx), sebagai berikut:

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Untuk memaksimalkan bandwidth ENA Ekspres, konfigurasikan batas antrean TCP Anda sebagai berikut:

  1. Tetapkan batas antrean kecil TCP ke 1MB atau lebih tinggi. Ini meningkatkan jumlah data yang antri untuk transmisi pada soket.

     ```
     sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
     ```

  2. Nonaktifkan batas antrean byte pada perangkat eth jika diaktifkan untuk distribusi Linux Anda. Ini meningkatkan antrean data untuk transmisi untuk antrian perangkat.

     ```
     sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/
     byte_queue_limits/limit_min; done'
     ```

     > **Note**
     >
     > Driver ENA untuk distribusi Amazon Linux menonaktifkan batas antrean byte secara default.

- Untuk meminimalkan latensi lalu lintas TCP ENA Express, Anda dapat menonaktifkan fitur autocorking TCP. Hal ini dapat mengakibatkan peningkatan minimal dalam paket overhead:

```
sudo bash -c 'echo 0 > /proc/sys/net/ipv4/tcp_autocorking'
```

Menyetel kinerja untuk pengaturan ENA Express pada instans Linux

Untuk memeriksa konfigurasi instans Linux Anda untuk kinerja ENA Express yang optimal, Anda dapat menjalankan skrip berikut yang tersedia di GitHub repositori Amazon:

https://github.com/amzn/amzn-ec2-ena- - .sh utilities/blob/main/ena-express/check ena-express-settings

Skrip menjalankan serangkaian tes dan menyarankan perubahan konfigurasi yang direkomendasikan dan yang diperlukan.

Tinjau pengaturan ENA Express untuk instans EC2 Anda

Anda dapat memverifikasi pengaturan ENA Express dengan contoh atau dengan antarmuka jaringan. Untuk memperbarui pengaturan ENA Express, lihatthe section called “Konfigurasikan pengaturan instans”.

Console

Untuk melihat pengaturan ENA Express untuk antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Antarmuka jaringan.
3. Pilih antarmuka jaringan untuk melihat detail untuk instans itu. Anda dapat memilih tautan ID antarmuka Jaringan untuk membuka halaman detail, atau Anda dapat memilih kotak centang di sisi kiri daftar.
4. Di bagian lampiran antarmuka Jaringan pada tab Detail atau halaman detail, tinjau pengaturan untuk ENA Express dan ENA Express UDP.

Untuk melihat pengaturan ENA Express untuk sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans.
3. Pilih instans untuk melihat detail untuk instans itu. Anda dapat memilih tautan ID Instans untuk membuka halaman detail, atau Anda dapat memilih kotak centang di sisi kiri daftar untuk melihat detail di panel detail di bagian bawah halaman.
4. Di bagian Antarmuka jaringan pada tab Jaringan, gulir ke kanan untuk meninjau pengaturan untuk ENA Ekspres dan UDP ENA Ekspres.

AWS CLI

Untuk mendapatkan pengaturan ENA Express untuk sebuah instance

Gunakan perintah describe-instances. Contoh perintah ini mengembalikan daftar konfigurasi ENA Express untuk antarmuka jaringan yang dilampirkan ke masing-masing instance yang berjalan yang ditentukan oleh parameter. `--instance-ids`

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7 \
    --query 'Reservations[*].Instances[*].[InstanceId,
 NetworkInterfaces[*].Attachment.EnaSrdSpecification]'
```

Berikut ini adalah output contoh.

```
[
    [
        [
            "i-1234567890abcdef0",
            [
                {
                    "EnaSrdEnabled": true,
                    "EnaSrdUdpSpecification": {
                        "EnaSrdUdpEnabled": false
                    }
                }
            ]
        ]
    ],
    [
        [
            "i-0598c7d356eba48d7",
            [
            {
                    "EnaSrdEnabled": true,
                    "EnaSrdUdpSpecification": {
                        "EnaSrdUdpEnabled": false
                    }
                }
            ]
        ]
    ]
]
```

Untuk mendapatkan pengaturan ENA Express untuk antarmuka jaringan

Gunakan perintah describe-network-interfaces.

```
aws ec2 describe-network-interfaces \
    --network-interface-ids eni-1234567890abcdef0 \
    --query NetworkInterfaces[].[NetworkInterfaceId,Attachment.EnaSrdSpecification]
```

Berikut ini adalah output contoh.

```
[
    [
        "eni-1234567890abcdef0",
        {
            "EnaSrdEnabled": true,
            "EnaSrdUdpSpecification": {
                "EnaSrdUdpEnabled": false
            }
        }
    ]
]
```

PowerShell

Untuk mendapatkan pengaturan ENA Express untuk antarmuka jaringan

Gunakan Get-EC2NetworkInterfacecmdlet.

```
Get-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
```

```
    @{Name = 'EnaSrdUdpEnabled'; Expression =
{ $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }
```

Berikut ini adalah output contoh.

```
Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex    : 0
InstanceId          : i-1234567890abcdef0
InstanceOwnerId     : 111122223333
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Konfigurasikan pengaturan ENA Express untuk instans EC2 Anda

Anda dapat mengonfigurasi ENA Ekspres untuk tipe instans EC2 yang didukung tanpa perlu menginstal perangkat lunak tambahan apa pun. Untuk informasi selengkapnya, lihat the section called “Tipe instans yang didukung untuk ENA Ekspres”.

Console

Untuk mengelola ENA Express untuk antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Antarmuka jaringan.
3. Pilih antarmuka jaringan yang dilampirkan ke sebuah instans. Anda dapat memilih tautan ID antarmuka Jaringan untuk membuka halaman detail, atau Anda dapat memilih kotak centang di sisi kiri daftar.
4. Pilih Kelola ENA Ekspres dari menu Tindakan di sisi kanan atas halaman. Ini membuka dialog Kelola ENA Ekspres, dengan ID antarmuka jaringan yang dipilih dan pengaturan saat ini ditampilkan.

   Jika antarmuka jaringan yang Anda pilih tidak dilampirkan ke sebuah instans, tindakan ini tidak muncul di menu.

5. Untuk menggunakan ENA Express, pilih kotak centang Aktifkan.
6. Ketika ENA Ekspres diaktifkan, Anda dapat mengonfigurasi pengaturan UDP. Untuk menggunakan ENA Express UDP, pilih kotak centang Aktifkan.
7. Untuk menyimpan pengaturan Anda, pilih Simpan.

Untuk mengelola ENA Express sebagai contoh

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans.
3. Pilih instans yang ingin Anda kelola. Anda dapat memilih ID Instans untuk membuka halaman detail, atau Anda dapat memilih kotak centang di sisi kiri daftar.
4. Pilih antarmuka Jaringan yang akan dikonfigurasi untuk instans Anda.
5. Pilih Kelola ENA Ekspres dari menu Tindakan di sisi kanan atas halaman.
6. Untuk mengonfigurasi ENA Ekspres untuk antarmuka jaringan yang dilampirkan ke instans Anda, pilih dari daftar antarmuka Jaringan.
7. Untuk menggunakan ENA Express untuk lampiran antarmuka jaringan yang dipilih, pilih kotak centang Aktifkan.
8. Ketika ENA Ekspres diaktifkan, Anda dapat mengonfigurasi pengaturan UDP. Untuk menggunakan ENA Express UDP, pilih kotak centang Aktifkan.
9. Untuk menyimpan pengaturan Anda, pilih Simpan.

Untuk mengkonfigurasi ENA Express saat Anda melampirkan antarmuka jaringan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Antarmuka jaringan.
3. Pilih antarmuka jaringan yang tidak dilampirkan ke instans (Status Tersedia). Anda dapat memilih tautan ID antarmuka Jaringan untuk membuka halaman detail, atau Anda dapat memilih kotak centang di sisi kiri daftar.
4. Pilih Instans yang akan Anda lampirkan.
5. Untuk menggunakan ENA Express setelah Anda melampirkan antarmuka jaringan ke instance, pilih kotak centang Aktifkan.
6. Ketika ENA Ekspres diaktifkan, Anda dapat mengonfigurasi pengaturan UDP. Untuk menggunakan ENA Express UDP, pilih kotak centang Aktifkan.

7. Untuk melampirkan antarmuka jaringan ke instans dan menyimpan pengaturan ENA Ekspres Anda, pilih Lampirkan.

AWS CLI

Untuk mengkonfigurasi ENA Express saat Anda melampirkan antarmuka jaringan

Gunakan attach-network-interfaceperintah, seperti yang ditunjukkan pada contoh berikut.

Contoh 1: Gunakan ENA Express untuk lalu lintas TCP, tetapi tidak lalu lintas UDP

Contoh ini mengkonfigurasi `EnaSrdEnabled` sebagai`true`, dan memungkinkan `EnaSrdUdpEnabled` untuk default `kefalse`.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1 \
    --ena-srd-specification 'EnaSrdEnabled=true'
```

Contoh 2: Gunakan ENA Ekspres untuk lalu lintas TCP dan lalu lintas UDP

Contoh ini mengkonfigurasi keduanya `EnaSrdEnabled` dan `EnaSrdUdpEnabled` sebagai`true`.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1 \
    --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Untuk memperbarui pengaturan ENA Express untuk lampiran antarmuka jaringan

Gunakan modify-network-interface-attributeperintah seperti yang ditunjukkan pada contoh berikut.

Contoh 1: Gunakan ENA Express untuk lalu lintas TCP, tetapi tidak lalu lintas UDP

Contoh ini mengkonfigurasi `EnaSrdEnabled` sebagai`true`, dan memungkinkan `EnaSrdUdpEnabled` untuk default `false` jika belum pernah disetel sebelumnya.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
```

```
    --ena-srd-specification 'EnaSrdEnabled=true'
```

Contoh 2: Gunakan ENA Ekspres untuk lalu lintas TCP dan lalu lintas UDP

Contoh ini mengkonfigurasi keduanya `EnaSrdEnabled` dan `EnaSrdUdpEnabled` sebagai`true`.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Contoh 3: Berhenti menggunakan ENA Ekspres untuk lalu lintas UDP

Contoh ini mengkonfigurasi `EnaSrdUdpEnabled` sebagai`false`.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Untuk mengkonfigurasi ENA Express saat Anda melampirkan antarmuka jaringan

Gunakan Add-EC2NetworkInterfacecmdlet seperti yang ditunjukkan pada contoh berikut.

Contoh 1: Gunakan ENA Express untuk lalu lintas TCP, tetapi tidak lalu lintas UDP

Contoh ini mengkonfigurasi `EnaSrdEnabled` sebagai`true`, dan memungkinkan `EnaSrdUdpEnabled` untuk default ke`false`.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1 `
    -EnaSrdSpecification_EnaSrdEnabled $true
```

Contoh 2: Gunakan ENA Ekspres untuk lalu lintas TCP dan lalu lintas UDP

Contoh ini mengkonfigurasi keduanya `EnaSrdEnabled` dan `EnaSrdUdpEnabled` sebagai`true`.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
```

```
    -DeviceIndex 1 `
    -EnaSrdSpecification_EnaSrdEnabled $true `
    -EnaSrdUdpSpecification_EnaSrdUdpEnabled $true
```

Untuk mengonfigurasi pengaturan ENA Express untuk lampiran antarmuka jaringan Anda

Gunakan Edit-EC2NetworkInterfaceAttributecmdlet seperti yang ditunjukkan pada contoh berikut.

Contoh 1: Gunakan ENA Express untuk lalu lintas TCP, tetapi tidak lalu lintas UDP

Contoh ini mengkonfigurasi `EnaSrdEnabled` sebagai`true`, dan memungkinkan `EnaSrdUdpEnabled` untuk default `false` jika belum pernah disetel sebelumnya.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Contoh 2: Gunakan ENA Ekspres untuk lalu lintas TCP dan lalu lintas UDP

Contoh ini mengkonfigurasi keduanya `EnaSrdEnabled` dan `EnaSrdUdpEnabled` sebagai`true`.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -EnaSrdSpecification_EnaSrdEnabled $true `
    -EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-1234567890abcdef0 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Contoh 3: Berhenti menggunakan ENA Ekspres untuk lalu lintas UDP

Contoh ini mengkonfigurasi `EnaSrdUdpEnabled` sebagai`false`.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-0123f4567890a1b23 `
    -EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Konfigurasikan ENA Express saat peluncuran

Anda dapat menggunakan salah satu metode berikut untuk mengkonfigurasi ENA Express secara langsung ketika Anda meluncurkan sebuah instance. Tautan yang ditentukan merujuk Anda ke Konsol Manajemen AWS instruksi untuk metode ini.

- Launch instance wizard - Anda dapat mengonfigurasi ENA Express saat peluncuran dengan wizard instance peluncuran. Untuk informasi selengkapnya, lihat Konfigurasi jaringan lanjutan di wizard Pengaturan jaringan untuk instance peluncuran.
- Peluncuran template - Anda dapat mengkonfigurasi ENA Express saat peluncuran ketika Anda menggunakan template peluncuran. Untuk informasi selengkapnya, lihat Buat template peluncuran Amazon EC2 halaman, lalu perluas bagian Pengaturan jaringan dan tinjau konfigurasi jaringan lanjutan.

Jaringan yang disempurnakan dengan antarmuka Intel 82599 VF

Untuk instance berbasis Xen, antarmuka Intel 82599 Virtual Function (VF) menyediakan kemampuan jaringan yang ditingkatkan. Antarmuka menggunakan `ixgbevf` driver Intel.

Tab berikut menunjukkan cara memverifikasi driver adaptor jaringan yang diinstal untuk sistem operasi instans Anda.

Linux

Driver antarmuka jaringan Linux

Gunakan perintah berikut untuk memverifikasi apakah modul sedang digunakan pada antarmuka tertentu, menggantikan nama antarmuka yang ingin Anda periksa. Jika Anda menggunakan antarmuka tunggal (default), ini adalah `eth0`. Jika sistem operasi mendukung nama jaringan yang dapat diprediksi, ini bisa menjadi nama seperti `ens5`.

Dalam contoh berikut, modul `ixgbevf` tidak dimuat, karena driver yang terdaftar adalah `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Dalam contoh ini, modul `ixgbevf` dimuat. Instans ini memiliki jaringan yang ditingkatkan, yang dikonfigurasi dengan benar.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Windows

Adaptor jaringan Windows

Untuk memverifikasi bahwa driver telah diinstal, sambungkan ke instans Anda dan buka Pengelola Perangkat. Anda akan melihat `Intel(R) 82599 Virtual Function` tercantum di bawah Adaptor jaringan.

Daftar Isi

- Siapkan instans Anda untuk jaringan yang disempurnakan
- Menguji apakah jaringan yang ditingkatkan diaktifkan
- Mengaktifkan jaringan yang ditingkatkan pada instans Anda
- Memecahkan masalah konektivitas

Siapkan instans Anda untuk jaringan yang disempurnakan

Untuk mempersiapkan jaringan yang ditingkatkan menggunakan antarmuka Intel 82599 VF, siapkan instans Anda sebagai berikut:

- Verifikasi bahwa jenis instans adalah salah satu dari yang berikut: C3, C4, D2, I2, M4 (tidak termasuk`m4.16xlarge`), dan R3.
- Pastikan instans tersebut memiliki konektivitas internet.
- Jika memiliki data penting pada instans yang ingin Anda pertahankan, Anda harus melakukan back up data tersebut sekarang dengan membuat AMI dari instans Anda. Memperbarui kernel dan modul kernel, serta mengaktifkan atribut `sriovNetSupport`, dapat menyebabkan instans yang tidak kompatibel atau sistem operasi tidak dapat dijangkau. Jika Anda memiliki back up terbaru, data Anda akan tetap disimpan jika hal ini terjadi.
- Instance Linux — Luncurkan instance dari AMI HVM menggunakan kernel Linux versi 2.6.32 atau yang lebih baru. Amazon Linux HVM terbaru AMIs memiliki modul yang diperlukan untuk jaringan yang ditingkatkan diinstal dan memiliki atribut yang diperlukan ditetapkan. Oleh karena itu, jika Anda meluncurkan instans yang didukung Amazon EBS dan jaringan yang ditingkatkan menggunakan AMI HVM Amazon Linux saat ini, jaringan yang ditingkatkan telah diaktifkan untuk instans Anda.

  > **Warning**
  >
  > Jaringan yang ditingkatkan hanya didukung untuk instans HVM. Mengaktifkan jaringan yang ditingkatkan dengan instans PV bisa menjadikannya tidak dapat dijangkau. Mengatur atribut ini tanpa modul yang tepat atau versi modul juga bisa membuat instans Anda tidak dapat dijangkau.

- Instans Windows — Luncurkan instance dari AMI HVM 64-bit. Anda tidak dapat mengaktifkan jaringan yang disempurnakan di Windows Server 2008. Jaringan yang disempurnakan sudah diaktifkan untuk Windows Server 2012 R2 dan Windows Server 2016 dan yang lebih baru

AMIs. Windows Server 2012 R2 menyertakan driver Intel 1.0.15.3 dan kami menyarankan Anda memperbarui driver tersebut ke versi terbaru menggunakan utilitas Pnputil.exe.

- Gunakan AWS CloudShelldari Konsol Manajemen AWS, atau instal dan konfigurasikan AWS CLIatau AWS Tools for Windows PowerShelldi komputer mana pun yang Anda pilih, sebaiknya desktop atau laptop lokal Anda. Untuk informasi selengkapnya, lihat Akses Amazon EC2 atau Panduan Pengguna AWS CloudShell. Jaringan yang ditingkatkan tidak dapat dikelola dari konsol Amazon EC2.

Menguji apakah jaringan yang ditingkatkan diaktifkan

Verifikasi bahwa `sriovNetSupport` atribut diatur pada instance atau gambar.

AWS CLI

Untuk memeriksa atribut instance (sriovNetSupport)

Gunakan perintah berikut describe-instance-attribute. Jika atribut diatur, nilainya adalah`simple`.

```
aws ec2 describe-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --attribute sriovNetSupport
```

Untuk memeriksa atribut image (sriovNetSupport)

Gunakan perintah berikut describe-images. Jika atribut diatur, nilainya adalah`simple`.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query "Images[].SriovNetSupport"
```

PowerShell

Untuk memeriksa atribut instance (sriovNetSupport)

Gunakan Get-EC2InstanceAttributecmdlet. Jika atribut diatur, nilainya adalah`simple`.

```
Get-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -Attribute sriovNetSupport
```

Untuk memeriksa atribut image (sriovNetSupport)

Gunakan perintah berikut describe-images. Jika atribut diatur, nilainya adalah`simple`.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).SriovNetSupport
```

Mengaktifkan jaringan yang ditingkatkan pada instans Anda

Prosedur yang Anda gunakan tergantung pada sistem operasi instance.

> **Warning**
>
> Tidak ada cara untuk menonaktifkan atribut jaringan yang ditingkatkan setelah Anda mengaktifkannya.

Amazon Linux

Amazon Linux HVM terbaru AMIs memiliki `ixgbevf` modul yang diperlukan untuk jaringan yang ditingkatkan diinstal dan memiliki set `sriovNetSupport` atribut yang diperlukan. Oleh karena itu, jika Anda meluncurkan tipe instans menggunakan AMI HVM Amazon Linux saat ini, jaringan yang ditingkatkan telah diaktifkan untuk instans Anda. Untuk informasi selengkapnya, lihat Menguji apakah jaringan yang ditingkatkan diaktifkan.

Jika Anda meluncurkan instans menggunakan AMI Amazon Linux versi lama dan jaringan yang ditingkatkan belum diaktifkan, gunakan prosedur berikut untuk mengaktifkan jaringan yang ditingkatkan.

Untuk mengaktifkan jaringan yang ditingkatkan

1. Terhubung ke instans Anda.
2. Dari instans, jalankan perintah berikut untuk memperbarui instans Anda dengan modul kernel dan kernel terbaru, termasuk `ixgbevf`:

   ```
   [ec2-user ~]$ sudo yum update
   ```
3. Dari komputer lokal Anda, reboot instans Anda menggunakan konsol Amazon EC2 atau salah satu perintah berikut: reboot-instances(AWS CLI) atau Restart-EC2Instance(AWS Tools for Windows PowerShell).

4. Hubungkan lagi ke instans Anda dan verifikasi bahwa modul `ixgbevf` telah diinstal dan pada versi minimum yang disarankan menggunakan perintah modinfo ixgbevf dari Menguji apakah jaringan yang ditingkatkan diaktifkan.
5. [Instans yang didukung EBS] Dari komputer lokal Anda, hentikan instans menggunakan konsol Amazon EC2 atau salah satu perintah berikut stop-instances:AWS CLI() atau () Stop-EC2Instance.AWS Tools for Windows PowerShell

   [Instans yang didukung penyimpanan instans] Anda tidak dapat menghentikan instans untuk memodifikasi atribut. Sebagai gantinya, lewati ke prosedur selanjutnya.
6. Dari komputer lokal Anda, aktifkan atribut jaringan yang ditingkatkan menggunakan salah satu dari perintah berikut ini:

   AWS CLI

   Gunakan perintah modify-instance-attribute sebagai berikut.

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 \
       --sriov-net-support simple
   ```

   PowerShell

   Gunakan Edit-EC2InstanceAttributecmdlet sebagai berikut.

   ```
   Edit-EC2InstanceAttribute `
       -InstanceId i-1234567890abcdef0 `
       -SriovNetSupport "simple"
   ```
7. (Opsional) Buat AMI dari instans, seperti yang dijelaskan di Buat AMI yang didukung Amazon EBS-Backed. AMI mewarisi atribut jaringan yang ditingkatkan dari instans. Oleh karena itu, Anda dapat menggunakan AMI ini untuk meluncurkan instans lain dengan jaringan yang ditingkatkan diaktifkan secara default.
8. Dari komputer lokal Anda, mulai instance menggunakan konsol Amazon EC2 atau salah satu perintah berikut: start-instances(AWS CLI) atau Start-EC2Instance(AWS Tools for Windows PowerShell).
9. Hubungkan ke instans Anda dan verifikasi bahwa modul `ixgbevf` diinstal dan dimuat di antarmuka jaringan Anda menggunakan perintah ethtool -i eth***n*** dari Menguji apakah jaringan yang ditingkatkan diaktifkan.

Untuk mengaktifkan jaringan yang ditingkatkan (instans yang didukung penyimpanan instans)

Ikuti prosedur sebelumnya hingga langkah tempat Anda menghentikan instans. Buat AMI baru seperti yang dijelaskan di Buat AMI yang didukung Amazon S3, pastikan untuk mengaktifkan atribut jaringan yang ditingkatkan saat Anda mendaftarkan AMI.

AWS CLI

Gunakan perintah register-image sebagai berikut.

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Gunakan Register-EC2Imagesebagai berikut.

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Sebelum Anda mulai, periksa apakah jaringan yang ditingkatkan telah diaktifkan pada instans Anda.

Quick Start Ubuntu HVM AMIs menyertakan driver yang diperlukan untuk meningkatkan jaringan. Jika Anda memiliki versi `ixgbevf` yang lebih lama dari 2.16.4, Anda dapat menginstal paket kernel `linux-aws` untuk mendapatkan driver jaringan terbaru yang ditingkatkan.

Prosedur berikut menyediakan langkah-langkah umum untuk mengompilasi modul `ixgbevf` pada instans Ubuntu.

Untuk menginstal **`linux-aws`** paket kernel

1. Connect ke instans Anda.
2. Perbarui cache paket dan paket.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Jika selama proses update Anda diminta untuk menginstal `grub`, gunakan `/dev/xvda` untuk menginstal `grub`, lalu pilih untuk mempertahankan versi `/boot/grub/menu.lst` saat ini.

Distribusi Linux lainnya

Sebelum Anda mulai, periksa apakah jaringan yang ditingkatkan telah diaktifkan pada instans Anda. Quick Start HVM terbaru AMIs menyertakan driver yang diperlukan untuk jaringan yang ditingkatkan, oleh karena itu Anda tidak perlu melakukan langkah tambahan.

Prosedur berikut menyediakan langkah-langkah umum jika Anda perlu mengaktifkan jaringan yang ditingkatkan dengan antarmuka Intel 82599 VF pada distribusi Linux selain Amazon Linux atau Ubuntu. Untuk informasi selengkapnya, seperti detail sintaksis untuk perintah, lokasi file, atau paket dan dukungan alat, lihat dokumentasi khusus untuk distribusi Linux Anda.

Untuk mengaktifkan jaringan yang ditingkatkan di Linux

1. Terhubung ke instans Anda.
2. Unduh sumber `ixgbevf` modul pada instance Anda dari Sourceforge di https://sourceforge. net/projects/e1000/files/ixgbevf%20stabil/.

   Versi `ixgbevf` yang lebih lama dari 2.16.4, termasuk versi 2.14.2, tidak dibuat dengan benar pada beberapa distribusi Linux, termasuk versi Ubuntu tertentu.
3. Lakukan kompilasi dan instal modul `ixgbevf` pada instans Anda.

   > **Warning**
   >
   > Jika Anda mengompilasi modul `ixgbevf` untuk kernel Anda saat ini lalu mengupgrade kernel Anda tanpa membuat kembali driver untuk kernel baru, sistem Anda mungkin akan kembali ke modul `ixgbevf` khusus distribusi pada boot ulang berikutnya. Ini dapat membuat sistem Anda tidak dapat dijangkau jika versi khusus distribusi tidak kompatibel dengan jaringan yang ditingkatkan.
4. Jalankan perintah sudo depmod untuk memperbarui dependensi modul.

5. Perbarui `initramfs` pada instans Anda untuk memastikan bahwa modul baru dimuat pada saat boot.
6. Tentukan apakah sistem Anda menggunakan nama antarmuka jaringan yang dapat diprediksi secara default. Sistem yang menggunakan systemd atau udev versi 197 atau lebih tinggi dapat mengganti nama perangkat Ethernet dan tidak menjamin bahwa satu antarmuka jaringan akan dinamai `eth0`. Perilaku ini dapat menyebabkan masalah saat terhubung ke instans Anda. Untuk informasi lebih lanjut dan untuk melihat opsi konfigurasi lainnya, lihat Nama Antarmuka Jaringan yang Dapat Diprediksi di situs web freedesktop.org.

   a. Anda dapat memeriksa versi systemd atau udev pada sistem berbasis RPM dengan perintah berikut:

   ```
   [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
       systemd-208-11.el7_0.2.x86_64
   ```

   Dalam contoh Red Hat Enterprise Linux 7 di atas, versi systemd adalah 208, jadi nama antarmuka jaringan yang dapat diprediksi harus dinonaktifkan.

   b. Nonaktifkan nama antarmuka jaringan yang dapat diprediksi dengan menambahkan opsi `net.ifnames=0` ke baris `GRUB_CMDLINE_LINUX` di `/etc/default/grub`.

   ```
   [ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /
   etc/default/grub
   ```

   c. Buat ulang file konfigurasi grub.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. [Instans yang didukung EBS] Dari komputer lokal Anda, hentikan instans menggunakan konsol Amazon EC2 atau salah satu perintah berikut: stop-instance AWS CLI() atau (). Stop-EC2InstanceAWS Tools for Windows PowerShell

   [Instans yang didukung penyimpanan instans] Anda tidak dapat menghentikan instans untuk memodifikasi atribut. Sebagai gantinya, lewati ke prosedur selanjutnya.
8. Dari komputer lokal Anda, aktifkan atribut jaringan yang ditingkatkan menggunakan salah satu dari perintah berikut ini:

   AWS CLI

   Gunakan perintah modify-instance-attribute sebagai berikut.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 -\
    -sriov-net-support simple
```

PowerShell

Gunakan Edit-EC2InstanceAttributecmdlet sebagai berikut.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -SriovNetSupport "simple"
```

9. (Opsional) Buat AMI dari instans, seperti yang dijelaskan di Buat AMI yang didukung Amazon EBS-Backed. AMI mewarisi atribut jaringan yang ditingkatkan dari instans. Oleh karena itu, Anda dapat menggunakan AMI ini untuk meluncurkan instans lain dengan jaringan yang ditingkatkan diaktifkan secara default.

   Jika sistem operasi instans Anda berisi file `/etc/udev/rules.d/70-persistent-net.rules`, Anda harus menghapusnya sebelum membuat AMI. File ini berisi alamat MAC untuk adaptor Ethernet dari instans asli. Jika instans lain melakukan booting dengan file ini, sistem operasi tersebut `eth0` tidak akan dapat menemukan perangkat dan mungkin gagal, yang menyebabkan masalah booting. File ini dibuat ulang pada siklus boot berikutnya, dan setiap instans yang diluncurkan dari AMI membuat versi file mereka sendiri.
10. Dari komputer lokal Anda, mulai instance menggunakan konsol Amazon EC2 atau salah satu perintah berikut: start-instances(AWS CLI) atau Start-EC2Instance(AWS Tools for Windows PowerShell).
11. (Opsional) Hubungkan ke instans Anda dan verifikasi bahwa modul telah diinstal.

Untuk mengaktifkan jaringan yang ditingkatkan (instans yang didukung penyimpanan instans)

Ikuti prosedur sebelumnya hingga langkah tempat Anda menghentikan instans. Buat AMI baru seperti yang dijelaskan di Buat AMI yang didukung Amazon S3, pastikan untuk mengaktifkan atribut jaringan yang ditingkatkan saat Anda mendaftarkan AMI.

AWS CLI

Gunakan perintah register-image sebagai berikut.

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Gunakan Register-EC2Imagesebagai berikut.

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Jika Anda meluncurkan instans dan instans tersebut belum mengaktifkan jaringan yang ditingkatkan, Anda harus mengunduh dan menginstal driver adaptor jaringan yang diperlukan pada instans Anda, lalu menyetel atribut instans `sriovNetSupport` untuk mengaktifkan jaringan yang ditingkatkan. Anda hanya dapat mengaktifkan atribut ini pada tipe instans yang didukung. Untuk informasi selengkapnya, lihat Jaringan yang disempurnakan di EC2 instans Amazon.

Important

Untuk melihat pembaruan driver terbaru di Windows AMIs, lihat riwayat versi Windows AMI di Referensi AMI AWS Windows.

Untuk mengaktifkan jaringan yang ditingkatkan

1. Hubungkan ke instans Anda dan masuk sebagai administrator lokal.
2. [Windows Server 2016 dan yang lebih baru] Jalankan PowerShell skrip Peluncuran EC2 berikut untuk mengonfigurasi instance setelah driver diinstal.

   ```
   PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
   Schedule
   ```

   Important

   Kata sandi administrator akan diatur ulang ketika Anda mengaktifkan skrip EC2Launch inisialisasi instans. Anda dapat memodifikasi file konfigurasi untuk menonaktifkan pengaturan ulang kata sandi administrator dengan menentukannya di pengaturan untuk tugas inisialisasi.

3. Dari instans, unduh driver adaptor jaringan Intel untuk sistem operasi Anda:

   - Windows Server 2022

     Kunjungi halaman unduh dan unduh `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2019 termasuk untuk Server versi 1809 dan yang lebih baru*

     Kunjungi halaman unduh dan unduh `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2016 termasuk untuk Server versi 1803 dan sebelumnya*

     Kunjungi halaman unduh dan unduh `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2012 R2

     Kunjungi halaman unduh dan unduh `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2012

     Kunjungi halaman unduh dan unduh `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2008 R2

     Kunjungi halaman unduh dan unduh `PROWinx64Legacy.exe`.

   *Server versi 1803 dan sebelumnya serta 1809 dan yang lebih baru tidak secara khusus ditujukan pada halaman Driver dan Software Intel.
4. Instal driver adaptor jaringan Intel untuk sistem operasi Anda.

   - Windows Server 2008 R2
     1. Di folder Unduh, cari file `PROWinx64Legacy.exe` dan namakan `PROWinx64Legacy.zip`.
     2. Ekstrak isi file `PROWinx64Legacy.zip` tersebut.
     3. Buka baris perintah, navigasi ke folder yang diekstrak, dan jalankan perintah berikut untuk menggunakan utilitas `pnputil` untuk menambahkan dan menginstal file INF di penyimpanan driver.

        ```
        C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
        ```
   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, dan Windows Server 2012
     1. Di folder Unduhan, ekstrak isi file `Wired_driver_`*`version`*`_x64.zip` tersebut.

2. Buka baris perintah, navigasi ke folder yang diekstrak, dan jalankan perintah berikut untuk menggunakan utilitas `pnputil` untuk menambahkan dan menginstal file INF di penyimpanan driver.

   - Windows Server 2022

     ```
     pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
     ```

   - Windows Server 2019

     ```
     pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
     ```

   - Windows Server 2016

     ```
     pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
     ```

   - Windows Server 2012 R2

     ```
     pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
     ```

   - Windows Server 2012

     ```
     pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
     ```

5. Dari komputer lokal Anda, aktifkan atribut jaringan yang ditingkatkan menggunakan salah satu dari perintah berikut ini:

   AWS CLI

   Gunakan perintah modify-instance-attribute sebagai berikut.

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 \
       --sriov-net-support simple
   ```

   PowerShell

   Gunakan Edit-EC2InstanceAttributecmdlet sebagai berikut.

   ```
   Edit-EC2InstanceAttribute `
       -InstanceId i-1234567890abcdef0 `
   ```

```
    -SriovNetSupport "simple"
```

6. (Opsional) Buat AMI dari instans, seperti yang dijelaskan di Buat AMI yang didukung Amazon EBS-Backed. AMI mewarisi atribut jaringan yang ditingkatkan dari instans. Oleh karena itu, Anda dapat menggunakan AMI ini untuk meluncurkan instans lain dengan jaringan yang ditingkatkan diaktifkan secara default.
7. Dari komputer lokal Anda, mulai instance menggunakan konsol Amazon EC2 atau salah satu perintah berikut: start-instances(AWS CLI) atau Start-EC2Instance(AWS Tools for Windows PowerShell).

Memecahkan masalah konektivitas

Jika Anda kehilangan konektivitas saat mengaktifkan jaringan yang ditingkatkan, modul `ixgbevf` mungkin tidak kompatibel dengan kernel tersebut. Coba instal versi modul `ixgbevf` yang disertakan dengan distribusi Linux untuk instans Anda.

Jika Anda mengaktifkan jaringan yang ditingkatkan untuk instans PV atau AMI, ini dapat membuat instans Anda tidak dapat dijangkau.

Untuk informasi selengkapnya, lihat Bagaimana cara mengaktifkan dan mengonfigurasi jaringan yang disempurnakan pada instans EC2 saya?

Pantau kinerja jaringan untuk pengaturan ENA pada instans EC2 Anda

Driver Adaptor Jaringan Elastis (ENA) menerbitkan metrik performa jaringan dari instans di mana mereka diaktifkan. Anda dapat menggunakan metrik ini untuk memecahkan masalah performa instans, memilih ukuran instans yang tepat untuk beban kerja, rencana aktivitas penskalaan secara proaktif, dan aplikasi tolok ukur untuk menentukan apakah mereka memaksimalkan performa yang tersedia pada instans.

Amazon EC2 mendefinisikan maksimum jaringan pada tingkat instans untuk memastikan pengalaman jaringan berkualitas tinggi, termasuk kinerja jaringan yang konsisten di seluruh ukuran instans. AWS memberikan maksimum untuk hal-hal berikut untuk setiap contoh:

- Kemampuan bandwidth — Setiap instans EC2 memiliki bandwidth maksimum untuk mengumpulkan lalu lintas masuk dan keluar, berdasarkan tipe dan ukuran instans. Beberapa contoh menggunakan mekanisme I/O kredit jaringan untuk mengalokasikan bandwidth jaringan berdasarkan pemanfaatan bandwidth rata-rata. Amazon EC2 juga memiliki bandwidth maksimum

untuk lalu lintas ke Direct Connect dan internet. Untuk informasi selengkapnya, lihat Bandwidth jaringan EC2 instans Amazon.

- Packet-per-second Kinerja (PPS) - Setiap instans EC2 memiliki kinerja PPS maksimum, berdasarkan jenis dan ukuran instans.
- Koneksi dilacak — Grup keamanan melacak setiap sambungan yang dibuat untuk memastikan bahwa paket kembali dikirim seperti yang diharapkan. Ada jumlah maksimum koneksi yang dapat dilacak per instans. Untuk informasi selengkapnya, lihat Pelacakan koneksi grup keamanan Amazon EC2
- Akses layanan link-lokal — Amazon EC2 menyediakan PPS maksimum per antarmuka jaringan untuk lalu lintas ke layanan proxy lokal seperti layanan DNS Amazon, Layanan Metadata Instans, dan Layanan Sinkronisasi Waktu Amazon.

Ketika lalu lintas jaringan untuk suatu instance melebihi maksimum, AWS membentuk lalu lintas yang melebihi maksimum dengan mengantri dan kemudian menjatuhkan paket jaringan. Anda dapat memantau kapan lalu lintas melebihi maksimum menggunakan metrik performa jaringan. Metrik ini memberi tahu Anda, secara langsung, tentang dampak terhadap lalu lintas jaringan dan kemungkinan masalah performa jaringan.

Daftar Isi

- Persyaratan
- Metrik untuk driver ENA
- Melihat metrik performa jaringan untuk instans Anda
- Metrik untuk ENA Ekspres
- Metrik performa jaringan dengan driver DPDK untuk ENA
- Metrik pada instans yang berjalan FreeBSD

Persyaratan

Instans Linux

- Menginstal driver ENA versi 2.2.10 atau yang lebih baru. Untuk memverifikasi versi terinstal, gunakan perintah ethtool berikut. Dalam contoh berikut, versi memenuhi persyaratan minimum.

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

Untuk memperbarui driver ENA Anda, lihat Jaringan yang ditingkatkan.

- Untuk mengimpor metrik ini ke Amazon CloudWatch, instal CloudWatch agen. Untuk informasi selengkapnya, lihat Mengumpulkan metrik performa jaringan di Panduan CloudWatch Pengguna Amazon.
- Untuk mendukung `conntrack_allowance_available` metrik, instal driver ENA versi 2.8.1 atau yang lebih baru.
- Untuk mengganti batas PPS fragmen jalan keluar 1024, instal driver ENA versi 2.13.3 atau yang lebih baru.

Instans Windows

- Menginstal driver ENA versi 2.2.2 atau yang lebih baru. Untuk memverifikasi versi yang diinstal, gunakan Pengelola Perangkat sebagai berikut.
  1. Buka Pengelola Perangkat dengan menjalankan `devmgmt.msc`.
  2. Perluas Adaptor Jaringan.
  3. Pilih Amazon Elastic Network Adapter, Properti.
  4. Pada tab Driver, temukan Versi Driver.

  Untuk memperbarui driver ENA Anda, lihat Jaringan yang ditingkatkan.
- Untuk mengimpor metrik ini ke Amazon CloudWatch, instal CloudWatch agen. Untuk informasi selengkapnya, lihat Mengumpulkan metrik jaringan lanjutan di Panduan CloudWatch Pengguna Amazon.

Metrik untuk driver ENA

Driver ENA memberikan metrik berikut untuk instans secara langsung. Mereka menyediakan jumlah kumulatif paket antri atau dijatuhkan pada setiap antarmuka jaringan sejak driver terakhir diatur ulang.

Metrik	Deskripsi	Didukung pada
`bw_in_allowance_exceeded`	Jumlah paket antri atau dijatuhkan karena kumpulan bandwidth	Semua tipe instans

Metrik	Deskripsi	Didukung pada
	yang masuk melebihi maksimum untuk instans.	
bw_out_allowance_exceeded	Jumlah paket antre atau dijatuhkan karena bandwidth agregat yang keluar melebihi maksimum untuk instans.	Semua tipe instans
conntrack_allowance_exceeded	Jumlah paket turun karena pelacakan koneksi melebihi maksimum untuk instans dan koneksi baru tidak dapat dibuat. Hal ini dapat mengakibatkan hilangnya paket untuk lalu lintas ke atau dari instans.	Semua tipe instans
conntrack_allowance_available	Jumlah koneksi yang dilacak yang dapat dibuat oleh instans sebelum menekan tunjangan Connections Tracked dari tipe instans tersebut.	Hanya contoh berbasis nitro
linklocal_allowance_exceeded	Jumlah paket turun karena PPS lalu lintas ke layanan proksi lokal melebihi batas maksimum untuk antarmuka jaringan. Hal ini memengaruhi lalu lintas ke layanan DNS Amazon, Layanan Metadata Instans, dan Layanan Sinkronisasi Waktu Amazon, tetapi tidak memengaruhi lalu lintas ke resolver DNS khusus.	Semua tipe instans

Metrik	Deskripsi	Didukung pada
`pps_allowance_exceeded`	Jumlah paket mengantri atau turun karena PPS dua arah melebihi maksimum untuk instance. *	Semua tipe instans

* Tergantung pada pengaturan mode proxy fragmen untuk driver ENA Linux v2.13.3 atau yang lebih baru, batas ini juga dapat mencakup penurunan fragmen keluar yang melebihi 1024 PPS untuk antarmuka jaringan. Jika mode proxy fragmen diaktifkan untuk driver Linux, fragmen keluar turun melewati batas 1024 PPS yang biasanya berlaku dan dihitung dalam tunjangan PPS standar. Mode proxy fragmen dinonaktifkan secara default.

Melihat metrik performa jaringan untuk instans Anda

Prosedur yang Anda gunakan tergantung pada sistem operasi instance.

Instans Linux

Anda dapat menerbitkan metrik ke alat favorit Anda untuk memvisualisasikan data metrik. Misalnya, Anda dapat mempublikasikan metrik ke Amazon CloudWatch menggunakan CloudWatch agen. Agen memungkinkan Anda untuk memilih metrik individu dan mengendalikan publikasi.

Anda juga dapat menggunakan ethtool untuk mengambil metrik untuk setiap antarmuka jaringan, seperti eth0, sebagai berikut.

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

Instans Windows

Anda dapat melihat metrik menggunakan pengukur performa Windows. Data dapat diuraikan sesuai dengan EnaPerfCounters manifes. Ini adalah file XML yang menentukan penyedia pengukur performa dan rangkaian penghitungnya.

Untuk menginstal manifes

Jika Anda meluncurkan instans menggunakan AMI yang berisi driver ENA 2.2.2 atau yang lebih baru, atau menggunakan skrip instal dalam paket driver ENA 2.2.2, manifes sudah terinstal. Untuk menginstal manifes secara manual, gunakan langkah-langkah berikut:

1. Menghapus manifes yang ada menggunakan perintah berikut:

```
unlodctr /m:EnaPerfCounters.man
```

2. Salin file manifes `EnaPerfCounters.man` dari paket instalasi driver ke `%SystemRoot%\System32\drivers`.
3. Instal manifes baru menggunakan perintah berikut:

```
lodctr /m:EnaPerfCounters.man
```

Untuk melihat metrik menggunakan Performance Monitor

1. Buka Monitor Performa.
2. Tekan Ctrl+N untuk menambahkan penghitung baru.
3. Pilih ENA Packets Shaping dari daftar.
4. Pilih instans untuk memantau dan pilih Tambahkan.
5. Pilih OKE.

Metrik untuk ENA Ekspres

ENA Express didukung oleh teknologi AWS Scalable Reliable Datagram (SRD). SRD adalah protokol transportasi jaringan performa tinggi yang menggunakan perutean dinamis untuk meningkatkan throughput dan meminimalkan latensi ekor. Jika Anda telah mengaktifkan ENA Express untuk lampiran antarmuka jaringan pada instans pengirim dan instans penerima, Anda dapat menggunakan metrik ENA Express untuk membantu memastikan bahwa instans Anda memanfaatkan sepenuhnya peningkatan kinerja yang disediakan oleh teknologi SRD. Contoh:

- Evaluasi sumber daya Anda untuk memastikan bahwa mereka memiliki kapasitas yang cukup untuk membangun lebih banyak koneksi SRD.
- Identifikasi di mana ada potensi masalah yang mencegah paket keluar yang memenuhi syarat menggunakan SRD.

- Hitung persentase lalu lintas keluar yang menggunakan SRD untuk instans tersebut.
- Hitung persentase lalu lintas masuk yang menggunakan SRD untuk instans tersebut.

> **Note**
>
> Untuk menghasilkan metrik, gunakan driver versi 2.8 atau lebih tinggi.

Untuk melihat daftar metrik untuk instance Linux Anda yang difilter untuk ENA Express, jalankan ethtool perintah berikut untuk antarmuka jaringan Anda (ditampilkan di sini sebagai`eth0`). Perhatikan nilai `ena_srd_mode` metrik.

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 1
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

Metrik berikut tersedia untuk semua instance yang mengaktifkan ENA Express.

ena_srd_mode

Menjelaskan fitur ENA Express mana yang diaktifkan. Nilai adalah sebagai berikut:

- `0` = ENA Ekspres mati, UDP mati
- `1` = ENA Ekspres aktif, UDP mati
- `2` = ENA Ekspres mati, UDP aktif

> **Note**
>
> Ini hanya terjadi ketika ENA Ekspres awalnya diaktifkan, dan UDP dikonfigurasi untuk menggunakannya. Nilai sebelumnya dipertahankan untuk lalu lintas UDP.

- `3` = ENA Ekspres aktif, UDP aktif

ena_srd_eligible_tx_pkts

Jumlah jaringan sebagai berikut:

- Baik tipe instans pengiriman maupun penerimaan didukung. Lihat tabel Tipe instans yang didukung untuk ENA Ekspres untuk informasi selengkapnya.
- Instans pengiriman dan penerimaan harus memiliki ENA Ekspres yang dikonfigurasi.
- Instance pengiriman dan penerimaan harus berjalan di Availability Zone yang sama.
- Jalur jaringan antara instans tidak boleh menyertakan kotak perangkat lunak perantara (middleware). ENA Ekspres saat ini tidak mendukung kotak perangkat lunak perantara (middleware).

> **Note**
>
> Metrik kelayakan ENA Ekspres mencakup persyaratan sumber dan tujuan, dan jaringan antara dua titik akhir. Paket yang memenuhi syarat masih dapat didiskualifikasi setelah dihitung. Misalnya, jika paket yang memenuhi syarat melebihi batas unit transmisi maksimum (MTU), paket tersebut jatuh kembali ke transmisi ENA standar, meskipun paket tersebut masih tercermin sebagai memenuhi syarat di konter.

ena_srd_tx_pkts

Jumlah paket SRD yang ditransmisikan dalam jangka waktu tertentu.

ena_srd_rx_pkts

Jumlah paket SRD yang diterima dalam jangka waktu tertentu.

ena_srd_resource_utilization

Persentase pemanfaatan memori maksimum yang diizinkan untuk koneksi SRD bersamaan yang telah dikonsumsi instance.

Untuk mengonfirmasi apakah transmisi paket menggunakan SRD, Anda dapat membandingkan jumlah paket yang memenuhi syarat (metrik `ena_srd_eligible_tx_pkts`) dengan jumlah paket SRD yang ditransmisikan (metrik `ena_srd_tx_pkts`) selama periode waktu tertentu.

Lalu lintas keluar (paket keluar)

Untuk memastikan bahwa lalu lintas jalan keluar Anda menggunakan SRD seperti yang diharapkan, bandingkan jumlah paket yang memenuhi syarat SRD (`ena_srd_eligible_tx_pkts`) dengan jumlah paket SRD yang dikirim (`ena_srd_tx_pkts`) selama periode waktu tertentu.

Perbedaan yang signifikan antara jumlah paket yang memenuhi syarat dan jumlah paket SRD yang dikirim sering disebabkan oleh masalah pemanfaatan sumber daya. Ketika kartu jaringan yang terpasang pada instans telah menggunakan sumber daya maksimumnya, atau jika paket melebihi batas MTU, paket yang memenuhi syarat tidak dapat ditransmisikan melalui SRD, dan harus kembali ke transmisi ENA standar. Paket juga dapat jatuh ke dalam celah ini selama migrasi langsung atau pembaruan server langsung. Pemecahan masalah tambahan diperlukan untuk menentukan akar penyebabnya.

> **Note**
>
> Anda dapat mengabaikan perbedaan kecil sesekali antara jumlah paket yang memenuhi syarat dan jumlah paket SRD. Ini dapat terjadi ketika instans Anda membuat koneksi ke instans lain untuk lalu lintas SRD, misalnya.

Untuk mengetahui berapa persentase total lalu lintas keluar Anda selama periode waktu tertentu menggunakan SRD, bandingkan jumlah paket SRD yang dikirim (`ena_srd_tx_pkts`) dengan jumlah total paket yang dikirim untuk instans (`NetworkPacketOut`) selama waktu itu.

Lalu lintas masuk (paket masuk)

Untuk mengetahui berapa persentase lalu lintas masuk Anda menggunakan SRD, bandingkan jumlah paket SRD yang diterima (`ena_srd_rx_pkts`) selama periode waktu tertentu dengan jumlah total paket yang diterima untuk instans (`NetworkPacketIn`) selama waktu itu.

Pemanfaatan Sumber Daya

Pemanfaatan sumber daya didasarkan pada jumlah koneksi SRD bersamaan yang dapat ditahan oleh satu instans pada waktu tertentu. Metrik pemanfaatan sumber daya (`ena_srd_resource_utilization`) melacak pemanfaatan Anda saat ini untuk instans tersebut. Saat pemanfaatan mendekati 100%, Anda dapat mengharapkan untuk melihat masalah performa. ENA Ekspres jatuh kembali dari SRD ke transmisi ENA standar, dan kemungkinan paket yang dijatuhkan meningkat. Pemanfaatan sumber daya yang tinggi adalah tanda bahwa sudah waktunya untuk meningkatkan skala instans untuk meningkatkan performa jaringan.

> **Note**
>
> Ketika lalu lintas jaringan untuk suatu instance melebihi maksimum, AWS membentuk lalu lintas yang melebihi maksimum dengan mengantri dan kemudian menjatuhkan paket jaringan.

Tetap

Metrik jalan keluar dan masuknya bertambah saat ENA Ekspres diaktifkan untuk instans. Metrik berhenti bertambah jika ENA Ekspres dinonaktifkan, tetapi tetap ada selama instans masih berjalan. Metrik diatur ulang jika instans reboot atau diakhiri, atau jika antarmuka jaringan terlepas dari instans.

Metrik performa jaringan dengan driver DPDK untuk ENA

ENA driver versi 2.2.0 dan yang lebih baru mendukung pelaporan metrik jaringan. DPDK 20.11 termasuk driver ENA 2.2.0 dan versi DPDK pertama untuk mendukung fitur ini.

Driver DPDK v25.03 atau yang lebih baru mendukung mode proxy fragmen. Jika mode proxy fragmen diaktifkan untuk driver DPDK, fragmen keluar turun melewati batas 1024 PPS yang biasanya berlaku dan dihitung dalam tunjangan PPS standar. Mode proxy fragmen dinonaktifkan secara default.

Anda dapat menggunakan contoh aplikasi untuk melihat statistik DPDK. Untuk memulai versi interaktif aplikasi contoh, jalankan perintah berikut.

```
./app/dpdk-testpmd -- -i
```

Dalam sesi interaktif ini, Anda dapat memasukkan perintah untuk mengambil statistik diperpanjang untuk port. Contoh perintah berikut mengambil statistik untuk port 0.

```
show port xstats 0
```

Berikut ini adalah contoh sesi interaktif dengan aplikasi contoh DPDK.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
```

```
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
        tx_good_bytes: 0
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
```

```
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
        testpmd>
```

Untuk informasi lebih lanjut tentang aplikasi contoh dan menggunakannya untuk mengambil statistik yang diperluas. lihat Panduan Pengguna Aplikasi Testpmd dalam dokumentasi DPDK.

Metrik pada instans yang berjalan FreeBSD

Dimulai dengan versi 2.3.0, FreeBSD driver ENA mendukung pengumpulan metrik kinerja jaringan pada instans yang berjalan. FreeBSD Untuk mengaktifkan koleksi FreeBSD metrik, masukkan perintah berikut dan atur *`interval`* ke nilai antara 1 dan 3600. Ini menentukan seberapa sering, dalam hitungan detik, untuk mengumpulkan FreeBSD metrik.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Misalnya, perintah berikut menetapkan driver untuk mengumpulkan FreeBSD metrik pada antarmuka jaringan 1 setiap 10 detik:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Untuk mematikan koleksi FreeBSD metrik, Anda dapat menjalankan perintah sebelumnya dan menentukan `0` sebagai. *`interval`*

Setelah mengaktifkan FreeBSD metrik pengumpulan, Anda dapat mengambil kumpulan metrik terbaru yang dikumpulkan dengan menjalankan perintah berikut.

```
sysctl dev.ena.network_interface.eni_metrics
```

Meningkatkan latensi jaringan untuk instance berbasis EC2 Linux

Latensi jaringan adalah jumlah waktu yang dibutuhkan untuk paket data untuk melakukan perjalanan dari sumbernya ke tujuannya. Aplikasi yang mengirim data ke seluruh jaringan bergantung pada respons tepat waktu untuk memberikan pengalaman pengguna yang positif. Latensi jaringan yang tinggi dapat menyebabkan berbagai masalah, seperti berikut ini:

- Waktu muat lambat untuk halaman web
- Kelambatan streaming video
- Kesulitan mengakses sumber daya online

Bagian ini menguraikan langkah-langkah yang dapat Anda ambil untuk meningkatkan latensi jaringan pada EC2 instans Amazon yang berjalan di Linux. Untuk mencapai latensi optimal, ikuti langkah-langkah berikut untuk mengonfigurasi pengaturan driver instans, kernel, dan ENA Anda. Untuk panduan konfigurasi tambahan, lihat Panduan Praktik Terbaik dan Pengoptimalan Kinerja Driver ENA LinuxGitHub.

> **Note**
>
> Langkah dan pengaturan mungkin sedikit berbeda, tergantung pada perangkat keras jaringan spesifik Anda, AMI tempat Anda meluncurkan instans, dan kasus penggunaan aplikasi Anda. Sebelum Anda membuat perubahan apa pun, uji dan pantau performa jaringan Anda secara menyeluruh untuk memastikan bahwa Anda mendapatkan hasil yang diinginkan.

Kurangi jumlah hop jaringan untuk paket data

Setiap lompatan yang diambil paket data saat bergerak dari router ke router meningkatkan latensi jaringan. Biasanya, lalu lintas harus mengambil beberapa lompatan untuk mencapai tujuan Anda. Ada dua cara untuk mengurangi hop jaringan untuk EC2 instans Amazon Anda, sebagai berikut:

- Grup penempatan klaster — Saat Anda menentukan grup penempatan klaster, Amazon EC2 meluncurkan instance yang berdekatan satu sama lain, secara fisik dalam Availability Zone (AZ)

yang sama dengan kemasan yang lebih ketat. Kedekatan fisik instans dalam grup memungkinkan mereka untuk memanfaatkan konektivitas berkecepatan tinggi, menghasilkan latensi rendah dan throughput aliran tunggal yang tinggi.

- Host Khusus — Host Khusus adalah server fisik yang didedikasikan untuk Anda gunakan. Dengan Host Khusus, Anda dapat meluncurkan instans Anda untuk berjalan di server fisik yang sama. Komunikasi antar instans yang berjalan pada Host Khusus yang sama dapat terjadi tanpa lompatan jaringan tambahan.

Bagaimana konfigurasi kernel Linux memengaruhi latensi

Konfigurasi kernel Linux dapat meningkatkan atau mengurangi latensi jaringan. Untuk mencapai tujuan optimasi latensi Anda, penting untuk menyempurnakan konfigurasi kernel Linux sesuai dengan persyaratan spesifik beban kerja Anda.

Ada banyak opsi konfigurasi untuk kernel Linux yang dapat membantu mengurangi latensi jaringan. Opsi yang paling berdampak adalah sebagai berikut.

- Aktifkan mode polling sibuk — Mode polling sibuk mengurangi latensi pada jalur penerimaan jaringan. Saat Anda mengaktifkan mode polling sibuk, kode lapisan soket dapat langsung melakukan polling antrean penerima perangkat jaringan. Kelemahan dari polling sibuk adalah penggunaan CPU yang lebih tinggi di host yang berasal dari polling untuk data baru dalam lingkaran ketat. Ada dua pengaturan global yang mengontrol jumlah mikrodetik untuk menunggu paket untuk semua antarmuka.

  `busy_read`

  Batas waktu polling sibuk latensi rendah untuk pembacaan soket. Ini mengontrol jumlah mikrodetik untuk menunggu lapisan soket membaca paket pada antrean perangkat. Untuk mengaktifkan fitur secara global dengan perintah sysctl, organisasi Kernel Linux merekomendasikan nilai 50 mikrodetik. Untuk informasi selengkapnya, lihat busy_read di panduan pengguna dan administrator kernel Linux.

  ```
  [ec2-user ~]$ sudo sysctl -w net.core.busy_read=50
  ```

`busy_poll`

Batas waktu polling sibuk latensi rendah untuk polling dan pilih. Ini mengontrol jumlah mikrodetik untuk menunggu peristiwa. Nilai yang disarankan adalah antara 50-100 mikrodetik, tergantung pada jumlah soket yang Anda polling. Semakin banyak soket yang Anda tambahkan, semakin tinggi angkanya.

```
[ec2-user ~]$ sudo sysctl -w net.core.busy_poll=50
```

- Konfigurasi status daya CPU (status-C) — Status-C mengontrol tingkat tidur yang mungkin dimasuki inti saat tidak aktif. Anda mungkin ingin mengontrol status-C untuk menyesuaikan sistem Anda untuk latensi versus performa. Dalam keadaan C yang lebih dalam, CPU pada dasarnya "tertidur" dan tidak dapat menanggapi permintaan sampai bangun dan beralih kembali ke keadaan aktif. Menidurkan inti membutuhkan waktu, dan meskipun inti tidur memungkinkan lebih banyak ruang kepala untuk inti lain untuk meningkat ke frekuensi yang lebih tinggi, inti tidur tersebut membutuhkan waktu untuk bangun kembali dan melakukan pekerjaan.

  Misalnya, jika inti yang ditugaskan untuk menangani interupsi paket jaringan tertidur, mungkin ada penundaan dalam melayani interupsi tersebut. Anda dapat mengonfigurasi sistem sehingga tidak menggunakan status C yang lebih dalam. Namun, meskipun konfigurasi ini mengurangi latensi reaksi prosesor, konfigurasi ini juga mengurangi ruang kepala yang tersedia untuk inti lain untuk Turbo Boost.

  Untuk mengurangi latensi reaksi prosesor, Anda dapat membatasi keadaan C yang lebih dalam. Untuk informasi selengkapnya, lihat Kinerja tinggi dan latensi rendah dengan membatasi status C yang lebih dalam di Panduan Pengguna Amazon Linux 2.

Moderasi interupsi

Driver jaringan ENA memungkinkan komunikasi antara instans dan jaringan. Driver memproses paket jaringan dan meneruskannya ke tumpukan jaringan atau ke kartu Nitro. Ketika paket jaringan masuk, kartu Nitro menghasilkan interupsi bagi CPU untuk memberi tahu perangkat lunak suatu peristiwa.

Menginterupsi

Interupsi adalah sinyal yang dikirim perangkat atau aplikasi ke prosesor. Interupsi memberi tahu prosesor bahwa suatu peristiwa telah terjadi atau suatu kondisi telah terpenuhi yang membutuhkan perhatian segera. Interupsi dapat menangani tugas yang sensitif terhadap waktu

seperti menerima data dari antarmuka jaringan, menangani peristiwa perangkat keras, atau melayani permintaan dari perangkat lain.

Moderasi interupsi

Moderasi interupsi adalah teknik yang mengurangi jumlah interupsi yang dihasilkan perangkat dengan menggabungkan atau menundanya. Tujuan dari moderasi interupsi adalah untuk meningkatkan performa sistem dengan mengurangi overhead yang terkait dengan penanganan sejumlah besar interupsi. Terlalu banyak interupsi meningkatkan penggunaan CPU, berdampak buruk pada throughput, sementara terlalu sedikit interupsi meningkatkan latensi.

Moderasi interupsi dinamis

Moderasi interupsi dinamis adalah bentuk peningkatan moderasi interupsi yang secara dinamis menyesuaikan tingkat interupsi berdasarkan beban sistem saat ini dan pola lalu lintas. Ini bertujuan untuk mencapai keseimbangan antara mengurangi interupsi overhead dan paket per detik, atau bandwidth.

> **Note**
>
> Moderasi interupsi dinamis diaktifkan secara default di beberapa AMIs (tetapi dapat diaktifkan atau dinonaktifkan di semua AMIs).

Untuk meminimalkan latensi jaringan, mungkin perlu menonaktifkan moderasi interupsi. Namun, ini juga dapat meningkatkan overhead pemrosesan interupsi. Penting untuk menemukan keseimbangan yang tepat antara mengurangi latensi dan meminimalkan overhead. Perintah `ethtool` dapat membantu Anda mengonfigurasi moderasi interupsi. Secara default, `rx-usecs` diatur ke `20`, dan `tx-usecs` diatur ke `64`.

Untuk mendapatkan konfigurasi modifikasi interupsi saat ini, gunakan perintah berikut.

```
[ec2-user ~]$ ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Untuk menonaktifkan modifikasi interupsi dan moderasi interupsi dinamis, gunakan perintah berikut.

```
[ec2-user ~]$ sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Pertimbangan sistem nitro untuk penyetelan kinerja

Sistem Nitro adalah kumpulan komponen perangkat keras dan perangkat lunak yang dibangun oleh AWS yang memungkinkan kinerja tinggi, ketersediaan tinggi, dan keamanan tinggi. Sistem Nitro menyediakan kemampuan seperti logam kosong yang menghilangkan overhead virtualisasi dan mendukung beban kerja yang memerlukan akses penuh ke perangkat keras host. Untuk informasi lebih rinci, lihat Sistem AWS Nitro.

Semua jenis instans EC2 generasi saat ini melakukan pemrosesan paket jaringan pada Kartu EC2 Nitro. Topik ini mencakup penanganan paket tingkat tinggi pada kartu Nitro, aspek umum arsitektur jaringan dan konfigurasi yang memengaruhi kinerja penanganan paket, dan tindakan apa yang dapat Anda ambil untuk mencapai kinerja puncak untuk instance berbasis Nitro Anda.

Kartu Nitro menangani semua input dan output (I/O) interfaces, such as those needed for Virtual Private Clouds (VPCs). For all of the components that send or receive information over the network, the Nitro cards act as a self-contained computing device for I/Olalu lintas yang secara fisik terpisah dari papan utama sistem tempat beban kerja pelanggan berjalan.

Aliran paket jaringan pada kartu Nitro

Instans EC2 yang dibangun di atas sistem Nitro memiliki kemampuan akselerasi perangkat keras yang memungkinkan pemrosesan paket lebih cepat, yang diukur dengan tingkat throughput paket per detik (PPS). Ketika kartu Nitro melakukan evaluasi awal untuk aliran baru, ia menyimpan informasi yang sama untuk semua paket dalam aliran, seperti grup keamanan, daftar kontrol akses, dan entri tabel rute. Ketika memproses paket tambahan untuk aliran yang sama, ia dapat menggunakan informasi yang disimpan untuk mengurangi overhead untuk paket-paket tersebut.

Tingkat koneksi Anda diukur dengan metrik koneksi per detik (CPS). Setiap koneksi baru memerlukan overhead pemrosesan tambahan yang harus diperhitungkan dalam perkiraan kemampuan beban kerja. Penting untuk mempertimbangkan metrik CPS dan PPS saat Anda mendesain beban kerja Anda.

Bagaimana koneksi dibuat

Ketika koneksi dibuat antara instance berbasis Nitro dan titik akhir lainnya, kartu Nitro mengevaluasi aliran penuh untuk paket pertama yang dikirim atau diterima antara dua titik akhir. Untuk paket berikutnya dari aliran yang sama, evaluasi ulang penuh biasanya tidak diperlukan. Namun, ada pengecualian. Untuk informasi lebih lanjut tentang pengecualian, lihatPaket yang tidak menggunakan akselerasi perangkat keras.

Properti berikut mendefinisikan dua titik akhir dan aliran paket di antara mereka. Kelima sifat ini bersama-sama dikenal sebagai aliran 5-tuple.

- IP sumber
- Port sumber
- IP Tujuan
- Port tujuan
- Protokol komunikasi

Arah aliran paket dikenal sebagai ingress (inbound) dan egress (outbound). Deskripsi tingkat tinggi berikut merangkum aliran paket jaringan ujung ke ujung.

- Ingress — Ketika kartu Nitro menangani paket jaringan masuk, ia mengevaluasi paket terhadap aturan firewall stateful dan daftar kontrol akses. Ini melacak koneksi, mengukurnya, dan melakukan tindakan lain yang berlaku. Kemudian meneruskan paket ke tujuannya pada CPU host.
- Egress — Ketika kartu Nitro menangani paket jaringan keluar, ia mencari tujuan antarmuka jarak jauh, mengevaluasi berbagai fungsi VPC, menerapkan batas kecepatan, dan melakukan tindakan lain yang berlaku. Kemudian meneruskan paket ke tujuan hop berikutnya di jaringan.

Rancang jaringan Anda untuk kinerja optimal

Untuk memanfaatkan kemampuan kinerja sistem Nitro Anda, Anda harus memahami apa kebutuhan pemrosesan jaringan Anda dan bagaimana kebutuhan tersebut memengaruhi beban kerja untuk sumber daya Nitro Anda. Kemudian Anda dapat merancang untuk kinerja optimal untuk lanskap jaringan Anda. Pengaturan infrastruktur serta desain dan konfigurasi beban kerja aplikasi Anda dapat memengaruhi pemrosesan paket dan tingkat koneksi. Misalnya, jika aplikasi Anda memiliki tingkat pembentukan koneksi yang tinggi, seperti layanan DNS, firewall, atau router virtual, itu akan memiliki lebih sedikit kesempatan untuk memanfaatkan akselerasi perangkat keras yang hanya terjadi setelah koneksi dibuat.

Anda dapat mengonfigurasi pengaturan aplikasi dan infrastruktur untuk merampingkan beban kerja dan meningkatkan kinerja jaringan. Namun, tidak semua paket memenuhi syarat untuk akselerasi. Sistem Nitro menggunakan aliran jaringan penuh untuk koneksi baru dan untuk paket yang tidak memenuhi syarat untuk akselerasi.

Sisa bagian ini akan fokus pada pertimbangan desain aplikasi dan infrastruktur untuk membantu memastikan bahwa paket mengalir dalam jalur yang dipercepat sebanyak mungkin.

Pertimbangan desain jaringan untuk sistem Nitro

Saat Anda mengonfigurasi lalu lintas jaringan untuk instans Anda, ada banyak aspek yang perlu dipertimbangkan yang dapat memengaruhi kinerja PPS. Setelah aliran terbentuk, sebagian besar paket yang secara teratur masuk atau keluar memenuhi syarat untuk akselerasi. Namun, ada pengecualian untuk memastikan bahwa desain infrastruktur dan aliran paket terus memenuhi standar protokol.

Untuk mendapatkan kinerja terbaik dari kartu Nitro Anda, Anda harus mempertimbangkan dengan cermat pro dan kontra dari detail konfigurasi berikut untuk infrastruktur dan aplikasi Anda.

Pertimbangan infrastruktur

Konfigurasi infrastruktur Anda dapat memengaruhi aliran paket dan efisiensi pemrosesan Anda. Daftar berikut mencakup beberapa pertimbangan penting.

Konfigurasi antarmuka jaringan dengan asimetri

Grup keamanan menggunakan pelacakan koneksi untuk melacak informasi tentang lalu lintas yang mengalir ke dan dari instance. Perutean asimetris, di mana lalu lintas masuk ke sebuah instance melalui satu antarmuka jaringan dan pergi melalui antarmuka jaringan yang berbeda, dapat mengurangi kinerja puncak yang dapat dicapai oleh instans jika arus dilacak. Untuk informasi selengkapnya tentang pelacakan koneksi grup keamanan, koneksi yang tidak dilacak, dan koneksi yang dilacak secara otomatis, lihat. Pelacakan koneksi grup keamanan Amazon EC2

Driver jaringan

Driver jaringan diperbarui dan dirilis secara teratur. Jika driver Anda kedaluwarsa, itu dapat secara signifikan mengganggu kinerja. Perbarui driver Anda untuk memastikan bahwa Anda memiliki tambalan terbaru dan dapat memanfaatkan peningkatan kinerja, seperti fitur jalur akselerasi yang hanya tersedia untuk driver generasi terbaru. Driver sebelumnya tidak mendukung fitur jalur akselerasi.

Untuk memanfaatkan fitur jalur akselerasi, kami sarankan Anda menginstal driver ENA terbaru pada instans Anda.

Instance Linux — ENA Linux driver 2.2.9 atau yang lebih baru. Untuk menginstal atau memperbarui driver ENA Linux dari GitHub repositori Amazon Drivers, lihat bagian kompilasi Driver dari file readme.

Instans Windows — ENA Windows driver 2.0.0 atau yang lebih baru. Untuk menginstal atau memperbarui driver ENA Windows, lihatInstal driver ENA pada instans EC2 Windows.

Jarak antara titik akhir

Koneksi antara dua instance di Availability Zone yang sama dapat memproses lebih banyak paket per detik daripada koneksi di seluruh Wilayah sebagai akibat dari windowing TCP pada lapisan aplikasi, yang menentukan berapa banyak data yang dapat terbang pada waktu tertentu. Jarak yang jauh antar instance meningkatkan latensi dan mengurangi jumlah paket yang dapat diproses titik akhir.

Batas antrian byte (BQL)

BQL adalah fitur yang membatasi jumlah byte yang diteruskan ke kartu Nitro untuk mengurangi antrian. BQL dinonaktifkan secara default di driver ENA, di sistem operasi Amazon Linux, dan di sebagian besar distribusi Linux. Jika BQL dan penggantian proxy fragmen keduanya diaktifkan, hal itu dapat mengakibatkan keterbatasan kinerja dengan membatasi jumlah byte yang diteruskan ke Nitro sebelum semua fragmen diproses.

Pertimbangan desain aplikasi

Ada aspek desain dan konfigurasi aplikasi yang dapat memengaruhi efisiensi pemrosesan Anda. Daftar berikut mencakup beberapa pertimbangan penting.

Ukuran paket

Ukuran paket yang lebih besar dapat meningkatkan throughput untuk data yang dapat dikirim dan diterima instance di jaringan. Amazon EC2 mendukung bingkai jumbo 9001 byte, namun layanan lain dapat memberlakukan batasan yang berbeda. Ukuran paket yang lebih kecil dapat meningkatkan laju proses paket, tetapi ini dapat mengurangi bandwidth maksimum yang dicapai ketika jumlah paket melebihi tunjangan PPS.

Jika ukuran paket melebihi Maximum Transmission Unit (MTU) dari jaringan hop, router di sepanjang jalur mungkin memecahnya. Fragmen paket yang dihasilkan dianggap pengecualian, dan biasanya diproses pada tingkat standar (tidak dipercepat). Ini dapat menyebabkan variasi dalam kinerja Anda. Namun, Anda dapat mengganti perilaku standar untuk paket terfragmentasi keluar dengan pengaturan mode proxy fragmen. Untuk informasi selengkapnya, lihat Maksimalkan kinerja jaringan pada sistem Nitro Anda. Kami menyarankan Anda mengevaluasi topologi Anda ketika Anda mengkonfigurasi MTU.

Pertukaran protokol

Protokol yang andal seperti TCP memiliki lebih banyak overhead daripada protokol yang tidak dapat diandalkan seperti UDP. Overhead yang lebih rendah dan pemrosesan jaringan yang

disederhanakan untuk protokol transport UDP dapat menghasilkan tingkat PPS yang lebih tinggi, tetapi dengan mengorbankan pengiriman paket yang andal. Jika pengiriman paket yang andal tidak penting untuk aplikasi Anda, UDP mungkin merupakan pilihan yang baik.

Meledak mikro

Micro-bursting terjadi ketika lalu lintas melebihi tunjangan selama periode waktu yang singkat daripada didistribusikan secara merata. Ini biasanya terjadi pada skala mikrodetik.

Misalnya, katakanlah Anda memiliki instance yang dapat mengirim hingga 10 Gbps, dan aplikasi Anda mengirimkan 10 Gb penuh dalam setengah detik. Ledakan mikro ini melebihi tunjangan selama paruh pertama kedua dan tidak meninggalkan apa pun untuk sisa detik. Meskipun Anda mengirim 10Gb dalam jangka waktu 1 detik, tunjangan di paruh pertama detik dapat mengakibatkan paket diantrian atau dijatuhkan.

Anda dapat menggunakan penjadwal jaringan seperti Linux Traffic Control untuk membantu mempercepat throughput Anda dan menghindari menyebabkan paket antrian atau jatuh sebagai akibat dari ledakan mikro.

Jumlah arus

Aliran tunggal dibatasi hingga 5 Gbps kecuali berada di dalam grup penempatan cluster yang mendukung hingga 10 Gbps, atau jika menggunakan ENA Express, yang mendukung hingga 25 Gbps.

Demikian pula, kartu Nitro dapat memproses lebih banyak paket di beberapa aliran dibandingkan dengan menggunakan aliran tunggal. Untuk mencapai tingkat pemrosesan paket puncak per instans, kami merekomendasikan setidaknya 100 aliran pada instans dengan bandwidth agregat 100 Gbps atau lebih tinggi. Ketika kemampuan bandwidth agregat meningkat, jumlah aliran yang dibutuhkan untuk mencapai tingkat pemrosesan puncak juga meningkat. Benchmarking akan membantu Anda menentukan konfigurasi apa yang Anda butuhkan untuk mencapai tingkat puncak di jaringan Anda.

Antrian Adaptor Jaringan Elastis (ENA)

ENA (Elastic Network Adapter) menggunakan beberapa antrian penerima (Rx) dan transmisi (Tx) (antrian ENA) untuk meningkatkan kinerja dan skalabilitas jaringan pada instans EC2. Antrian ini secara efisien mengelola lalu lintas jaringan dengan menyeimbangkan beban data yang dikirim dan diterima di seluruh antrian yang tersedia.

Untuk informasi selengkapnya, lihat the section called “Antrian ENA”.

Overhead proses fitur

Fitur seperti Traffic Mirroring dan ENA Express dapat menambahkan lebih banyak overhead pemrosesan, yang dapat mengurangi kinerja pemrosesan paket absolut. Anda dapat membatasi penggunaan fitur atau menonaktifkan fitur untuk meningkatkan tingkat pemrosesan paket.

Pelacakan koneksi untuk mempertahankan status

Grup keamanan Anda menggunakan pelacakan koneksi untuk menyimpan informasi tentang lalu lintas ke dan dari instance. Pelacakan koneksi menerapkan aturan terhadap setiap arus lalu lintas jaringan individu untuk menentukan apakah lalu lintas diizinkan atau ditolak. Kartu Nitro menggunakan pelacakan aliran untuk mempertahankan status aliran. Karena semakin banyak aturan kelompok keamanan diterapkan, lebih banyak pekerjaan diperlukan untuk mengevaluasi aliran.

> **Note**
>
> Tidak semua arus lalu lintas jaringan dilacak. Jika aturan grup keamanan dikonfigurasiKoneksi-koneksi yang tidak dilacak, tidak ada pekerjaan tambahan yang diperlukan kecuali untuk koneksi yang dilacak secara otomatis untuk memastikan perutean simetris ketika ada beberapa jalur balasan yang valid.

Paket yang tidak menggunakan akselerasi perangkat keras

Tidak semua paket dapat memanfaatkan akselerasi perangkat keras. Penanganan pengecualian ini melibatkan beberapa overhead pemrosesan yang diperlukan untuk memastikan kesehatan arus jaringan Anda. Alur jaringan harus andal memenuhi standar protokol, sesuai dengan perubahan dalam desain VPC, dan paket rute hanya ke tujuan yang diizinkan. Namun, overhead mengurangi kinerja Anda.

Fragmen paket

Seperti disebutkan di bawah pertimbangan Aplikasi, fragmen paket yang dihasilkan dari paket yang melebihi MTU jaringan biasanya ditangani sebagai pengecualian, dan tidak dapat memanfaatkan akselerasi perangkat keras. Namun, Anda dapat melewati batasan fragmen jalan keluar dengan mode proxy fragmen, tergantung pada versi driver Anda. Untuk informasi selengkapnya, lihat tindakan yang dapat Anda lakukan di Maksimalkan kinerja jaringan pada sistem Nitro Anda bagian ini.

Koneksi menganggur

Ketika koneksi tidak memiliki aktivitas untuk sementara waktu, bahkan jika koneksi belum mencapai batas waktu tunggu, sistem dapat tidak memprioritaskannya. Kemudian, jika data masuk setelah koneksi tidak diprioritaskan, sistem perlu menanganinya sebagai pengecualian untuk menyambung kembali.

Untuk mengelola koneksi, Anda dapat menggunakan batas waktu pelacakan koneksi untuk menutup koneksi idle. Anda juga dapat menggunakan TCP keepalives untuk menjaga koneksi idle tetap terbuka. Untuk informasi selengkapnya, lihat Waktu habis pelacakan koneksi idle.

Mutasi VPC

Pembaruan untuk grup keamanan, tabel rute, dan daftar kontrol akses semuanya perlu dievaluasi ulang di jalur pemrosesan untuk memastikan bahwa entri rute dan aturan grup keamanan masih berlaku seperti yang diharapkan.

Aliran ICMP

Internet Control Message Protocol (ICMP) adalah protokol lapisan jaringan yang digunakan perangkat jaringan untuk mendiagnosis masalah komunikasi jaringan. Paket-paket ini selalu menggunakan aliran penuh.

Aliran L2 asimetris

NitroV3 dan platform sebelumnya tidak menggunakan akselerasi perangkat keras untuk lalu lintas antara dua ENIs di subnet yang sama di mana satu ENI menggunakan router gateway default dan yang lainnya tidak. NitroV4 dan platform yang lebih baru menggunakan akselerasi perangkat keras dalam skenario ini. Untuk kinerja yang lebih baik pada NitroV3 atau platform sebelumnya, pastikan bahwa router gateway default menggunakan kecocokan antara keduanya ENIs, atau yang ENIs berada di subnet yang berbeda.

Maksimalkan kinerja jaringan pada sistem Nitro Anda

Anda dapat memaksimalkan kinerja jaringan Anda pada sistem Nitro dengan menyesuaikan pengaturan jaringan.

Topik

- Pertimbangan-pertimbangan
- Tune kinerja PPS

- Konfigurasikan alokasi antrian ENA
- Pantau kinerja pada instance Linux

Pertimbangan-pertimbangan

Sebelum Anda membuat keputusan desain atau menyesuaikan pengaturan jaringan apa pun pada instans Anda, kami sarankan Anda mengambil langkah-langkah berikut untuk membantu memastikan bahwa Anda mendapatkan hasil terbaik:

1. Pahami pro dan kontra dari tindakan yang dapat Anda ambil untuk meningkatkan kinerja dengan meninjauPertimbangan desain jaringan untuk sistem Nitro.

   Untuk pertimbangan dan praktik terbaik lainnya untuk konfigurasi instans Anda di Linux, lihat Panduan Praktik Terbaik dan Pengoptimalan Kinerja Driver ENA Linux di GitHub.
2. Benchmark beban kerja Anda dengan jumlah alur aktif puncak untuk menentukan dasar kinerja aplikasi Anda. Dengan baseline kinerja, Anda dapat menguji variasi dalam pengaturan atau desain aplikasi untuk memahami pertimbangan mana yang paling berdampak, terutama jika Anda berencana untuk meningkatkan atau meningkatkan skala.

Tune kinerja PPS

Daftar berikut berisi tindakan yang dapat Anda lakukan untuk menyesuaikan kinerja PPS Anda, tergantung pada kebutuhan sistem Anda.

- Kurangi jarak fisik antara dua contoh. Saat mengirim dan menerima instance berada di Availability Zone yang sama atau menggunakan grup penempatan cluster, Anda dapat mengurangi jumlah hop yang perlu diambil paket untuk melakukan perjalanan dari satu titik akhir ke titik akhir lainnya.
- Gunakan Koneksi-koneksi yang tidak dilacak.
- Gunakan protokol UDP untuk lalu lintas jaringan.
- Untuk instans EC2 dengan bandwidth agregat 100 Gbps atau lebih, distribusikan beban kerja lebih dari 100 atau lebih aliran individu untuk menyebarkan pekerjaan secara merata di seluruh kartu Nitro.
- Untuk mengatasi batas PPS fragmen keluar pada instans EC2, Anda dapat mengaktifkan mode proxy fragmen (tergantung pada versi driver Anda). Pengaturan ini memungkinkan paket terfragmentasi untuk dievaluasi di jalur pemrosesan, sehingga mengatasi batas PPS jalan keluar 1024. Saat memuat driver, jalankan salah satu perintah berikut untuk mengaktifkan atau menonaktifkan mode proxy fragmen:

Aktifkan mode proxy fragmen

```
sudo insmod ena.ko enable_frag_bypass=1
```

Nonaktifkan mode proxy fragmen

```
sudo insmod ena.ko enable_frag_bypass=0
```

Konfigurasikan alokasi antrian ENA

Pada jenis instans yang didukung, Anda dapat mengalokasikan antrian ini secara dinamis di seluruh Elastic Network Interfaces (). ENIs Alokasi antrian ENA yang fleksibel mengoptimalkan distribusi sumber daya, memungkinkan pemanfaatan vCPU maksimum. Beban kerja kinerja jaringan yang tinggi biasanya memerlukan beberapa antrian ENA. Untuk informasi selengkapnya, lihat Antrian ENA.

Pantau kinerja pada instance Linux

Anda dapat menggunakan metrik Ethtool pada instans Linux untuk memantau indikator kinerja jaringan instans seperti bandwidth, laju paket, dan pelacakan koneksi. Lihat informasi yang lebih lengkap di Pantau kinerja jaringan untuk pengaturan ENA pada instans EC2 Anda.

Optimalkan kinerja jaringan pada instance EC2 Windows

Untuk mencapai kinerja jaringan maksimum pada instance Windows Anda dengan jaringan yang disempurnakan, Anda mungkin perlu memodifikasi konfigurasi sistem operasi default. Kami merekomendasikan perubahan konfigurasi berikut untuk aplikasi yang memerlukan performa jaringan tinggi. Pengoptimalan lain (seperti mengaktifkan pembongkaran checksum dan mengaktifkan RSS, misalnya) sudah dikonfigurasi pada Windows resmi. AMIs

> **Note**
>
> TCP chimney offloading harus dinonaktifkan di sebagian besar kasus penggunaan, dan sudah tidak digunakan lagi mulai Windows Server 2016.

Selain pengoptimalan sistem operasi ini, Anda juga harus mempertimbangkan unit transmisi maksimum (MTU) lalu lintas jaringan Anda, dan menyesuaikannya dengan beban kerja dan arsitektur

jaringan Anda. Untuk informasi selengkapnya, lihat Unit transmisi maksimum jaringan (MTU) untuk instans Anda EC2.

AWS secara teratur mengukur latensi pulang-pergi rata-rata antara instance yang diluncurkan dalam kelompok penempatan cluster 50us dan latensi ekor 200us pada persentil 99,9. Jika aplikasi Anda membutuhkan latensi rendah secara konsisten, kami merekomendasikan menggunakan driver ENA versi terbaru pada instans berbasis Nitro dengan performa tetap.

Konfigurasikan afinitas CPU penskalaan sisi Terima

Receive side scaling (RSS) digunakan untuk mendistribusikan beban CPU lalu lintas jaringan ke beberapa prosesor. Secara default, Amazon Windows resmi AMIs dikonfigurasi dengan RSS diaktifkan. Antarmuka jaringan elastis ENA menyediakan hingga delapan antrian RSS. Dengan menentukan afinitas CPU untuk antrean RSS, serta untuk proses sistem lainnya, dimungkinkan untuk menyebarkan beban CPU melalui sistem multi-core, yang memungkinkan lebih banyak lalu lintas jaringan untuk diproses. Pada jenis instans dengan lebih dari 16 vCPUs, kami menyarankan Anda menggunakan `Set-NetAdapterRSS` PowerShell cmdlet, yang secara manual mengecualikan prosesor boot (prosesor logis 0 dan 1 ketika hyper-threading diaktifkan) dari konfigurasi RSS untuk semua antarmuka jaringan elastis, untuk mencegah pertengkaran dengan berbagai komponen sistem.

Windows sangat sadar dan memastikan bahwa antrian RSS dari kartu antarmuka jaringan tunggal (NIC) selalu ditempatkan pada inti fisik yang berbeda. Oleh karena itu, kecuali hyper-threading dinonaktifkan, untuk sepenuhnya mencegah pertengkaran dengan yang lain NICs, sebarkan konfigurasi RSS setiap NIC di antara kisaran 16 prosesor logis. `Set-NetAdapterRss`Cmdlet memungkinkan Anda untuk menentukan rentang per-NIC prosesor logis yang valid dengan mendefinisikan nilai BaseProcessorGroup,,, BaseProcessorNumber MaxProcessingGroup MaxProcessorNumber, dan (opsional). NumaNode Jika tidak ada inti fisik yang cukup untuk sepenuhnya menghilangkan pertentangan antar-NIC, meminimalkan rentang yang tumpang tindih atau kurangi jumlah prosesor logis dalam rentang antarmuka elastic network tergantung pada beban kerja antarmuka yang diharapkan (dengan kata lain, antarmuka jaringan administratif volume rendah mungkin tidak memerlukan banyak antrian RSS yang ditetapkan). Juga, seperti yang disebutkan sebelumnya, berbagai komponen harus berjalan pada CPU 0, dan oleh karena itu kami sarankan untuk mengecualikannya dari semua konfigurasi RSS ketika v CPUs cukup tersedia.

Misalnya, ketika ada tiga antarmuka jaringan elastis pada instance 72 vCPU dengan 2 node NUMA dengan hyper-threading diaktifkan, perintah berikut menyebarkan beban jaringan antara CPUs keduanya tanpa tumpang tindih dan mencegah penggunaan inti 0 sepenuhnya.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Perhatikan bahwa pengaturan ini tetap ada untuk setiap adaptor jaringan. Jika sebuah instance diubah ukurannya menjadi satu dengan jumlah v yang berbedaCPUs, Anda harus mengevaluasi kembali konfigurasi RSS untuk setiap antarmuka elastic network yang diaktifkan. Dokumentasi Microsoft lengkap untuk cmdlet dapat ditemukan di sini: Set -. NetAdapterRss

Catatan khusus untuk beban kerja SQL: Kami juga menyarankan Anda meninjau pengaturan afinitas I/O thread Anda bersama dengan konfigurasi RSS elastic network interface Anda untuk meminimalkan I/O dan pertentangan jaringan untuk hal yang sama. CPUs Lihat Konfigurasi server: topeng afinitas.

Adaptor Kain Elastis untuk AI/ML dan beban kerja HPC di Amazon EC2

Elastic Fabric Adapter (EFA) adalah perangkat jaringan yang dapat Anda lampirkan ke instans Amazon EC2 untuk mempercepat aplikasi Artificial Intelligence (AI), Machine Learning (ML), dan High Performance Computing (HPC). EFA memungkinkan Anda mencapai kinerja aplikasi klaster AI/ML/HPC lokal, dengan skalabilitas, fleksibilitas, dan elastisitas yang disediakan oleh Cloud. AWS

EFA memberikan latensi yang lebih rendah dan lebih konsisten serta throughput yang lebih tinggi dibandingkan transportasi TCP yang secara tradisional digunakan dalam sistem HPC berbasis cloud. Ini meningkatkan kinerja komunikasi antar-instance yang sangat penting untuk penskalaan AI/ML dan aplikasi HPC. Hal ini dioptimalkan untuk bekerja pada infrastruktur AWS jaringan yang ada dan dapat skala tergantung pada persyaratan aplikasi.

EFA terintegrasi dengan Libfabric, dan mendukung Nvidia Collective Communications Library (NCCL) dan NVIDIA Inference Xfer Library (NIXL) untuk aplikasi AI dan ML, dan Open MPI 4.1 dan yang lebih baru dan Intel MPI 2019 Update 5 dan yang lebih baru untuk aplikasi HPC. NCCL dan MPI terintegrasi dengan Libfabric 1.7.0 dan yang lebih baru. NIXL terintegrasi dengan Libfabric 1.21.0 dan yang lebih baru.

EFA mendukung penulisan RDMA (Remote Direct Memory Access) pada sebagian besar jenis instans yang didukung yang memiliki Nitro versi 4 dan yang lebih baru. Pembacaan RDMA didukung

pada semua instance dengan Nitro versi 4 dan yang lebih baru. Untuk informasi selengkapnya, lihat Tipe instans yang didukung.

Daftar Isi

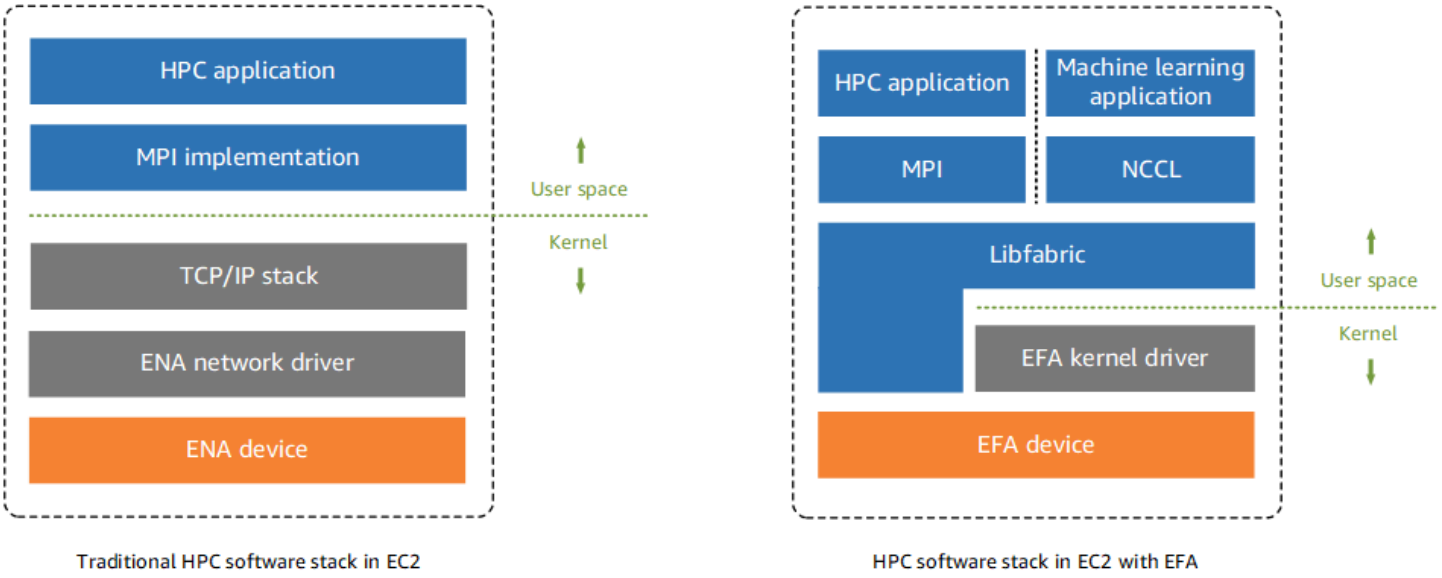
- Dasar-dasar EFA
- Antarmuka dan pustaka yang didukung
- Tipe instans yang didukung
- Sistem operasi yang didukung
- Batasan EFA
- Harga EFA
- Memulai EFA dan MPI untuk beban kerja HPC di Amazon EC2
- Memulai dengan EFA dan NCCL untuk beban kerja ML di Amazon EC2
- Memulai EFA dan NIXL untuk beban kerja inferensi di Amazon EC2
- Maksimalkan bandwidth jaringan pada instans Amazon EC2 dengan beberapa kartu jaringan
- Membuat dan melampirkan Adaptor Kain Elastis ke instans Amazon EC2
- Lepaskan dan hapus EFA dari instans Amazon EC2
- Pantau Adaptor Kain Elastis di Amazon EC2
- Memverifikasi penginstal EFA menggunakan checksum
- Catatan rilis Adaptor Kain Elastis

Dasar-dasar EFA

Perangkat EFA dapat dilampirkan ke instans EC2 dengan dua cara:

1. Menggunakan antarmuka EFA tradisional, juga disebut EFA dengan ENA, yang menciptakan perangkat EFA dan perangkat ENA.
2. Menggunakan antarmuka khusus EFA, yang hanya menciptakan perangkat EFA.

Perangkat EFA menyediakan kemampuan seperti built-in OS-bypass dan kontrol kemacetan melalui protokol Scalable Reliable Datagram (SRD). Fitur perangkat EFA memungkinkan fungsionalitas transportasi latensi rendah dan andal yang memungkinkan antarmuka EFA memberikan kinerja aplikasi yang lebih baik untuk aplikasi HPC dan ML di Amazon EC2. Sedangkan perangkat ENA menawarkan jaringan IP tradisional.



Secara tradisional, AI/ML aplikasi menggunakan NCCL dan NIXL (untuk inferensi terpilah). Aplikasi HPC menggunakan Message Passing Interface (MPI) untuk berinteraksi dengan transportasi jaringan sistem. Di AWS cloud, ini berarti bahwa antarmuka aplikasi dengan NCCL, NIXL, atau MPI, yang kemudian menggunakan TCP/IP tumpukan sistem operasi dan driver perangkat ENA untuk mengaktifkan komunikasi jaringan antar instance.

Dengan EFA tradisional (EFA dengan ENA) atau antarmuka khusus EFA, AI/ML aplikasi menggunakan NCCL dan NIXL (untuk inferensi terpilah). Aplikasi HPC menggunakan MPI, untuk berinteraksi langsung dengan API Libfabric. API Libfabric memintas kernel sistem operasi dan berkomunikasi secara langsung dengan perangkat ITEFA untuk menempatkan paket pada jaringan. Ini mengurangi overhead dan memungkinkan AI/ML dan aplikasi HPC berjalan lebih efisien.

> **Note**
>
> Libfabric adalah komponen inti dari kerangka OpenFabrics Interfaces (OFI), yang mendefinisikan dan mengekspor API ruang pengguna OFI. Untuk informasi lebih lanjut, lihat situs web Libfabric OpenFabrics.

Perbedaan antara antarmuka jaringan ENA, EFA, dan EFA

Amazon EC2 menyediakan dua jenis antarmuka jaringan:

- Antarmuka ENA menyediakan semua jaringan IP tradisional dan fitur routing yang diperlukan untuk mendukung jaringan IP untuk VPC. Untuk informasi selengkapnya, lihat Aktifkan jaringan yang disempurnakan dengan ENA pada instans EC2 Anda.
- Antarmuka EFA (EFA dengan ENA) menyediakan perangkat ENA untuk jaringan IP dan perangkat EFA untuk komunikasi latensi rendah dan throughput tinggi.
- Antarmuka khusus EFA hanya mendukung kemampuan perangkat EFA, tanpa perangkat ENA untuk jaringan IP tradisional.

Tabel berikut memberikan perbandingan antarmuka jaringan ENA, EFA, dan EFA saja.

	ENA	EFA (EFA dengan ENA)	Khusus EFA
Mendukung fungsionalitas jaringan IP	Ya	Ya	Tidak
Dapat ditugaskan IPv4 atau IPv6 alamat	Ya	Ya	Tidak
Dapat digunakan sebagai antarmuka jaringan utama misalnya	Ya	Ya	Tidak
Menghitung batas lampiran ENI misalnya	Ya	Ya	Ya
Dukungan tipe instans	Didukung pada semua jenis instans berbasis Nitro	Jenis instans yang didukung	Jenis instans yang didukung

	ENA	EFA (EFA dengan ENA)	Khusus EFA
Penamaan parameter di EC2 APIs	`interface`	`efa`	`efa-only`
Penamaan bidang di konsol EC2	Tidak ada pilihan	EFA dengan ENA	Khusus EFA

Antarmuka dan pustaka yang didukung

EFAs mendukung antarmuka dan pustaka berikut:

- Buka MPI 4.1 dan yang lebih baru
- Pembaruan 5 Intel MPI 2019 dan versi yang lebih baru
- NVIDIA Collective Communications Library (NCCL) 2.4.2 dan yang lebih baru
- NVIDIA Inference Xfer Library (NIXL) 1.0.0 dan yang lebih baru
- AWS Neuron SDK versi 2.3 dan yang lebih baru

Tipe instans yang didukung

Semua jenis contoh berikut mendukung EFA. Selain itu, tabel menunjukkan dukungan baca RDMA dan penulisan RDMA untuk jenis instance.

Nitro v6

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
Tujuan Umum		
m8a.48xlarge	Ya	Ya
m8a.logam-48xl	Ya	Ya
m8azn.24xlarge	Ya	Ya

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
m8azn.metal-24xl	Ya	Ya
m8gb.16xlarge	Ya	Ya
m8gb.24xlarge	Ya	Ya
m8gb.48xlarge	Ya	Ya
m8gb.metal-24xl	Ya	Ya
m8gb.logam-48xl	Ya	Ya
m8gn.16xlarge	Ya	Ya
m8gn.24xlarge	Ya	Ya
m8gn.48xlarge	Ya	Ya
m8gn.metal-24xl	Ya	Ya
m8gn.metal-48xl	Ya	Ya
m8i.48xlarge	Ya	Ya
m8i.96xlarge	Ya	Ya
m8i.logam-48xl	Ya	Ya
m8i.logam-96xl	Ya	Ya
m8id.48xlarge	Ya	Ya
m8id.96xlarge	Ya	Ya
m8id.metal-48xl	Ya	Ya
m8id.metal-96xl	Ya	Ya
Komputasi yang Dioptimalkan		
c8a.48xlarge	Ya	Ya

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
c8a.metal-48xl	Ya	Ya
c8gb.16xlarge	Ya	Ya
c8gb.24xlarge	Ya	Ya
c8gb.48xlarge	Ya	Ya
c8gb.metal-24xl	Ya	Ya
c8gb.metal-48xl	Ya	Ya
c8gn.16xlarge	Ya	Ya
c8gn.24xlarge	Ya	Ya
c8gn.48xlarge	Ya	Ya
c8gn.metal-24xl	Ya	Ya
c8gn.metal-48xl	Ya	Ya
c8i.48xlarge	Ya	Ya
c8i.96xlarge	Ya	Ya
c8i.logam-48xl	Ya	Ya
c8i.logam-96xl	Ya	Ya
c8id.48xlarge	Ya	Ya
c8id.96xlarge	Ya	Ya
c8id.metal-48xl	Ya	Ya
c8id.metal-96xl	Ya	Ya
Memori Dioptimalkan		
r8a.48xlarge	Ya	Ya

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
r8a.metal-48xl	Ya	Ya
r8gb.16xlarge	Ya	Ya
r8gb.24xlarge	Ya	Ya
r8gb.48xlarge	Ya	Ya
r8gb.metal-24xl	Ya	Ya
r8gb.metal-48xl	Ya	Ya
r8gn.16xlarge	Ya	Ya
r8gn.24xlarge	Ya	Ya
r8gn.48xlarge	Ya	Ya
r8gn.metal-24xl	Ya	Ya
r8gn.metal-48xl	Ya	Ya
r8i.48xlarge	Ya	Ya
r8i.96xlarge	Ya	Ya
r8i.logam-48xl	Ya	Ya
r8i.logam-96xl	Ya	Ya
r8id.48xlarge	Ya	Ya
r8id.96xlarge	Ya	Ya
r8id.metal-48xl	Ya	Ya
r8id.metal-96xl	Ya	Ya
x8aedz.24xlarge	Ya	Ya
x8aedz.metal-24xl	Ya	Ya

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
x8i.48xlarge	Ya	Ya
x8i.64xlarge	Ya	Ya
x8i.96xlarge	Ya	Ya
x8i.logam-48xl	Ya	Ya
x8i.logam-96xl	Ya	Ya
Penyimpanan Dioptimalkan		
i8ge.48xlarge	Ya	Tidak
i8ge.metal-48xl	Ya	Tidak
Komputasi yang Dipercepat		
g7e.8xlarge	Ya	Ya
g7e.12xlarge	Ya	Ya
g7e.24xlarge	Ya	Ya
g7e.48xlarge	Ya	Ya
p6-b200.48xlarge	Ya	Ya
p6-b300.48xlarge	Ya	Ya
Komputasi Performa Tinggi		
hpc8a.96xlarge	Ya	Ya

Nitro v5

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
Tujuan Umum		

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
m8g.24xlarge	Ya	Tidak
m8g.48xlarge	Ya	Tidak
m8g.logam-24xl	Ya	Tidak
m8g.logam-48xl	Ya	Tidak
m8gd.24xlarge	Tidak	Tidak
m8gd.48xlarge	Tidak	Tidak
m8gd.metal-24xl	Tidak	Tidak
m8gd.metal-48xl	Tidak	Tidak
Komputasi yang Dioptimalkan		
c7gn.16xlarge	Ya	Tidak
c7gn.logam	Ya	Tidak
c8g.24xlarge	Ya	Tidak
c8g.48xlarge	Ya	Tidak
c8g.logam-24xl	Ya	Tidak
c8g.logam-48xl	Ya	Tidak
c8gd.24xlarge	Tidak	Tidak
c8gd.48xlarge	Tidak	Tidak
c8gd.metal-24xl	Tidak	Tidak
c8gd.metal-48xl	Tidak	Tidak
Memori Dioptimalkan		
r8g.24xlarge	Tidak	Tidak

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
r8g.48xlarge	Tidak	Tidak
r8g.logam-24xl	Tidak	Tidak
r8g.logam-48xl	Tidak	Tidak
r8gd.24xlarge	Tidak	Tidak
r8gd.48xlarge	Tidak	Tidak
r8gd.metal-24xl	Tidak	Tidak
r8gd.metal-48xl	Tidak	Tidak
x8g.24xlarge	Tidak	Tidak
x8g.48xlarge	Tidak	Tidak
x8g.logam-24xl	Tidak	Tidak
x8g.logam-48xl	Tidak	Tidak
Penyimpanan Dioptimalkan		
i7ie.48xlarge	Ya	Tidak
i7ie.logam-48xl	Ya	Tidak
i8g.48xlarge	Tidak	Tidak
i8g.logam-48xl	Tidak	Tidak
Komputasi yang Dipercepat		
p5en.48xlarge	Ya	Ya
p6e-gb200.36xlarge	Ya	Ya
trn2.3xlarge	Ya	Ya
trn2.48xlarge	Ya	Ya

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
trn2u.48xlarge	Ya	Ya
Komputasi Performa Tinggi		
hpc7g.4xlarge	Ya	Tidak
hpc7g.8xlarge	Ya	Tidak
hpc7g.16xlarge	Ya	Tidak

Nitro v4

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
Tujuan Umum		
m6a.48xlarge	Ya	Ya
m6a.metal	Ya	Ya
m6i.32xlarge	Ya	Ya
m6i.metal	Ya	Ya
m6id.32xlarge	Ya	Ya
m6id.metal	Ya	Ya
m6idn.32xlarge	Ya	Ya
m6idn.metal	Ya	Ya
m6in.32xlarge	Ya	Ya
m6in.metal	Ya	Ya
m7a.48xlarge	Ya	Tidak
m7a.metal-48xl	Ya	Tidak

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
m7g.16xlarge	Ya	Tidak
m7g.metal	Ya	Tidak
m7gd.16xlarge	Ya	Tidak
m7gd.metal	Ya	Tidak
m7i.48xlarge	Ya	Tidak
m7i.metal-48xl	Ya	Tidak
Komputasi yang Dioptimalkan		
c6a.48xlarge	Ya	Ya
c6a.metal	Ya	Ya
c6gn.16xlarge	Ya	Ya
c6i.32xlarge	Ya	Ya
c6i.metal	Ya	Ya
c6id.32xlarge	Ya	Ya
c6id.metal	Ya	Ya
c6in.32xlarge	Ya	Ya
c6in.metal	Ya	Ya
c7a.48xlarge	Ya	Tidak
c7a.metal-48xl	Ya	Tidak
c7g.16xlarge	Ya	Ya
c7g.metal	Ya	Ya
c7gd.16xlarge	Ya	Tidak

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
c7gd.metal	Ya	Tidak
c7i.48xlarge	Ya	Tidak
c7i.metal-48xl	Ya	Tidak
Memori Dioptimalkan		
r6a.48xlarge	Ya	Ya
r6a.metal	Ya	Ya
r6i.32xlarge	Ya	Ya
r6i.metal	Ya	Ya
r6id.32xlarge	Ya	Ya
r6id.metal	Ya	Ya
r6idn.32xlarge	Ya	Ya
r6idn.metal	Ya	Ya
r6in.32xlarge	Ya	Ya
r6in.metal	Ya	Ya
r7a.48xlarge	Tidak	Tidak
r7a.metal-48xl	Tidak	Tidak
r7g.16xlarge	Tidak	Tidak
r7g.metal	Tidak	Tidak
r7gd.16xlarge	Tidak	Tidak
r7gd.logam	Tidak	Tidak
r7i.48xlarge	Tidak	Tidak

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
r7i.metal-48xl	Tidak	Tidak
r7iz.32xlarge	Tidak	Tidak
r7iz.metal-32xl	Tidak	Tidak
u7i-6tb.112xlarge	Ya	Ya
u7i-8tb.112xlarge	Ya	Ya
u7i-12tb.224xlarge	Ya	Ya
u7in-16tb.224xlarge	Ya	Ya
u7in-24tb.224xlarge	Ya	Ya
u7in-32tb.224xlarge	Ya	Ya
u7inh-32tb.480xlarge	Ya	Ya
x2idn.32xlarge	Ya	Ya
x2idn.metal	Ya	Ya
x2iedn.32xlarge	Ya	Ya
x2iedn.metal	Ya	Ya
Penyimpanan Dioptimalkan		
i4g.16xlarge	Ya	Ya
i4i.32xlarge	Ya	Ya
i4i.metal	Ya	Ya
i7i.24xlarge	Ya	Tidak
i7i.48xlarge	Ya	Tidak
i7i.logam-48xl	Ya	Tidak

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
im4gn.16xlarge	Ya	Ya
Komputasi yang Dipercepat		
f2.48xbesar	Ya	Ya
g6.8xlarge	Ya	Ya
g6.12xlarge	Ya	Ya
g6.16xlarge	Ya	Ya
g6.24xlarge	Ya	Ya
g6.48xlarge	Ya	Ya
g6e.8xlarge	Ya	Ya
g6e.12xlarge	Ya	Ya
g6e.16xlarge	Ya	Ya
g6e.24xlarge	Ya	Ya
g6e.48xlarge	Ya	Ya
gr6.8xbesar	Ya	Ya
p5.4xbesar	Ya	Ya
p5.48xlarge	Ya	Ya
p5e.48xlarge	Ya	Ya
trn1.32xlarge	Ya	Ya
trn1n.32xlarge	Ya	Ya
Komputasi Performa Tinggi		
hpc6a.48xlarge	Ya	Ya

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
hpc6id.32xlarge	Ya	Ya
hpc7a.12xlarge	Ya	Tidak
hpc7a.24xlarge	Ya	Tidak
hpc7a.48xlarge	Ya	Tidak
hpc7a.96xlarge	Ya	Tidak

Nitro v3

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
Tujuan Umum		
m5dn.24xlarge	Tidak	Tidak
m5dn.metal	Tidak	Tidak
m5n.24xlarge	Tidak	Tidak
m5n.metal	Tidak	Tidak
m5zn.12xlarge	Tidak	Tidak
m5zn.metal	Tidak	Tidak
Komputasi yang Dioptimalkan		
c5n.9xlarge	Tidak	Tidak
c5n.18xlarge	Tidak	Tidak
c5n.metal	Tidak	Tidak
Memori Dioptimalkan		
r5dn.24xlarge	Tidak	Tidak

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
r5dn.metal	Tidak	Tidak
r5n.24xlarge	Tidak	Tidak
r5n.metal	Tidak	Tidak
x2iezn.12xlarge	Tidak	Tidak
x2iezn.metal	Tidak	Tidak
Penyimpanan Dioptimalkan		
i3en.12xlarge	Tidak	Tidak
i3en.24xlarge	Tidak	Tidak
i3en.metal	Tidak	Tidak
Komputasi yang Dipercepat		
dl1.24xlarge	Ya	Tidak
dl2q.24xlarge	Tidak	Tidak
g4dn.8xlarge	Tidak	Tidak
g4dn.12xlarge	Tidak	Tidak
g4dn.16xlarge	Tidak	Tidak
g4dn.metal	Tidak	Tidak
g5.8xlarge	Tidak	Tidak
g5.12xlarge	Tidak	Tidak
g5.16xlarge	Tidak	Tidak
g5.24xlarge	Tidak	Tidak
g5.48xlarge	Tidak	Tidak

Tipe instans	Dukungan baca RDMA	Dukungan tulis RDMA
inf1.24xlarge	Tidak	Tidak
p3dn.24xlarge	Tidak	Tidak
p4d.24xlarge	Ya	Tidak
p4de.24xlarge	Ya	Tidak
vt1.24xlarge	Tidak	Tidak
Generasi Sebelumnya		
p3dn.24xlarge	Tidak	Tidak

Untuk melihat jenis instans yang tersedia yang mendukung EFAs di Wilayah tertentu

Tipe instans yang tersedia berbeda-beda menurut Wilayah. Untuk melihat jenis instance yang tersedia yang mendukung EFAs di Region, gunakan describe-instance-typesperintah dengan `--region` parameter. Sertakan parameter `--filters` untuk cakupan hasil ke tipe instans yang mendukung EFA dan `--query` parameter untuk cakupan output ke nilai `InstanceType`.

```
aws ec2 describe-instance-types \
    --region us-east-1  \
    --filters Name=network-info.efa-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]"  \
    --output text | sort
```

Sistem operasi yang didukung

Dukungan sistem operasi berbeda tergantung pada jenis prosesor. Tabel berikut menunjukkan sistem operasi yang didukung.

Sistem operasi	Intel/AMD (**x86_64**) jenis instans	AWS Graviton (**arm64**) jenis contoh
Amazon Linux 2023	✓	✓

Sistem operasi	Intel/AMD (**x86_64**) jenis instans	AWS Graviton (**arm64**) jenis contoh
Amazon Linux 2	✓	✓
RHEL 8 dan 9	✓	✓
Debian 11, 12, dan 13	✓	✓
Rocky Linux 8 dan 9	✓	✓
Ubuntu 22.04 dan 24.04	✓	✓
SUSE Linux Enterprise 15 SP2 dan yang lebih baru	✓	✓
openSUSE Leap 15.5 dan yang lebih baru	✓	

> **Note**
>
> Beberapa sistem operasi yang terdaftar mungkin tidak didukung dengan Intel MPI. Jika Anda menggunakan Intel MPI, lihat dokumentasi Intel MPI untuk memverifikasi dukungan untuk sistem operasi Anda.

Batasan EFA

EFAs memiliki batasan berikut:

- Penulisan RDMA tidak didukung dengan semua jenis instance. Untuk informasi selengkapnya, lihat Tipe instans yang didukung.
- Lalu lintas EFA [1] antara instans P4 d/P4de/DL 1 dan jenis instans lainnya saat ini tidak didukung.

- Tipe instans yang mendukung beberapa kartu jaringan dapat dikonfigurasi dengan satu EFA per kartu jaringan. Semua tipe instans yang didukung hanya mendukung satu EFA per instans.
- `c7g.16xlarge`,`m7g.16xlarge`, dan Instans `r7g.16xlarge` Khusus dan Host Khusus tidak didukung saat EFA dilampirkan.
- Lalu lintas EFA [1] tidak dapat melintasi Availability Zone atau VPCs. Ini tidak berlaku untuk lalu lintas IP normal dari perangkat ENA antarmuka EFA.
- Lalu lintas EFA [1] tidak dapat dirutekan. Lalu lintas IP normal dari perangkat ENA antarmuka EFA tetap dapat dirutekan.
- EFA tidak didukung pada AWS Outposts.
- Perangkat EFA dari antarmuka EFA (EFA dengan ENA) didukung pada instance Windows hanya untuk AWS Cloud Digital Interface aplikasi berbasis Software Development Kit (AWS CDI SDK). Jika Anda melampirkan antarmuka EFA (EFA dengan ENA) ke instance Windows untuk aplikasi berbasis SDK non-CDI, itu berfungsi sebagai antarmuka ENA, tanpa kemampuan perangkat EFA tambahan. Antarmuka khusus EFA tidak didukung oleh aplikasi AWS CDI berbasis pada Windows atau Linux. Untuk informasi selengkapnya, lihat Panduan Pengguna Kit Pengembangan AWS Cloud Digital Interface Perangkat Lunak (AWS CDI SDK).

[1] Lalu lintas EFA mengacu pada lalu lintas yang ditransmisikan melalui perangkat EFA baik EFA (EFA dengan ENA) atau antarmuka khusus EFA.

Harga EFA

EFA tersedia sebagai fitur jaringan Amazon EC2 opsional yang dapat Anda aktifkan pada instans apa pun yang didukung tanpa biaya tambahan.

Memulai EFA dan MPI untuk beban kerja HPC di Amazon EC2

Tutorial berikut membantu Anda meluncurkan klaster instans yang diaktifkan EFA dan MPI untuk beban kerja HPC.

> **Note**
>
> Instance `u7i-12tb.224xlargeu7in-16tb.224xlarge`,`u7in-24tb.224xlarge`, dan `u7in-32tb.224xlarge` instans dapat menjalankan hingga 128 proses MPI paralel dengan Open MPI atau hingga 256 proses MPI paralel dengan Intel MPI.

Tugas

- Langkah 1: Siapkan grup keamanan yang diaktifkan EFA
- Langkah 2: Luncurkan instans sementara
- Langkah 3: Instal perangkat lunak EFA
- Langkah 4: (Opsional) Mengaktifkan Open MPI 5
- Langkah 5: (Opsional) Instal Intel MPI
- Langkah 6: Menonaktifkan perlindungan ptrace
- Langkah 7. Konfirmasi instalasi
- Langkah 8: Menginstal aplikasi HPC Anda
- Langkah 9: Membuat AMI yang diaktifkan EFA
- Langkah 10: Meluncurkan instans yang diaktifkan EFA ke dalam grup penempatan klaster
- Langkah 11: Mengakhiri instans sementara
- Langkah 12: Mengaktifkan SSH tanpa kata sandi

Langkah 1: Siapkan grup keamanan yang diaktifkan EFA

EFA memerlukan grup keamanan yang memungkinkan semua lalu lintas masuk dan keluar ke dan dari grup keamanan itu sendiri. Prosedur berikut membuat grup keamanan yang memungkinkan semua lalu lintas masuk dan keluar ke dan dari dirinya sendiri, dan yang memungkinkan lalu lintas SSH masuk dari IPv4 alamat apa pun untuk konektivitas SSH.

> **Important**
>
> Grup keamanan ini ditujukan untuk tujuan pengujian saja. Untuk lingkungan produksi Anda, kami sarankan Anda membuat aturan SSH masuk yang memungkinkan lalu lintas hanya dari alamat IP dari mana Anda terhubung, seperti alamat IP komputer Anda, atau berbagai alamat IP di jaringan lokal Anda.

Untuk skenario lainnya, lihat Aturan-aturan grup keamanan untuk kasus penggunaan yang berbeda.

Untuk membuat grup keamanan yang diaktifkan EFA

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Dalam panel navigasi, pilih Grup Keamanan, lalu pilih Buat grup keamanan.
3. Di jendela Buat Grup Keamanan, lakukan hal berikut:
   a. Untuk Nama grup keamanan, masukkan nama deskriptif untuk grup keamanan, seperti `EFA-enabled security group`.
   b. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat grup keamanan.
   c. Untuk VPC, pilih VPC untuk tujuan peluncuran instans Anda yang didukung EFA.
   d. Pilih Buat grup keamanan.
4. Pilih grup keamanan yang Anda buat, dan pada tab Detail, salin ID grup keamanan.
5. Dengan grup keamanan yang masih dipilih, pilih Tindakan, Edit aturan masuk, lalu lakukan hal berikut:
   a. Pilih Tambahkan aturan.
   b. Untuk Tipe, pilih Semua lalu lintas.
   c. Untuk Tipe sumber, pilih Kustom dan tempelkan ID grup keamanan yang Anda salin ke dalam bidang.
   d. Pilih Tambahkan aturan.
   e. Untuk Tipe, pilih SSH.
   f. Untuk jenis Sumber, pilih Anywhere- IPv4.
   g. Pilih Simpan aturan.
6. Dengan grup keamanan yang masih dipilih, pilih Tindakan, Edit aturan keluar, lalu lakukan hal berikut:
   a. Pilih Tambahkan aturan.
   b. Untuk Tipe, pilih Semua lalu lintas.
   c. Untuk Tipe tujuan, pilih Kustom dan tempelkan ID grup keamanan yang Anda salin ke dalam bidang.
   d. Pilih Simpan aturan.

Langkah 2: Luncurkan instans sementara

Luncurkan instans sementara yang dapat Anda gunakan untuk menginstal dan mengonfigurasi komponen perangkat lunak EFA. Anda menggunakan instans ini untuk membuat AMI yang diaktifkan EFA sebagai tempat untuk meluncurkan instans Anda yang diaktifkan EFA.

Untuk meluncurkan instans sementara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih Luncurkan Instans untuk membuka wizard peluncuran instans baru.
3. (Opsional) Di bagian Nama dan tanda, berikan nama untuk instans, seperti `EFA-instance`. Nama ditetapkan ke instans sebagai tanda sumber daya (`Name=`*`EFA-instance`*).
4. Di bagian Application and OS Images, pilih AMI untuk salah satu sistem operasi yang didukung.
5. Di bagian Tipe instans, pilih tipe instans yang didukung.
6. Pada bagian Pasangan kunci, pilih pasangan kunci yang akan digunakan untuk instans.
7. Di bagian Pengaturan jaringan, pilih Edit, lalu lakukan hal berikut:

   a. Untuk Subnet, pilih subnet untuk meluncurkan instans. Jika Anda tidak memilih subnet, Anda tidak dapat mengaktifkan instans untuk EFA.

   b. Untuk Firewall (grup keamanan), pilih Pilih grup keamanan yang ada, lalu pilih grup keamanan yang Anda buat di langkah sebelumnya.

   c. Perluas bagian Konfigurasi jaringan lanjutan.

      Untuk antarmuka Jaringan 1, pilih Indeks kartu jaringan = 0, Indeks perangkat = 0, dan Jenis antarmuka = EFA dengan ENA.

      (Opsional) Jika Anda menggunakan jenis instans multi-kartu, seperti **`p4d.24xlarge`** atau**`p5.48xlarge`**, untuk setiap antarmuka jaringan tambahan yang diperlukan, pilih Tambahkan antarmuka jaringan, untuk indeks kartu jaringan pilih indeks berikutnya yang tidak digunakan, lalu pilih Indeks perangkat = 1 dan Jenis antarmuka = EFA dengan ENA atau EFA saja.
8. Di bagian Penyimpanan, konfigurasikan volume sesuai kebutuhan.
9. Di panel Ringkasan di sebelah kanan, pilih Luncurkan instans.

> **Note**
>
> Pertimbangkan untuk mewajibkan penggunaan IMDSv2 untuk instance sementara serta AMI yang akan Anda buat di Langkah 9 kecuali Anda telah menetapkan IMDSv2 sebagai default untuk akun tersebut. Untuk informasi selengkapnya tentang langkah-langkah IMDSv2 konfigurasi, lihatMengonfigurasi opsi metadata instans untuk instans baru.

Langkah 3: Instal perangkat lunak EFA

Instal kernel yang diaktifkan EFA, driver EFA, Libfabric, dan tumpukan Open MPI yang diperlukan untuk mendukung EFA pada instans sementara Anda.

Langkah-langkahnya berbeda tergantung pada apakah Anda bermaksud untuk menggunakan EFA dengan Open MPI, Intel MPI, atau dengan Open MPI dan Intel MPI.

> **Note**
>
> Beberapa sistem operasi mungkin tidak didukung dengan Intel MPI. Jika Anda menggunakan Intel MPI, lihat dokumentasi Intel MPI untuk memverifikasi dukungan untuk sistem operasi Anda.

Untuk menginstal perangkat lunak EFA

1. Hubungkan ke instans yang Anda luncurkan. Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..
2. Untuk memastikan bahwa semua paket perangkat lunak Anda telah diperbarui, lakukan pembaruan perangkat lunak cepat di instans Anda. Proses ini mungkin memerlukan waktu beberapa menit.
   - Amazon Linux 2023, Amazon Linux 2, RHEL 8/9, Rocky Linux 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu dan Debian

     ```
     $ sudo apt-get update && sudo apt-get upgrade -y
     ```

   - SUSE Linux Enterprise

     ```
     $ sudo zypper update -y
     ```

3. Boot ulang dan terhubung kembali ke instans Anda.
4. Unduh file penginstalan perangkat lunak EFA. File penginstalan perangkat lunak dikemas menjadi file tarball (`.tar.gz`) yang dikompresi. Untuk mengunduh versi stabil terbaru, gunakan perintah berikut.

Anda juga bisa mendapatkan versi terbaru dengan mengganti nomor versi dengan `latest` dalam perintah sebelumnya.

```
$ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz
```

5. (Opsional) Verifikasi keaslian dan integritas file tarball EFA (`.tar.gz`).

   Kami menyarankan Anda melakukan hal ini untuk memverifikasi identitas penerbit perangkat lunak dan memeriksa apakah file tersebut tidak diubah atau rusak sejak file tersebut diterbitkan. Jika Anda tidak ingin memverifikasi file tarball, lewati langkah ini.

   > **Note**
   >
   > Atau, jika Anda lebih suka memverifikasi file tarball dengan menggunakan MD5 atau SHA256 checksum sebagai gantinya, lihat. Memverifikasi penginstal EFA menggunakan checksum

   a. Unduh kunci GPG publik dan impor ke dalam keyring Anda.

      ```
      $ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
      import aws-efa-installer.key
      ```

      Perintah tersebut harus mengembalikan nilai kunci. Catat nilai kunci, karena Anda membutuhkannya di langkah selanjutnya.

   b. Verifikasi sidik jari kunci GPG. Jalankan perintah berikut dan tentukan nilai kunci dari langkah sebelumnya.

      ```
      $ gpg --fingerprint key_value
      ```

      Perintah tersebut harus mengembalikan sidik jari yang identik dengan `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Jika sidik jari tidak cocok, jangan jalankan skrip instalasi EFA, dan hubungi Dukungan.

   c. Unduh file tanda tangan dan verifikasi tanda tangan pada file tarball EFA.

      ```
      $ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz.sig
       && gpg --verify ./aws-efa-installer-1.47.0.tar.gz.sig
      ```

Berikut ini adalah contoh output.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Jika hasilnya mencakup `Good signature`, dan sidik jari cocok dengan sidik jari yang dikembalikan di langkah sebelumnya, lanjutkan ke langkah berikutnya. Jika tidak, jangan jalankan skrip instalasi EFA, dan hubungi Dukungan.

6. Ekstraksi file dari file `.tar.gz` yang dikompresi dan navigasi ke dalam direktori yang diekstraksi.

```
$ tar -xf aws-efa-installer-1.47.0.tar.gz && cd aws-efa-installer
```

7. Instal perangkat lunak EFA. Lakukan salah satu langkah berikut sesuai dengan kasus penggunaan Anda.

> **Note**
>
> EFA tidak mendukung NVIDIA GPUDirect dengan SUSE Linux. Jika menggunakan SUSE Linux, Anda juga harus menentukan opsi `--skip-kmod` untuk mencegah penginstalan kmod. Secara default, SUSE Linux tidak mengizinkan modul out-of-tree kernel.

Open MPI and Intel MPI

Jika bermaksud untuk menggunakan EFA dengan Open MPI dan MPI Intel, Anda harus menginstal perangkat lunak EFA dengan Libfabric dan Open MPI, serta harus menyelesaikan Langkah 5: Menginstal MPI Intel.

Untuk menginstal perangkat lunak EFA dengan Libfabric dan Open MPI, jalankan perintah berikut.

> **Note**
>
> Dari EFA 1.30.0, Open MPI 4.1 dan Open MPI 5 diinstal secara default. Anda dapat secara opsional menentukan versi Open MPI yang ingin diinstal. Untuk menginstal hanya Buka MPI 4.1, sertakan`--mpi=openmpi4`. Untuk menginstal Open MPI 5 saja, sertakan `--mpi=openmpi5`. Untuk menginstal keduanya, hilangkan opsi `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric diinstal ke `/opt/amazon/efa`. Buka MPI 4.1 diinstal ke`/opt/amazon/openmpi`. Open MPI 5 diinstal ke `/opt/amazon/openmpi5`.

Open MPI only

Jika bermaksud untuk menggunakan EFA dengan Open MPI saja, Anda harus menginstal perangkat lunak EFA dengan Libfabric dan Open MPI. Anda juga dapat melewati Langkah 5: Menginstal MPI Intel. Untuk menginstal perangkat lunak EFA dengan Libfabric dan Open MPI, jalankan perintah berikut.

> **Note**
>
> Dari EFA 1.30.0, Open MPI 4.1 dan Open MPI 5 diinstal secara default. Anda dapat secara opsional menentukan versi Open MPI yang ingin diinstal. Untuk menginstal hanya Buka MPI 4.1, sertakan`--mpi=openmpi4`. Untuk menginstal Open MPI 5 saja, sertakan `--mpi=openmpi5`. Untuk menginstal keduanya, hilangkan opsi `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric diinstal ke `/opt/amazon/efa`. Buka MPI 4.1 diinstal ke`/opt/amazon/openmpi`. Open MPI 5 diinstal ke `/opt/amazon/openmpi5`.

Intel MPI only

Jika Anda berniat untuk menggunakan EFA dengan hanya Intel MPI, Anda harus menginstal perangkat lunak EFA tanpa Libfabric dan Open MPI. Dalam kasus ini, Intel MPI menggunakan Libfabric-nya yang tertanam. Jika memilih untuk melakukan ini, Anda harus menyelesaikan Langkah 5: Menginstal MPI Intel.

Untuk menginstal perangkat lunak EFA tanpa Libfabric dan Open MPI, jalankan perintah berikut.

```
$ sudo ./efa_installer.sh -y --minimal
```

8. Jika penginstal EFA meminta Anda untuk me-reboot instans, lakukanlah dan kemudian sambungkan kembali ke instans. Jika tidak, log out dari instans lalu log kembali untuk menyelesaikan penginstalan.
9. Hapus tarball yang tidak terkompresi dan tarball itu sendiri. Jika tidak, ini akan disertakan dalam AMI berkemampuan EFA yang Anda buat, meningkatkan ukurannya.

Langkah 4: (Opsional) Mengaktifkan Open MPI 5

> **Note**
>
> Lakukan langkah ini hanya jika Anda bermaksud menggunakan Open MPI 5.

Dari EFA 1.30.0, Open MPI 4.1 dan Open MPI 5 diinstal secara default. Atau, Anda dapat memilih untuk menginstal hanya Open MPI 4.1 atau Open MPI 5.

Jika memilih untuk menginstal Open MPI 5 pada Langkah 3: Menginstal perangkat lunak EFA, dan bermaksud menggunakannya, Anda harus melakukan langkah-langkah berikut untuk mengaktifkannya.

Untuk mengaktifkan Open MPI 5

1. Tambahkan Open MPI 5 ke variabel lingkungan PATH.

```
$ module load openmpi5
```

2. Verifikasi bahwa Open MPI 5 aktif untuk digunakan.

```
$ which mpicc
```

Perintah harus menampilkan direktori penginstalan Open MPI 5 - `/opt/amazon/openmpi5`.

3. (Opsional) Untuk memastikan bahwa Open MPI 5 ditambahkan ke variabel lingkungan PATH setiap kali instans dimulai, lakukan hal berikut:

   bash shell

   Tambahkan `module load openmpi5` ke `/home/`*`username`*`/.bashrc` dan `/home/`*`username`*`/.bash_profile`.

   csh and tcsh shells

   Tambahkan `module load openmpi5` ke `/home/`*`username`*`/.cshrc`.

Jika Anda perlu menghapus Open MPI 5 dari variabel lingkungan PATH, jalankan perintah berikut dan hapus perintah dari skrip startup shell.

```
$ module unload openmpi5
```

Langkah 5: (Opsional) Instal Intel MPI

> **Important**
>
> Lakukan langkah ini hanya jika Anda ingin menggunakan Intel MPI. Jika Anda hanya ingin menggunakan Open MPI, lewati langkah ini.

Intel MPI membutuhkan instalasi tambahan dan konfigurasi variabel lingkungan.

Prasyarat

Pastikan bahwa pengguna yang melakukan langkah-langkah berikut ini memiliki izin sudo.

Untuk menginstal Intel MPI

1. Untuk mengunduh skrip penginstalan Intel MPI, lakukan hal berikut

   a. Kunjungi situs web Intel.

b. Di bagian Perpustakaan Intel MPI di halaman web, pilih tautan untuk penginstal Intel MPI Library for Linux Offline.

2. Jalankan skrip penginstalan yang Anda unduh di langkah sebelumnya.

```
$ sudo bash installation_script_name.sh
```

3. Di installer, pilih Accept & install.
4. Baca Program Peningkatan Intel, pilih opsi yang sesuai, lalu pilih Mulai Instalasi.
5. Saat instalasi selesai, pilih Tutup.
6. Secara default, Intel MPI menggunakan Libfabric (internal) yang disematkan. Anda dapat mengonfigurasi Intel MPI untuk menggunakan Libfabric yang dikirimkan dengan penginstal EFA sebagai gantinya. Biasanya, installer EFA dikirimkan dengan versi Libfabric yang lebih baru daripada Intel MPI. Dalam beberapa kasus, Libfabric yang dikirimkan dengan installer EFA lebih berperforma daripada Intel MPI. Untuk mengonfigurasi Intel MPI agar menggunakan Libfabric yang dikirimkan bersama penginstal EFA, lakukan salah satu hal berikut tergantung pada shell Anda.

   bash shells

   Tambahkan pernyataan berikut ke /home/*username*/.bashrc dan /home/*username*/.bash_profile.

   ```
   export I_MPI_OFI_LIBRARY_INTERNAL=0
   ```

   csh and tcsh shells

   Tambahkan pernyataan berikut ke /home/*username*/.cshrc.

   ```
   setenv I_MPI_OFI_LIBRARY_INTERNAL 0
   ```

7. Tambahkan perintah source berikut ke skrip shell Anda untuk sumber skrip `vars.sh` dari direktori instalasi untuk mengatur lingkungan kompiler setiap kali instans dimulai. Lakukan salah satu langkah berikut sesuai dengan shell Anda.

   bash shells

   Tambahkan pernyataan berikut ke /home/*username*/.bashrc dan /home/*username*/.bash_profile.

```
source /opt/intel/oneapi/mpi/latest/env/vars.sh
```

csh and tcsh shells

Tambahkan pernyataan berikut ke /home/*username*/.cshrc.

```
source /opt/intel/oneapi/mpi/latest/env/vars.csh
```

8. Secara default, jika EFA tidak tersedia karena kesalahan konfigurasi, Intel MPI default ke tumpukan TCP/IP jaringan, yang mungkin mengakibatkan kinerja aplikasi lebih lambat. Anda dapat mencegahnya dengan mengatur `I_MPI_OFI_PROVIDER` ke `efa`. Hal ini menyebabkan Intel MPI gagal dengan kesalahan berikut jika EFA tidak tersedia:

```
Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
 error,
MPIR_Init_thread (XXX).......:
MPID_Init (XXXX).............:
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX)...........:
find_provider (XXXX).........:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Lakukan salah satu langkah berikut sesuai dengan shell Anda.

bash shells

Tambahkan pernyataan berikut ke /home/*username*/.bashrc dan /home/*username*/.bash_profile.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Tambahkan pernyataan berikut ke /home/*username*/.cshrc.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Secara default, Intel MPI tidak mencetak informasi debugging. Anda dapat menentukan tingkat verbositas yang berbeda untuk mengontrol informasi debugging. Nilai yang mungkin (dalam

urutan jumlah detail yang mereka berikan) adalah: `0` (default), `1`, `2`, `3`, `4`, `5`. Level `1` dan lebih tinggi mencetak `libfabric version` dan `libfabric provider`. Gunakan `libfabric version` untuk memeriksa apakah Intel MPI menggunakan Libfabric internal atau Libfabric yang dikirimkan bersama penginstal EFA. Jika menggunakan Libfabric internal, versinya berakhiran dengan `impi`. Gunakan `libfabric provider` untuk memeriksa dengan Intel MPI menggunakan EFA atau jaringan. TCP/IP Jika menggunakan EFA, nilainya adalah `efa`. Jika menggunakan TCP/IP, nilainya adalah `tcp;ofi_rxm`.

Untuk mengaktifkan informasi debugging, lakukan salah satu hal berikut sesuai dengan shell Anda.

bash shells

Tambahkan pernyataan berikut ke /home/*username*/.bashrc dan /home/*username*/.bash_profile.

```
export I_MPI_DEBUG=value
```

csh and tcsh shells

Tambahkan pernyataan berikut ke /home/*username*/.cshrc.

```
setenv I_MPI_DEBUG value
```

10. Secara default, Intel MPI menggunakan memori bersama (`shm`) sistem operasi untuk komunikasi intra-simpul, dan menggunakan Libfabric (`ofi`) hanya untuk komunikasi antar simpul. Umumnya, konfigurasi ini memberikan performa terbaik. Namun, dalam beberapa kasus kain Intel MPI shm dapat menyebabkan aplikasi tertentu menggantung tanpa batas waktu.

    Untuk mengatasi masalah ini, Anda dapat memaksa Intel MPI untuk menggunakan Libfabric untuk komunikasi intra-simpul dan antar-simpul. Untuk melakukannya, lakukan salah satu langkah berikut sesuai dengan shell Anda.

    bash shells

    Tambahkan pernyataan berikut ke /home/*username*/.bashrc dan /home/*username*/.bash_profile.

    ```
    export I_MPI_FABRICS=ofi
    ```

csh and tcsh shells

Tambahkan pernyataan berikut ke /home/*username*/.cshrc.

```
setenv I_MPI_FABRICS ofi
```

> **Note**
>
> Penyedia Libfabric EFA menggunakan memori bersama sistem operasi untuk komunikasi intra-simpul. Ini berarti bahwa pengaturan `I_MPI_FABRICS` untuk `ofi` menghasilkan performa yang mirip dengan konfigurasi `shm:ofi` default.

11. Keluar dari instans lalu masuk kembali.

Jika Anda tidak ingin menggunakan Intel MPI lagi, hapus variabel lingkungan dari skrip startup shell.

Langkah 6: Menonaktifkan perlindungan ptrace

Untuk meningkatkan performa aplikasi HPC Anda, Libfabric menggunakan memori lokal instans untuk komunikasi antarproses ketika proses berjalan pada instans yang sama.

Fitur memori bersama menggunakan Cross Memory Attach (CMA), yang tidak didukung oleh perlindungan ptrace. Jika Anda menggunakan distribusi Linux yang memiliki perlindungan ptrace yang diaktifkan secara default, seperti Ubuntu, Anda harus menonaktifkannya. Jika distribusi Linux Anda tidak memiliki perlindungan ptrace yang diaktifkan secara default, lewati langkah ini.

Untuk menonaktifkan perlindungan ptrace

Lakukan salah satu langkah berikut:

- Untuk menonaktifkan sementara perlindungan ptrace untuk tujuan pengujian, jalankan perintah berikut.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Untuk menonaktifkan perlindungan ptrace secara permanen, tambahkan `kernel.yama.ptrace_scope = 0` ke `/etc/sysctl.d/10-ptrace.conf` dan nyalakan ulang instans.

Langkah 7. Konfirmasi instalasi

Untuk mengkonfirmasi instalasi yang berhasil

1. Untuk mengonfirmasi bahwa MPI berhasil diinstal, jalankan perintah berikut:

   ```
   $ which mpicc
   ```

   - Untuk Open MPI, jalur yang dikembalikan harus menyertakan `/opt/amazon/`
   - Untuk Intel MPI, jalur yang dikembalikan harus menyertakan `/opt/intel/`. Jika Anda tidak mendapatkan output yang diharapkan, pastikan Anda telah mendapatkan skrip Intel MPI `vars.sh`.
2. Untuk mengonfirmasi bahwa komponen perangkat lunak EFA dan Libfabric berhasil diinstal, jalankan perintah berikut.

   ```
   $ fi_info -p efa -t FI_EP_RDM
   ```

   Perintah tersebut harus mengembalikan informasi tentang antarmuka Libfabric EFA. Contoh berikut menunjukkan output perintah.

   ```
   provider: efa
       fabric: EFA-fe80::94:3dff:fe89:1b70
       domain: efa_0-rdm
       version: 2.0
       type: FI_EP_RDM
       protocol: FI_PROTO_EFA
   ```

Langkah 8: Menginstal aplikasi HPC Anda

Instal aplikasi HPC di instans sementara. Prosedur penginstalan bervariasi tergantung pada aplikasi HPC tertentu. Untuk informasi selengkapnya, lihat Mengelola perangkat lunak pada AL2 instans Anda di Panduan Pengguna Amazon Linux 2.

> **Note**
>
> Lihat dokumentasi aplikasi HPC Anda untuk petunjuk penginstalan.

Langkah 9: Membuat AMI yang diaktifkan EFA

Setelah menginstal komponen perangkat lunak yang diperlukan, Anda membuat AMI yang dapat digunakan kembali untuk meluncurkan instans Anda dengan EFA yang diaktifkan.

Untuk membuat AMI dari instans sementara Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans sementara yang Anda buat dan pilih Tindakan, Gambar, Buat gambar.
4. Untuk Buat gambar, lakukan hal berikut:
   a. Untuk Nama gambar, masukkan nama deskriptif untuk AMI.
   b. (Opsional) Untuk Deskripsi gambar, masukkan deskripsi singkat tentang tujuan AMI.
   c. Pilih Buat gambar.
5. Di panel navigasi, pilih AMIs.
6. Temukan AMI yang Anda buat dalam daftar. Tunggu hingga status berubah dari `pending` menjadi `available` sebelum melanjutkan ke langkah berikutnya.

Langkah 10: Meluncurkan instans yang diaktifkan EFA ke dalam grup penempatan klaster

Luncurkan instans yang diaktifkan EFA Anda ke dalam grup penempatan klaster menggunakan AMI yang diaktifkan EFA yang Anda buat di Langkah 7, dan grup keamanan yang diaktifkan EFA yang Anda buat di Langkah 1.

> **Note**
>
> - Meluncurkan instans yang diaktifkan EFA ke dalam grup penempatan kluster bukanlah persyaratan mutlak. Namun, kami menyarankan Anda untuk menjalankan instans yang diaktifkan EFA dalam grup penempatan klaster saat instans diluncurkan ke grup dengan latensi rendah di Zona Ketersediaan tunggal.
> - Untuk memastikan kapasitas tersedia saat Anda menskalakan instans klaster, Anda dapat membuat Reservasi Kapasitas untuk grup penempatan klaster Anda. Untuk informasi selengkapnya, lihat Gunakan Reservasi Kapasitas dengan grup penempatan klaster.

Untuk meluncurkan sebuah instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih Luncurkan Instans untuk membuka wizard peluncuran instans baru.
3. (Opsional) Di bagian Nama dan tanda, berikan nama untuk instans, seperti `EFA-instance`. Nama ditetapkan ke instans sebagai tanda sumber daya (`Name=`*`EFA-instance`*).
4. Di bagian Application and OS ImagesAMIs, pilih My, lalu pilih AMI yang Anda buat pada langkah sebelumnya.
5. Di bagian Tipe instans, pilih tipe instans yang didukung.
6. Pada bagian Pasangan kunci, pilih pasangan kunci yang akan digunakan untuk instans.
7. Di bagian Pengaturan jaringan, pilih Edit, lalu lakukan hal berikut:

   a. Untuk Subnet, pilih subnet untuk meluncurkan instans. Jika Anda tidak memilih subnet, Anda tidak dapat mengaktifkan instans untuk EFA.

   b. Untuk Firewall (grup keamanan), pilih Pilih grup keamanan yang ada, lalu pilih grup keamanan yang Anda buat di langkah sebelumnya.

   c. Perluas bagian Konfigurasi jaringan lanjutan.

      Untuk antarmuka Jaringan 1, pilih Indeks kartu jaringan = 0, Indeks perangkat = 0, dan Jenis antarmuka = EFA dengan ENA.

      (Opsional) Jika Anda menggunakan jenis instans multi-kartu, seperti **`p4d.24xlarge`** atau**`p5.48xlarge`**, untuk setiap antarmuka jaringan tambahan yang diperlukan, pilih Tambahkan antarmuka jaringan, untuk indeks kartu jaringan pilih indeks berikutnya yang tidak digunakan, lalu pilih Indeks perangkat = 1 dan Jenis antarmuka = EFA dengan ENA atau EFA saja.
8. (Opsional) Di bagian Penyimpanan, konfigurasikan volume sesuai kebutuhan.
9. Di bagian Detail lanjutan, untuk nama grup Penempatan, pilih grup penempatan klaster untuk meluncurkan instans. Jika Anda perlu membuat grup penempatan klaster baru, pilih Buat grup penempatan baru.
10. Di panel Ringkasan di sebelah kanan, untuk Jumlah instans, masukkan jumlah instans yang diaktifkan EFA yang ingin Anda luncurkan, lalu pilih Luncurkan instans.

Langkah 11: Mengakhiri instans sementara

Pada titik ini, Anda tidak lagi memerlukan instance yang Anda luncurkan di Langkah 2. Anda dapat mengakhiri instans agar biaya tidak dibebankan lagi padanya.

Untuk mengakhiri instans sementara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance sementara yang Anda buat lalu pilih Actions, Instance state, Terminate (delete) instance.
4. Saat diminta konfirmasi, pilih Hentikan (hapus).

Langkah 12: Mengaktifkan SSH tanpa kata sandi

Agar aplikasi Anda dapat berjalan di semua instans dalam klaster, Anda harus mengaktifkan akses SSH tanpa kata sandi dari simpul pemimpin ke simpul anggota. Simpul pemimpin adalah instans dari mana Anda menjalankan aplikasi Anda. Instans yang tersisa di klaster adalah simpul anggota.

Untuk mengaktifkan SSH tanpa kata sandi antar instans dalam klaster

1. Pilih satu instans dalam klaster sebagai simpul pemimpin, dan hubungkan ke instans tersebut.
2. Nonaktifkan `strictHostKeyChecking` dan aktifkan `ForwardAgent` pada simpul pemimpin. Buka `~/.ssh/config` menggunakan editor teks pilihan Anda dan tambahkan berikut ini.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Membuat pasangan kunci RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   Pasangan kunci dibuat dalam direktori `$HOME/.ssh/`.

4. Ubah izin kunci privat pada simpul pemimpin.

```
$ chmod 600 ~/.ssh/id_rsa
```

```
chmod 600 ~/.ssh/config
```

5. Buka `~/.ssh/id_rsa.pub` menggunakan editor teks pilihan Anda dan salin kunci.
6. Untuk setiap simpul anggota di klaster, lakukan hal berikut:
   a. Hubungkan dengan instans.
   b. Buka `~/.ssh/authorized_keys` menggunakan editor teks pilihan Anda tambahkan kunci publik yang Anda salin sebelumnya.
7. Untuk menguji apakah SSH tanpa kata sandi berfungsi seperti yang diharapkan, hubungkan ke simpul pemimpin Anda dan jalankan perintah berikut.

   ```
   $ ssh member_node_private_ip
   ```

   Anda harus terhubung ke simpul anggota tanpa diminta untuk memasukkan kunci atau kata sandi.

Memulai dengan EFA dan NCCL untuk beban kerja ML di Amazon EC2

NVIDIA Collective Communications Library (NCCL) adalah perpustakaan rutinitas komunikasi kolektif standar untuk beberapa GPUs di satu node atau beberapa node. NCCL dapat digunakan bersama-sama dengan EFA, Libfabric, dan MPI untuk mendukung berbagai beban kerja machine learning. Untuk informasi lebih lanjut, lihat situs web NCCL.

Persyaratan

- Hanya tipe instans seri P komputasi yang dipercepat yang didukung. Untuk informasi selengkapnya, lihat instans komputasi akselerasi Amazon EC2.
- Hanya Amazon Linux 2023, Amazon Linux 2, Ubuntu 24.04, dan basis AMIs Ubuntu 22.04 yang didukung.
- Hanya NCCL 2.4.2 dan yang lebih baru yang didukung EFA.

Untuk informasi selengkapnya tentang menjalankan beban kerja pembelajaran mesin dengan EFA dan NCCL menggunakan AWS Deep Learning AMIs, lihat Menggunakan EFA pada DLAMI di Panduan Pengembang.AWS Deep Learning AMIs

Langkah-langkah

- Langkah 1: Siapkan grup keamanan yang diaktifkan EFA

- Langkah 2: Luncurkan instans sementara
- Langkah 3: Instal driver Nvidia GPU, kit alat CUDA Nvidia, dan cuDNN
- Langkah 4: Instal GDRCopy
- Langkah 5: Instal perangkat lunak EFA
- Langkah 6: Instal NCCL
- Langkah 7: Instal uji NCCL
- Langkah 8: Uji konfigurasi EFA dan NCCL Anda
- Langkah 9: Instal aplikasi machine learning Anda
- Langkah 10: Membuat AMI dengan EFA dan NCCL yang diaktifkan
- Langkah 11: Mengakhiri instans sementara
- Langkah 12: Luncurkan instans yang diaktifkan EFA dan NCCL ke dalam grup penempatan klaster
- Langkah 13: Mengaktifkan SSH tanpa kata sandi

Langkah 1: Siapkan grup keamanan yang diaktifkan EFA

EFA memerlukan grup keamanan yang memungkinkan semua lalu lintas masuk dan keluar ke dan dari grup keamanan itu sendiri. Prosedur berikut membuat grup keamanan yang memungkinkan semua lalu lintas masuk dan keluar ke dan dari dirinya sendiri, dan yang memungkinkan lalu lintas SSH masuk dari IPv4 alamat apa pun untuk konektivitas SSH.

> **Important**
>
> Grup keamanan ini ditujukan untuk tujuan pengujian saja. Untuk lingkungan produksi Anda, kami sarankan Anda membuat aturan SSH masuk yang memungkinkan lalu lintas hanya dari alamat IP dari mana Anda terhubung, seperti alamat IP komputer Anda, atau berbagai alamat IP di jaringan lokal Anda.

Untuk skenario lainnya, lihat Aturan-aturan grup keamanan untuk kasus penggunaan yang berbeda.

Untuk membuat grup keamanan yang diaktifkan EFA

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dalam panel navigasi, pilih Grup Keamanan, lalu pilih Buat grup keamanan.
3. Di jendela Buat Grup Keamanan, lakukan hal berikut:

a. Untuk Nama grup keamanan, masukkan nama deskriptif untuk grup keamanan, seperti `EFA-enabled security group`.

b. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat grup keamanan.

c. Untuk VPC, pilih VPC untuk tujuan peluncuran instans Anda yang didukung EFA.

d. Pilih Buat grup keamanan.

4. Pilih grup keamanan yang Anda buat, dan pada tab Detail, salin ID grup keamanan.
5. Dengan grup keamanan yang masih dipilih, pilih Tindakan, Edit aturan masuk, lalu lakukan hal berikut:

a. Pilih Tambahkan aturan.

b. Untuk Tipe, pilih Semua lalu lintas.

c. Untuk Tipe sumber, pilih Kustom dan tempelkan ID grup keamanan yang Anda salin ke dalam bidang.

d. Pilih Tambahkan aturan.

e. Untuk Tipe, pilih SSH.

f. Untuk jenis Sumber, pilih Anywhere- IPv4.

g. Pilih Simpan aturan.

6. Dengan grup keamanan yang masih dipilih, pilih Tindakan, Edit aturan keluar, lalu lakukan hal berikut:

a. Pilih Tambahkan aturan.

b. Untuk Tipe, pilih Semua lalu lintas.

c. Untuk Tipe tujuan, pilih Kustom dan tempelkan ID grup keamanan yang Anda salin ke dalam bidang.

d. Pilih Simpan aturan.

Langkah 2: Luncurkan instans sementara

Luncurkan instans sementara yang dapat Anda gunakan untuk menginstal dan mengonfigurasi komponen perangkat lunak EFA. Anda menggunakan instans ini untuk membuat AMI yang diaktifkan EFA sebagai tempat untuk meluncurkan instans Anda yang diaktifkan EFA.

Untuk meluncurkan instans sementara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih Luncurkan Instans untuk membuka wizard peluncuran instans baru.
3. (Opsional) Di bagian Nama dan tanda, berikan nama untuk instans, seperti `EFA-instance`. Nama ditetapkan ke instans sebagai tanda sumber daya (`Name=`*`EFA-instance`*).
4. Di bagian Application and OS Images, pilih AMI untuk salah satu sistem operasi yang didukung.
5. Di bagian Jenis instans, pilih jenis instans yang didukung.
6. Pada bagian Pasangan kunci, pilih pasangan kunci yang akan digunakan untuk instans.
7. Di bagian Pengaturan jaringan, pilih Edit, lalu lakukan hal berikut:

   a. Untuk Subnet, pilih subnet untuk meluncurkan instans. Jika Anda tidak memilih subnet, Anda tidak dapat mengaktifkan instans untuk EFA.

   b. Untuk Firewall (grup keamanan), pilih Pilih grup keamanan yang ada, lalu pilih grup keamanan yang Anda buat di langkah sebelumnya.

   c. Perluas bagian Konfigurasi jaringan lanjutan.

      Untuk antarmuka Jaringan 1, pilih Indeks kartu jaringan = 0, Indeks perangkat = 0, dan Jenis antarmuka = EFA dengan ENA.

      (Opsional) Jika Anda menggunakan jenis instans multi-kartu, seperti **`p4d.24xlarge`** atau**`p5.48xlarge`**, untuk setiap antarmuka jaringan tambahan yang diperlukan, pilih Tambahkan antarmuka jaringan, untuk indeks kartu jaringan pilih indeks berikutnya yang tidak digunakan, lalu pilih Indeks perangkat = 1 dan Jenis antarmuka = EFA dengan ENA atau EFA saja.

8. Di bagian Penyimpanan, konfigurasikan volume sesuai kebutuhan.

   > **Note**
   >
   > Anda harus menyediakan penyimpanan tambahan 10 hingga 20 GiB untuk Nvidia CUDA. Jika Anda tidak menyediakan penyimpanan yang cukup, Anda akan menerima kesalahan `insufficient disk space` saat mencoba menginstal driver Nvidia dan toolkit CUDA.

9. Di panel Ringkasan di sebelah kanan, pilih Luncurkan instans.

Langkah 3: Instal driver Nvidia GPU, kit alat CUDA Nvidia, dan cuDNN

Amazon Linux 2023 and Amazon Linux 2

Untuk menginstal driver Nvidia GPU, kit alat CUDA Nvidia, dan cuDNN

1. Untuk memastikan bahwa semua paket perangkat lunak Anda telah diperbarui, lakukan pembaruan perangkat lunak cepat di instans Anda.

   ```
   $ sudo yum upgrade -y && sudo reboot
   ```

   Hubungkan kembali ke instans Anda setelah boot ulang.

2. Pasang utilitas yang diperlukan untuk memasang driver GPU Nvidia dan toolkit Nvidia CUDA.

   ```
   $ sudo yum groupinstall 'Development Tools' -y
   ```

3. Nonaktifkan driver `nouveau` open source.

   a. Instal utilitas yang diperlukan dan paket header kernel untuk versi kernel yang sedang Anda jalankan.

   ```
   $ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -
   r)
   ```

   b. Tambahkan `nouveau` ke file daftar penolakan `/etc/modprobe.d/blacklist.conf` .

   ```
   $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   c. Tambahkan `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` ke file `grub` dan bangun kembali konfigurasi Grub.

   ```
   $ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
   default/grub \
   ```

```
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Boot ulang dan terhubung kembali ke instans Anda.
5. Siapkan repositori yang dibutuhkan

   a. Aktifkan repositori EPEL dan atur distribusi ke. `rhel7`

   ```
   $ sudo amazon-linux-extras install epel \
   && distribution='rhel7'
   ```

   b. Siapkan repositori jaringan CUDA dan perbarui cache repositori.

   ```
   $ ARCH=$( /bin/arch ) \
   && sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
   compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
   && sudo yum clean expire-cache
   ```

   c. (Kernel versi 5.10 saja) Lakukan langkah-langkah ini hanya jika Anda menggunakan Amazon Linux 2 dengan kernel versi 5.10. Jika Anda menggunakan Amazon Linux 2 dengan kernel versi 4.12, lewati langkah-langkah ini. Untuk memeriksa versi kernel Anda, jalankan uname -r.

      i. Buat file konfigurasi driver Nvidia bernama `/etc/dkms/nvidia.conf`.

      ```
      $ sudo mkdir -p /etc/dkms \
      && echo "MAKE[0]=\"'make' -j2 module SYSSRC=\${kernel_source_dir}
       IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1
       CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
      ```

      ii. (`p4d.24xlarge` dan `p5.48xlarge` saja) Salin file konfigurasi driver Nvidia.

      ```
      $ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
      ```

6. Instal driver Nvidia GPU, kit alat CUDA Nvidia, dan cuDNN.

   ```
   $ sudo yum clean all \
   && sudo yum -y install nvidia-driver-latest-dkms \
   && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
   ```

7. Boot ulang dan terhubung kembali ke instans Anda.

8. (`p4d.24xlarge` dan `p5.48xlarge` saja) Mulai layanan Nvidia Fabric Manager, dan pastikan bahwa layanan tersebut dimulai secara otomatis saat instans dimulai. Nvidia Fabric Manager diperlukan untuk NV Switch Management.

```
$ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
fabricmanager
```

9. Pastikan bahwa jalur CUDA diatur setiap kali instans dimulai.

   - Untuk shell bash, tambahkan pernyataan berikut ke `/home/username/.bashrc` dan `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

   - Untuk shell tcsh, tambahkan pernyataan berikut ke `/home/username/.cshrc`.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

10. Untuk mengonfirmasi bahwa driver Nvidia GPU berfungsi, jalankan perintah berikut.

```
$ nvidia-smi -q | head
```

    Perintah tersebut harus mengembalikan informasi tentang Nvidia GPUs, driver GPU Nvidia, dan toolkit Nvidia CUDA.

Ubuntu 24.04 and Ubuntu 22.04

Untuk menginstal driver Nvidia GPU, kit alat CUDA Nvidia, dan cuDNN

1. Untuk memastikan bahwa semua paket perangkat lunak Anda telah diperbarui, lakukan pembaruan perangkat lunak cepat di instans Anda.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Pasang utilitas yang diperlukan untuk memasang driver GPU Nvidia dan toolkit Nvidia CUDA.

```
$ sudo apt-get update && sudo apt-get install build-essential -y
```

3. Untuk menggunakan driver GPU Nvidia, Anda harus menonaktifkan driver sumber terbuka `nouveau` terlebih dahulu.

   a. Instal utilitas yang diperlukan dan paket header kernel untuk versi kernel yang sedang Anda jalankan.

   ```
   $ sudo apt-get install -y gcc make linux-headers-$(uname -r)
   ```

   b. Tambahkan `nouveau` ke file daftar penolakan `/etc/modprobe.d/blacklist.conf` .

   ```
   $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   c. Buka `/etc/default/grub` menggunakan editor teks pilihan Anda dan tambahkan berikut ini.

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   d. Buat kembali konfigurasi Grub.

   ```
   $ sudo update-grub
   ```

4. Boot ulang dan terhubung kembali ke instans Anda.
5. Tambahkan repositori CUDA dan instal driver Nvidia GPU, toolkit CUDA NVIDIA, dan cuDNN.

   - `p3dn.24xlarge`

   ```
   $ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
   machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
   && wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
   machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
   ubuntu2004_1.0.0-1_amd64.deb \
   ```

```
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

- `p4d.24xlarge` dan `p5.48xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-kernel-open-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Boot ulang dan terhubung kembali ke instans Anda.
7. (`p4d.24xlarge` dan `p5.48xlarge` saja) Instal Nvidia Fabric Manager.

   a. Anda harus menginstal versi Nvidia Fabric Manager yang cocok dengan versi modul kernel Nvidia yang Anda instal pada langkah sebelumnya.

      Jalankan perintah berikut untuk menentukan versi modul kernel Nvidia.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

Berikut ini adalah output contoh.

```
NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15
 21:26:37 UTC 2021
```

Pada contoh di atas, versi utama `450` dari modul kernel diinstal. Ini berarti Anda perlu menginstal versi Nvidia Fabric Manager `450`.

b. Instal Nvidia Fabric Manager. Jalankan perintah berikut dan tentukan versi utama yang diidentifikasi pada langkah sebelumnya.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-major_version_number
```

Misalnya, jika versi `450` utama modul kernel diinstal, gunakan perintah berikut untuk menginstal versi Nvidia Fabric Manager yang cocok.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-450
```

c. Mulai layanan, dan pastikan bahwa layanan tersebut dimulai secara otomatis ketika instans dimulai. Nvidia Fabric Manager diperlukan untuk NV Switch Management.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Pastikan bahwa jalur CUDA diatur setiap kali instans dimulai.

- Untuk shell bash, tambahkan pernyataan berikut ke `/home/username/.bashrc` dan `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Untuk shell tcsh, tambahkan pernyataan berikut ke `/home/username/.cshrc`.

```
setenv PATH=/usr/local/cuda/bin:$PATH
```

```
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Untuk mengonfirmasi bahwa driver Nvidia GPU berfungsi, jalankan perintah berikut.

```
$ nvidia-smi -q | head
```

Perintah tersebut harus mengembalikan informasi tentang Nvidia GPUs, driver GPU Nvidia, dan toolkit Nvidia CUDA.

Langkah 4: Instal GDRCopy

Instal GDRCopy untuk meningkatkan kinerja Libfabric. Untuk informasi selengkapnyaGDRCopy, lihat GDRCopy repositori.

Amazon Linux 2023 and Amazon Linux 2

Untuk menginstal GDRCopy

1. Instal dependensi yang diperlukan.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Unduh dan ekstrak GDRCopy paketnya.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Bangun paket GDRCopy RPM.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Instal paket GDRCopy RPM.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.4-1dkms.noarch*.rpm \
&& sudo rpm -Uvh gdrcopy-2.4-1.x86_64*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.4-1.noarch*.rpm
```

Ubuntu 24.04 and Ubuntu 22.04

Untuk menginstal GDRCopy

1. Instal dependensi yang diperlukan.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Unduh dan ekstrak GDRCopy paketnya.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Bangun paket GDRCopy RPM.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Instal paket GDRCopy RPM.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

Langkah 5: Instal perangkat lunak EFA

Instal kernel berkemampuan EFA, driver EFA, Libfabric, aws-ofi-nccl plugin, dan tumpukan MPI Terbuka yang diperlukan untuk mendukung EFA pada instans Anda.

Untuk menginstal perangkat lunak EFA

1. Hubungkan ke instans yang Anda luncurkan. Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..
2. Unduh file penginstalan perangkat lunak EFA. File penginstalan perangkat lunak dikemas menjadi file tarball (`.tar.gz`) yang dikompresi. Untuk mengunduh versi stabil terbaru, gunakan perintah berikut.

Anda juga bisa mendapatkan versi terbaru dengan mengganti nomor versi dengan `latest` dalam perintah sebelumnya.

```
$ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz
```

3. (Opsional) Verifikasi keaslian dan integritas file tarball EFA (`.tar.gz`).

   Kami menyarankan Anda melakukan hal ini untuk memverifikasi identitas penerbit perangkat lunak dan memeriksa apakah file tersebut tidak diubah atau rusak sejak file tersebut diterbitkan. Jika Anda tidak ingin memverifikasi file tarball, lewati langkah ini.

   > **Note**
   >
   > Atau, jika Anda lebih suka memverifikasi file tarball dengan menggunakan MD5 atau SHA256 checksum sebagai gantinya, lihat. Memverifikasi penginstal EFA menggunakan checksum

   a. Unduh kunci GPG publik dan impor ke dalam keyring Anda.

   ```
   $ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
   import aws-efa-installer.key
   ```

   Perintah tersebut harus mengembalikan nilai kunci. Catat nilai kunci, karena Anda membutuhkannya di langkah selanjutnya.

   b. Verifikasi sidik jari kunci GPG. Jalankan perintah berikut dan tentukan nilai kunci dari langkah sebelumnya.

   ```
   $ gpg --fingerprint key_value
   ```

   Perintah tersebut harus mengembalikan sidik jari yang identik dengan `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Jika sidik jari tidak cocok, jangan jalankan skrip instalasi EFA, dan hubungi Dukungan.

   c. Unduh file tanda tangan dan verifikasi tanda tangan pada file tarball EFA.

   ```
   $ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz.sig
    && gpg --verify ./aws-efa-installer-1.47.0.tar.gz.sig
   ```

Berikut ini adalah contoh output.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Jika hasilnya mencakup `Good signature`, dan sidik jari cocok dengan sidik jari yang dikembalikan di langkah sebelumnya, lanjutkan ke langkah berikutnya. Jika tidak, jangan jalankan skrip instalasi EFA, dan hubungi Dukungan.

4. Ekstraksi file dari file `.tar.gz` yang dikompresi dan navigasi ke dalam direktori yang diekstraksi.

```
$ tar -xf aws-efa-installer-1.47.0.tar.gz && cd aws-efa-installer
```

5. Unduh skrip penginstalan perangkat lunak EFA.

> **Note**
>
> Dari EFA 1.30.0, Open MPI 4.1 dan Open MPI 5 diinstal secara default. Kecuali Anda membutuhkan Open MPI 5, kami sarankan Anda hanya menginstal Open MPI 4.1. Perintah berikut menginstal Open MPI 4.1 saja. Jika Anda ingin menginstal Open MPI 4.1 and Open MPI 5, hapus. `--mpi=openmpi4`

```
$ sudo ./efa_installer.sh -y --mpi=openmpi4
```

Libfabric diinstal di `/opt/amazon/efa` direktori. aws-ofi-nccl Plugin diinstal di `/opt/amazon/ofi-nccl` direktori. Buka MPI diinstal di `/opt/amazon/openmpi` direktori.

6. Jika penginstal EFA meminta Anda untuk me-reboot instans, lakukanlah dan kemudian sambungkan kembali ke instans. Jika tidak, log out dari instans lalu log kembali untuk menyelesaikan penginstalan.
7. Pastikan bahwa komponen perangkat lunak EFA telah berhasil diinstal.

```
$ fi_info -p efa -t FI_EP_RDM
```

Perintah tersebut harus mengembalikan informasi tentang antarmuka Libfabric EFA. Contoh berikut menunjukkan output perintah.

- `p3dn.24xlarge` dengan satu antarmuka jaringan

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` dan `p5.48xlarge` dengan berbagai antarmuka jaringan

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Langkah 6: Instal NCCL

Instal NCCL. Untuk informasi lebih lanjut tentang NCCL, lihat repositori NCCL.

Untuk menginstal NCCL

1. Buka direktori `/opt` tersebut.

```
$ cd /opt
```

2. Gandakan repositori NCCL resmi ke instans dan navigasi ke repositori klon lokal.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git -b v2.23.4-1 && cd nccl
```

3. Bangun dan instal NCCL dan tentukan direktori instalasi CUDA.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Langkah 7: Instal uji NCCL

Instal uji NCCL. Uji NCCL memungkinkan Anda untuk mengonfirmasi bahwa NCCL diinstal dengan benar dan beroperasi sesuai harapan. Untuk informasi lebih lanjut tentang pengujian NCCL, lihat repositori nccl-tests.

Untuk menginstal pengujian EFA

1. Navigasi ke direktori beranda Anda.

```
$ cd $HOME
```

2. Gandakan repositori nccl-tests resmi ke instans dan navigasi ke repositori klon lokal.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Tambahkan direktori Libfabric ke variabel `LD_LIBRARY_PATH`.

   - Amazon Linux 2023 dan Amazon Linux 2

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

   - Ubuntu 24.04 dan Ubuntu 22.04

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
```

4. Instal pengujian NCCL dan tentukan direktori penginstalan MPI, NCCL, dan CUDA.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
local/cuda
```

Langkah 8: Uji konfigurasi EFA dan NCCL Anda

Jalankan pengujian untuk memastikan bahwa instans sementara Anda sudah dikonfigurasi dengan benar untuk EFA dan NCCL.

Untuk menguji konfigurasi EFA dan NCCL Anda

1. Buat file host yang menentukan host untuk menjalankan pengujian. Perintah berikut membuat file host dengan nama `my-hosts` yang mencakup referensi ke instans itu sendiri.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Jalankan pengujian dan tentukan file host (`--hostfile`) dan jumlah GPUs yang akan digunakan (`-n`). Perintah berikut menjalankan `all_reduce_perf` pengujian pada 8 GPUs pada instance itu sendiri, dan menentukan variabel lingkungan berikut.

   - `FI_EFA_USE_DEVICE_RDMA=1`—(hanya `p4d.24xlarge`) menggunakan fungsi RDMA perangkat untuk transfer satu sisi dan dua sisi.
   - `NCCL_DEBUG=INFO`—memungkinkan output debug terperinci. Anda juga dapat menentukan `VERSION` untuk mencetak versi NCCL saja di awal pengujian, atau `WARN` untuk menerima pesan kesalahan saja.

Untuk informasi lebih lanjut mengenai argumen uji NCCL, lihat Tes NCCL README dalam repositori nccl-tests resmi.

- `p3dn.24xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/amazon/ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- `p4d.24xlarge` dan `p5.48xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_EFA_USE_DEVICE_RDMA=1 \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/amazon/ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Anda dapat mengonfirmasi bahwa EFA aktif sebagai penyedia pokok NCCL ketika log `NCCL_DEBUG` dicetak.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Informasi tambahan berikut ditampilkan saat menggunakan instans `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Langkah 9: Instal aplikasi machine learning Anda

Instal aplikasi machine learning di instans sementara. Prosedur penginstalan bervariasi tergantung pada aplikasi machine learning tertentu. Untuk informasi selengkapnya tentang menginstal perangkat lunak pada instans Linux Anda, lihat Mengelola perangkat lunak di instans Amazon Linux 2 Anda.

> **Note**
>
> Lihat dokumentasi aplikasi machine learning Anda untuk petunjuk penginstalan.

Langkah 10: Membuat AMI dengan EFA dan NCCL yang diaktifkan

Setelah menginstal komponen perangkat lunak yang diperlukan, Anda membuat AMI yang dapat digunakan kembali untuk meluncurkan instans Anda dengan EFA yang diaktifkan.

Untuk membuat AMI dari instans sementara Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans sementara yang Anda buat dan pilih Tindakan, Gambar, Buat gambar.
4. Untuk Buat gambar, lakukan hal berikut:
   a. Untuk Nama gambar, masukkan nama deskriptif untuk AMI.
   b. (Opsional) Untuk Deskripsi gambar, masukkan deskripsi singkat tentang tujuan AMI.
   c. Pilih Buat gambar.
5. Di panel navigasi, pilih AMIs.
6. Temukan AMI yang Anda buat dalam daftar. Tunggu hingga status berubah dari `pending` menjadi `available` sebelum melanjutkan ke langkah berikutnya.

Langkah 11: Mengakhiri instans sementara

Pada titik ini, Anda tidak memerlukan lagi instans sementara yang Anda luncurkan. Anda dapat mengakhiri instans agar biaya tidak dibebankan lagi padanya.

Untuk mengakhiri instans sementara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Di panel navigasi, pilih Instans.
3. Pilih instans sementara yang Anda buat dan pilih Tindakan, Status instans, Akhiri instans.
4. Ketika diminta konfirmasi, pilih Akhiri.

Langkah 12: Luncurkan instans yang diaktifkan EFA dan NCCL ke dalam grup penempatan klaster

Luncurkan instans yang diaktifkan EFA dan NCCL Anda ke dalam grup penempatan klaster menggunakan AMI yang diaktifkan EFA dan grup keamanan yang diaktifkan EFA yang Anda buat sebelumnya.

> **Note**
>
> - Meluncurkan instans yang diaktifkan EFA ke dalam grup penempatan kluster bukanlah persyaratan mutlak. Namun, kami menyarankan Anda untuk menjalankan instans yang diaktifkan EFA dalam grup penempatan klaster saat instans diluncurkan ke grup dengan latensi rendah di Zona Ketersediaan tunggal.
> - Untuk memastikan kapasitas tersedia saat Anda menskalakan instans klaster, Anda dapat membuat Reservasi Kapasitas untuk grup penempatan klaster Anda. Untuk informasi selengkapnya, lihat Gunakan Reservasi Kapasitas dengan grup penempatan klaster.

New console

Untuk meluncurkan instans sementara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih Luncurkan Instans untuk membuka wizard peluncuran instans baru.
3. (Opsional) Di bagian Nama dan tanda, berikan nama untuk instans, seperti `EFA-instance`. Nama ditetapkan ke instans sebagai tanda sumber daya (`Name=EFA-instance`).
4. Di bagian Application and OS ImagesAMIs, pilih My, lalu pilih AMI yang Anda buat pada langkah sebelumnya.
5. Di bagian Tipe instans, pilih `p3dn.24xlarge` atau `p4d.24xlarge`.
6. Pada bagian Pasangan kunci, pilih pasangan kunci yang akan digunakan untuk instans.

7. Di bagian Pengaturan jaringan, pilih Edit, lalu lakukan hal berikut:

   a. Untuk Subnet, pilih subnet untuk meluncurkan instans. Jika Anda tidak memilih subnet, Anda tidak dapat mengaktifkan instans untuk EFA.

   b. Untuk Firewall (grup keamanan), pilih Pilih grup keamanan yang ada, lalu pilih grup keamanan yang Anda buat di langkah sebelumnya.

   c. Perluas bagian Konfigurasi jaringan lanjutan.

      Untuk antarmuka Jaringan 1, pilih Indeks kartu jaringan = 0, Indeks perangkat = 0, dan Jenis antarmuka = EFA dengan ENA.

      (Opsional) Jika Anda menggunakan jenis instans multi-kartu, seperti **`p4d.24xlarge`** atau**`p5.48xlarge`**, untuk setiap antarmuka jaringan tambahan yang diperlukan, pilih Tambahkan antarmuka jaringan, untuk indeks kartu jaringan pilih indeks yang tidak digunakan berikutnya, lalu pilih Indeks perangkat = 1 dan Jenis antarmuka = EFA eith ENA atau EFA saja.

8. (Opsional) Di bagian Penyimpanan, konfigurasikan volume sesuai kebutuhan.
9. Di bagian Detail lanjutan, untuk nama grup Penempatan, pilih grup penempatan klaster untuk meluncurkan instans. Jika Anda perlu membuat grup penempatan klaster baru, pilih Buat grup penempatan baru.
10. Di panel Ringkasan di sebelah kanan, untuk Jumlah instans, masukkan jumlah instans yang diaktifkan EFA yang ingin Anda luncurkan, lalu pilih Luncurkan instans.

Old console

Untuk meluncurkan instans yang diaktifkan EFA dan NCCL ke dalam grup penempatan klaster

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Luncurkan Instans.
3. Pada halaman Pilih AMI, pilih Milik Saya AMIs, temukan AMI yang Anda buat sebelumnya, lalu pilih Pilih.
4. Di halaman Pilih Tipe Instans, pilih p3dn.24xlarge lalu pilih Berikutnya: Konfigurasikan Detail Instans.
5. Pada halaman Konfigurasi Detail Instans, lakukan langkah berikut:

a. Untuk Jumlah instans, masukkan jumlah instans yang diaktifkan EFA dan NCCL yang ingin Anda luncurkan.

b. Untuk Jaringan dan Subnet, pilih VPC dan subnet sebagai tujuan peluncuran instans.

c. Untuk Grup penempatan, pilih Tambahkan instans ke grup penempatan.

d. Untuk Nama grup penempatan, pilih Tambahkan ke grup penempatan baru, lalu masukkan nama deskriptif untuk grup penempatan. Lalu untuk Strategi grup penempatan, pilih klaster.

e. Untuk EFA, pilih Aktifkan.

f. Di bagian Antarmuka Jaringan, untuk perangkat eth0, pilih Antarmuka jaringan baru. Anda dapat secara opsional menentukan IPv4 alamat utama dan satu atau lebih IPv4 alamat sekunder. Jika Anda meluncurkan instance ke subnet yang memiliki blok IPv6 CIDR terkait, Anda dapat secara opsional menentukan IPv6 alamat utama dan satu atau beberapa alamat sekunder. IPv6

g. Pilih Berikutnya: Tambahkan Penyimpanan.

6. Di halaman Tambahkan Penyimpanan, tentukan volume yang akan dipasang ke instans selain volume yang ditentukan oleh AMI (seperti volume perangkat root). Lalu, pilih Berikutnya: Tambahkan Tanda.
7. Di halaman Tambahkan Tanda, tentukan tanda untuk instans, seperti nama yang mudah digunakan, lalu pilih Selanjutnya: Konfigurasikan Grup Keamanan.
8. Di halaman Mengonfigurasi Grup Keamanan, untuk Tetapkan grup keamanan, pilih Pilih grup keamanan yang sudah ada, lalu pilih grup keamanan yang Anda buat sebelumnya.
9. Pilih Tinjau dan Luncurkan.
10. Di halaman Meninjau Peluncuran Instans, tinjau pengaturannya, lalu pilih Luncurkan untuk memilih key pair dan meluncurkan instans Anda.

Langkah 13: Mengaktifkan SSH tanpa kata sandi

Agar aplikasi Anda dapat berjalan di semua instans dalam klaster, Anda harus mengaktifkan akses SSH tanpa kata sandi dari simpul pemimpin ke simpul anggota. Simpul pemimpin adalah instans dari mana Anda menjalankan aplikasi Anda. Instans yang tersisa di klaster adalah simpul anggota.

Untuk mengaktifkan SSH tanpa kata sandi antar instans dalam klaster

1. Pilih satu instans dalam klaster sebagai simpul pemimpin, dan hubungkan ke instans tersebut.

2. Nonaktifkan `strictHostKeyChecking` dan aktifkan `ForwardAgent` pada simpul pemimpin. Buka `~/.ssh/config` menggunakan editor teks pilihan Anda dan tambahkan berikut ini.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Membuat pasangan kunci RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   Pasangan kunci dibuat dalam direktori `$HOME/.ssh/`.

4. Ubah izin kunci privat pada simpul pemimpin.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Buka `~/.ssh/id_rsa.pub` menggunakan editor teks pilihan Anda dan salin kunci.
6. Untuk setiap simpul anggota di klaster, lakukan hal berikut:

   a. Hubungkan dengan instans.

   b. Buka `~/.ssh/authorized_keys` menggunakan editor teks pilihan Anda tambahkan kunci publik yang Anda salin sebelumnya.

7. Untuk menguji apakah SSH tanpa kata sandi berfungsi seperti yang diharapkan, hubungkan ke simpul pemimpin Anda dan jalankan perintah berikut.

```
$ ssh member_node_private_ip
```

   Anda harus terhubung ke simpul anggota tanpa diminta untuk memasukkan kunci atau kata sandi.

Memulai EFA dan NIXL untuk beban kerja inferensi di Amazon EC2

NVIDIA Inference Xfer Library (NIXL) adalah pustaka komunikasi latensi rendah throughput tinggi yang dirancang khusus untuk beban kerja inferensi terpilah. NIXL dapat digunakan bersama dengan EFA dan Libfabric untuk mendukung transfer KV-cache antara prefill dan decode node, dan

memungkinkan pergerakan KV-cache yang efisien antara berbagai lapisan penyimpanan. Untuk informasi lebih lanjut, lihat situs web NIXL.

Persyaratan

- Hanya basis Ubuntu 24.04 dan Ubuntu 22.04 AMIs yang didukung.
- EFA hanya mendukung NIXL 1.0.0 dan yang lebih baru.

Langkah 1: Siapkan grup keamanan yang diaktifkan EFA

EFA memerlukan grup keamanan yang memungkinkan semua lalu lintas masuk dan keluar ke dan dari grup keamanan itu sendiri. Prosedur berikut membuat grup keamanan yang memungkinkan semua lalu lintas masuk dan keluar ke dan dari dirinya sendiri, dan yang memungkinkan lalu lintas SSH masuk dari IPv4 alamat apa pun untuk konektivitas SSH.

> **Important**
>
> Grup keamanan ini ditujukan untuk tujuan pengujian saja. Untuk lingkungan produksi Anda, kami sarankan Anda membuat aturan SSH masuk yang memungkinkan lalu lintas hanya dari alamat IP dari mana Anda terhubung, seperti alamat IP komputer Anda, atau berbagai alamat IP di jaringan lokal Anda.

Untuk skenario lainnya, lihat Aturan-aturan grup keamanan untuk kasus penggunaan yang berbeda.

Untuk membuat grup keamanan yang diaktifkan EFA

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dalam panel navigasi, pilih Grup Keamanan, lalu pilih Buat grup keamanan.
3. Di jendela Buat Grup Keamanan, lakukan hal berikut:
   a. Untuk Nama grup keamanan, masukkan nama deskriptif untuk grup keamanan, seperti `EFA-enabled security group`.
   b. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat grup keamanan.
   c. Untuk VPC, pilih VPC untuk tujuan peluncuran instans Anda yang didukung EFA.
   d. Pilih Buat grup keamanan.
4. Pilih grup keamanan yang Anda buat, dan pada tab Detail, salin ID grup keamanan.

5. Dengan grup keamanan yang masih dipilih, pilih Tindakan, Edit aturan masuk, lalu lakukan hal berikut:

   a. Pilih Tambahkan aturan.

   b. Untuk Tipe, pilih Semua lalu lintas.

   c. Untuk Tipe sumber, pilih Kustom dan tempelkan ID grup keamanan yang Anda salin ke dalam bidang.

   d. Pilih Tambahkan aturan.

   e. Untuk Tipe, pilih SSH.

   f. Untuk jenis Sumber, pilih Anywhere- IPv4.

   g. Pilih Simpan aturan.

6. Dengan grup keamanan yang masih dipilih, pilih Tindakan, Edit aturan keluar, lalu lakukan hal berikut:

   a. Pilih Tambahkan aturan.

   b. Untuk Tipe, pilih Semua lalu lintas.

   c. Untuk Tipe tujuan, pilih Kustom dan tempelkan ID grup keamanan yang Anda salin ke dalam bidang.

   d. Pilih Simpan aturan.

Langkah 2: Luncurkan instans sementara

Luncurkan instans sementara yang dapat Anda gunakan untuk menginstal dan mengonfigurasi komponen perangkat lunak EFA. Anda menggunakan instans ini untuk membuat AMI yang diaktifkan EFA sebagai tempat untuk meluncurkan instans Anda yang diaktifkan EFA.

Untuk meluncurkan instans sementara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih Luncurkan Instans untuk membuka wizard peluncuran instans baru.
3. (Opsional) Di bagian Nama dan tanda, berikan nama untuk instans, seperti `EFA-instance`. Nama ditetapkan ke instans sebagai tanda sumber daya (`Name=`*`EFA-instance`*).

4. Di bagian Aplikasi dan Gambar OS, pilih AMI untuk salah satu sistem operasi yang didukung. Anda juga dapat memilih DLAMI yang didukung yang ditemukan di Halaman Catatan Rilis DLAMI.
5. Di bagian Jenis instans, pilih jenis instans yang didukung.
6. Pada bagian Pasangan kunci, pilih pasangan kunci yang akan digunakan untuk instans.
7. Di bagian Pengaturan jaringan, pilih Edit, lalu lakukan hal berikut:

   a. Untuk Subnet, pilih subnet untuk meluncurkan instans. Jika Anda tidak memilih subnet, Anda tidak dapat mengaktifkan instans untuk EFA.

   b. Untuk Firewall (grup keamanan), pilih Pilih grup keamanan yang ada, lalu pilih grup keamanan yang Anda buat di langkah sebelumnya.

   c. Perluas bagian Konfigurasi jaringan lanjutan.

      Untuk antarmuka Jaringan 1, pilih Indeks kartu jaringan = 0, Indeks perangkat = 0, dan Jenis antarmuka = EFA dengan ENA.

      (Opsional) Jika Anda menggunakan jenis instans multi-kartu, seperti **`p4d.24xlarge`** atau**`p5.48xlarge`**, untuk setiap antarmuka jaringan tambahan yang diperlukan, pilih Tambahkan antarmuka jaringan, untuk indeks kartu jaringan pilih indeks berikutnya yang tidak digunakan, lalu pilih Indeks perangkat = 1 dan Jenis antarmuka = EFA dengan ENA atau EFA saja.
8. Di bagian Penyimpanan, konfigurasikan volume sesuai kebutuhan.

   > **Note**
   >
   > Anda harus menyediakan penyimpanan tambahan 10 hingga 20 GiB untuk Nvidia CUDA. Jika Anda tidak menyediakan penyimpanan yang cukup, Anda akan menerima kesalahan `insufficient disk space` saat mencoba menginstal driver Nvidia dan toolkit CUDA.
9. Di panel Ringkasan di sebelah kanan, pilih Luncurkan instans.

> **Important**
>
> Lewati Langkah 3 jika AMI Anda sudah menyertakan driver GPU Nvidia, toolkit CUDA, dan cuDNN, atau jika Anda menggunakan instance non-GPU.

Langkah 3: Instal driver Nvidia GPU, kit alat CUDA Nvidia, dan cuDNN

Untuk menginstal driver Nvidia GPU, kit alat CUDA Nvidia, dan cuDNN

1. Untuk memastikan bahwa semua paket perangkat lunak Anda telah diperbarui, lakukan pembaruan perangkat lunak cepat di instans Anda.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Pasang utilitas yang diperlukan untuk memasang driver GPU Nvidia dan toolkit Nvidia CUDA.

```
$ sudo apt-get install build-essential -y
```

3. Untuk menggunakan driver GPU Nvidia, Anda harus menonaktifkan driver sumber terbuka `nouveau` terlebih dahulu.

   a. Instal utilitas yang diperlukan dan paket header kernel untuk versi kernel yang sedang Anda jalankan.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

   b. Tambahkan `nouveau` ke file daftar penolakan `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   c. Buka `/etc/default/grub` menggunakan editor teks pilihan Anda dan tambahkan berikut ini.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   d. Buat kembali konfigurasi Grub.

```
$ sudo update-grub
```

4. Boot ulang dan terhubung kembali ke instans Anda.

5. Tambahkan repositori CUDA dan instal driver Nvidia GPU, toolkit CUDA NVIDIA, dan cuDNN.

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/
compute/machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/repos/
ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535 cuda-
toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Boot ulang dan terhubung kembali ke instans Anda.

7. (`p4d.24xlarge` dan `p5.48xlarge` saja) Instal Nvidia Fabric Manager.

   a. Anda harus menginstal versi Nvidia Fabric Manager yang cocok dengan versi modul kernel Nvidia yang Anda instal pada langkah sebelumnya.

      Jalankan perintah berikut untuk menentukan versi modul kernel Nvidia.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      Berikut ini adalah output contoh.

      ```
      NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15 21:26:37
       UTC 2021
      ```

      Pada contoh di atas, versi utama `450` dari modul kernel diinstal. Ini berarti Anda perlu menginstal versi Nvidia Fabric Manager `450`.

   b. Instal Nvidia Fabric Manager. Jalankan perintah berikut dan tentukan versi utama yang diidentifikasi pada langkah sebelumnya.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-major_version_number
```

Misalnya, jika versi `450` utama modul kernel diinstal, gunakan perintah berikut untuk menginstal versi Nvidia Fabric Manager yang cocok.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-450
```

c. Mulai layanan, dan pastikan bahwa layanan tersebut dimulai secara otomatis ketika instans dimulai. Nvidia Fabric Manager diperlukan untuk NV Switch Management.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Pastikan bahwa jalur CUDA diatur setiap kali instans dimulai.

- Untuk shell bash, tambahkan pernyataan berikut ke /home/*username*/.bashrc dan /home/*username*/.bash_profile.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:
$LD_LIBRARY_PATH
```

- Untuk shell tcsh, tambahkan pernyataan berikut ke /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:
$LD_LIBRARY_PATH
```

9. Untuk mengonfirmasi bahwa driver Nvidia GPU berfungsi, jalankan perintah berikut.

```
$ nvidia-smi -q | head
```

Perintah tersebut harus mengembalikan informasi tentang Nvidia GPUs, driver GPU Nvidia, dan toolkit Nvidia CUDA.

> **Important**
>
> Lewati Langkah 4 jika AMI Anda sudah termasuk GDRCopy, atau jika Anda menggunakan instance non-GPU.

Langkah 4: Instal GDRCopy

Instal GDRCopy untuk meningkatkan kinerja Libfabric pada platform berbasis GPU. Untuk informasi selengkapnyaGDRCopy, lihat GDRCopy repositori.

Untuk menginstal GDRCopy

1. Instal dependensi yang diperlukan.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Unduh dan ekstrak GDRCopy paketnya.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Bangun paket GDRCopy DEB.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Instal paket GDRCopy DEB.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

> **Important**
>
> Lewati Langkah 5 jika AMI Anda sudah menyertakan penginstal EFA terbaru.

Langkah 5: Instal perangkat lunak EFA

Instal kernel berkemampuan EFA, driver EFA, dan tumpukan Libfabric yang diperlukan untuk mendukung EFA pada instans Anda.

Untuk menginstal perangkat lunak EFA

1. Hubungkan ke instans yang Anda luncurkan. Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..
2. Unduh file penginstalan perangkat lunak EFA. File penginstalan perangkat lunak dikemas menjadi file tarball (`.tar.gz`) yang dikompresi. Untuk mengunduh versi stabil terbaru, gunakan perintah berikut.

   ```
   $ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz
   ```
3. Ekstrak file dari file terkompresi`.tar.gz`, hapus tarball, dan navigasikan ke direktori yang diekstraksi.

   ```
   $ tar -xf aws-efa-installer-1.47.0.tar.gz && rm -rf aws-efa-installer-1.47.0.tar.gz
    && cd aws-efa-installer
   ```
4. Unduh skrip penginstalan perangkat lunak EFA.

   ```
   $ sudo ./efa_installer.sh -y
   ```

   Libfabric diinstal di `/opt/amazon/efa` direktori.
5. Jika penginstal EFA meminta Anda untuk me-reboot instans, lakukanlah dan kemudian sambungkan kembali ke instans. Jika tidak, log out dari instans lalu log kembali untuk menyelesaikan penginstalan.
6. Pastikan bahwa komponen perangkat lunak EFA telah berhasil diinstal.

   ```
   $ fi_info -p efa -t FI_EP_RDM
   ```

   Perintah tersebut harus mengembalikan informasi tentang antarmuka Libfabric EFA. Contoh berikut menunjukkan output perintah.

   - `p3dn.24xlarge` dengan satu antarmuka jaringan

     ```
     provider: efa
     ```

```
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` dan `p5.48xlarge` dengan berbagai antarmuka jaringan

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Langkah 6: Instal NIXL

Instal NIXL. Untuk informasi selengkapnya tentang NIXL, lihat repositori NIXL.

Pre-built distributions

Untuk menginstal NIXL menggunakan PyPI

1. Instal dependensi yang diperlukan.

```
$ sudo apt install pip
```

2. Instal NIXL.

```
$ pip install nixl
```

Build from source

Untuk membangun dan menginstal NIXL dari sumber

1. Instal dependensi yang diperlukan.

```
$ sudo apt install cmake pkg-config meson pybind11-dev libaio-dev nvidia-cuda-
toolkit pip libhwloc-dev \
&& pip install meson ninja pybind11
```

2. Navigasi ke direktori beranda Anda.

```
$ cd $HOME
```

3. Kloning repositori NIXL resmi ke instance dan navigasikan ke repositori kloning lokal.

```
$ sudo git clone https://github.com/ai-dynamo/nixl.git && cd nixl
```

4. Bangun dan instal NIXL dan tentukan jalur ke direktori instalasi Libfabric.

```
$ sudo meson setup . nixl --prefix=/usr/local/nixl -Dlibfabric_path=/opt/amazon/
efa
$ cd nixl && sudo ninja && sudo ninja install
```

Langkah 7: Instal NIXL Benchmark dan uji konfigurasi EFA dan NIXL Anda

Instal Benchmark NIXL dan jalankan pengujian untuk memastikan bahwa instans sementara Anda dikonfigurasi dengan benar untuk EFA dan NIXL. Benchmark NIXL memungkinkan Anda untuk mengonfirmasi bahwa NIXL diinstal dengan benar dan beroperasi seperti yang diharapkan. Untuk informasi selengkapnya, lihat repositori nixlbench.

NIXL Benchmark (nixlbench) membutuhkan ETCD untuk koordinasi antara klien dan server. Untuk menggunakan ETCD dengan NIXL memerlukan ETCD Server dan Klien, dan ETCD CPP API.

Build from Docker

Untuk menginstal dan menguji NIXL Benchmark menggunakan Docker

1. Kloning repositori NIXL resmi ke instance dan navigasikan ke direktori build nixlbench.

```
$ git clone https://github.com/ai-dynamo/nixl.git
$ cd nixl/benchmark/nixlbench/contrib
```

2. Bangun wadahnya.

```
$ ./build.sh
```

Untuk informasi selengkapnya tentang opsi build Docker, lihat repositori nixlbench.

3. Pasang Docker.

```
$ sudo apt install docker.io -y
```

4. Mulai server ETCD untuk koordinasi.

```
$ docker run -d --name etcd-server \
    -p 2379:2379 -p 2380:2380 \
    quay.io/coreos/etcd:v3.5.18 \
    /usr/local/bin/etcd \
    --data-dir=/etcd-data \
    --listen-client-urls=http://0.0.0.0:2379 \
    --advertise-client-urls=http://0.0.0.0:2379 \
    --listen-peer-urls=http://0.0.0.0:2380 \
    --initial-advertise-peer-urls=http://0.0.0.0:2380 \
    --initial-cluster=default=http://0.0.0.0:2380
```

5. Validasi bahwa server ETCD sedang berjalan.

```
$ curl -L http://localhost:2379/health
```

Keluaran yang diharapkan

```
{"health":"true"}
```

6. Buka dua terminal untuk contoh. Pada kedua terminal, jalankan perintah berikut untuk memverifikasi instalasi. Perintah menggunakan server ETCD pada instance yang sama, menggunakan Libfabric sebagai backend, dan beroperasi menggunakan memori GPU.

```
$ docker run -it --gpus all --network host nixlbench:latest \
    nixlbench --etcd_endpoints http://localhost:2379 \
    --backend LIBFABRIC \
    --initiator_seg_type VRAM \
    --target_seg_type VRAM
```

> **Note**
>
> Gunakan nilai `DRAM` alih-alih `VRAM` untuk instance non-GPU.

Build from source

> **Important**
>
> Ikuti tab ini hanya jika Anda memilih Build from source di Langkah 6.

Untuk menginstal NIXL Benchmark

1. Instal dependensi sistem yang diperlukan.

```
$ sudo apt install libgflags-dev
```

2. Instal ETCD Server dan Klien.

```
$ sudo apt install -y etcd-server etcd-client
```

3. Instal ETCD CPP API.

   a. Instal dependensi yang diperlukan untuk ETCD CPP API.

```
$ sudo apt install libboost-all-dev libssl-dev libgrpc-dev libgrpc++-dev
 libprotobuf-dev protobuf-compiler-grpc libcpprest-dev
```

b. Kloning dan instal ETCD CPP API.

```
$ cd $HOME
$ git clone https://github.com/etcd-cpp-apiv3/etcd-cpp-apiv3.git
$ cd etcd-cpp-apiv3
$ mkdir build && cd build
$ cmake ..
$ sudo make -j$(nproc) && sudo make install
```

4. Bangun dan instal nixlbench.

```
$ sudo meson setup . $HOME/nixl/benchmark/nixlbench -Dnixl_path=/usr/local/nixl/
$ sudo ninja && sudo ninja install
```

Untuk menguji konfigurasi EFA dan NIXL

1. Mulai server ETCD pada instance.

```
$ etcd --listen-client-urls "http://0.0.0.0:2379" \
    --advertise-client-urls "http://localhost:2379" &
```

2. Validasi bahwa server ETCD sedang berjalan.

```
$ curl -L http://localhost:2379/health
```

Keluaran yang diharapkan

```
{"health":"true"}
```

3. Buka dua terminal untuk contoh. Di kedua terminal, selesaikan langkah-langkah berikut untuk menjalankan nixlbench.

a. Arahkan ke direktori tempat nixlbench diinstal.

```
$ cd /usr/local/nixlbench/bin/
```

b. Jalankan pengujian dan tentukan backend, alamat server ETCD, dan tipe segmen inisiator. Perintah berikut menggunakan server ETCD pada contoh yang sama, menggunakan Libfabric sebagai backend, dan beroperasi menggunakan memori GPU. Variabel lingkungan mengkonfigurasi berikut ini:

   - `NIXL_LOG_LEVEL=INFO`- Mengaktifkan output debugging rinci. Anda juga dapat menentukan `WARN` untuk hanya menerima pesan kesalahan.
   - `LD_LIBRARY_PATH`— Menetapkan jalur untuk perpustakaan NIXL.

   Untuk informasi lebih lanjut tentang argumen Benchmark NIXL, lihat NIXLbenchREADME di repositori nixlbench resmi.

```
$ export NIXL_LOG_LEVEL=INFO
$ export LD_LIBRARY_PATH=/usr/local/nixl/lib/$(gcc -dumpmachine):
$LD_LIBRARY_PATH

$ nixlbench --etcd-endpoints 'http://localhost:2379' \
    --backend 'LIBFABRIC' \
    --initiator_seg_type 'VRAM' \
    --target_seg_type 'VRAM'
```

> **Note**
>
> Gunakan nilai `DRAM` alih-alih `VRAM` untuk instance non-GPU.

Langkah 8: Instal aplikasi pembelajaran mesin Anda

Instal aplikasi machine learning di instans sementara. Prosedur penginstalan bervariasi tergantung pada aplikasi machine learning tertentu.

> **Note**
>
> Lihat dokumentasi aplikasi pembelajaran mesin Anda untuk petunjuk pemasangan.

Langkah 9: Buat AMI yang mendukung EFA dan NIXL

Setelah menginstal komponen perangkat lunak yang diperlukan, Anda membuat AMI yang dapat digunakan kembali untuk meluncurkan instans Anda dengan EFA yang diaktifkan.

Untuk membuat AMI dari instans sementara Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans sementara yang Anda buat dan pilih Tindakan, Gambar, Buat gambar.
4. Untuk Buat gambar, lakukan hal berikut:
   a. Untuk Nama gambar, masukkan nama deskriptif untuk AMI.
   b. (Opsional) Untuk Deskripsi gambar, masukkan deskripsi singkat tentang tujuan AMI.
   c. Pilih Buat gambar.
5. Di panel navigasi, pilih AMIs.
6. Temukan AMI yang Anda buat dalam daftar. Tunggu hingga status berubah dari `pending` menjadi `available` sebelum melanjutkan ke langkah berikutnya.

Langkah 10: Mengakhiri instans sementara

Pada titik ini, Anda tidak memerlukan lagi instans sementara yang Anda luncurkan. Anda dapat mengakhiri instans agar biaya tidak dibebankan lagi padanya.

Untuk mengakhiri instans sementara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans sementara yang Anda buat dan pilih Tindakan, Status instans, Akhiri instans.
4. Saat diminta konfirmasi, pilih Akhiri.

Langkah 11: Luncurkan instans yang mendukung EFA dan NIXL

Luncurkan instans berkemampuan EFA dan NIXL Anda menggunakan AMI berkemampuan EFA yang Anda buat di Langkah 9, dan grup keamanan berkemampuan EFA yang Anda buat di Langkah 1.

Untuk meluncurkan instans yang mendukung EFA dan NIXL

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih Luncurkan Instans untuk membuka wizard peluncuran instans baru.
3. (Opsional) Di bagian Nama dan tanda, berikan nama untuk instans, seperti `EFA-instance`. Nama ditetapkan ke instans sebagai tanda sumber daya (`Name=`*`EFA-instance`*).
4. Di bagian Application and OS ImagesAMIs, pilih My, lalu pilih AMI yang Anda buat pada langkah sebelumnya.
5. Di bagian Jenis instans, pilih jenis instans yang didukung.
6. Pada bagian Pasangan kunci, pilih pasangan kunci yang akan digunakan untuk instans.
7. Di bagian Pengaturan jaringan, pilih Edit, lalu lakukan hal berikut:

   a. Untuk Subnet, pilih subnet untuk meluncurkan instans. Jika Anda tidak memilih subnet, Anda tidak dapat mengaktifkan instans untuk EFA.

   b. Untuk Firewall (grup keamanan), pilih Pilih grup keamanan yang ada, lalu pilih grup keamanan yang Anda buat di Langkah 1.

   c. Perluas bagian Konfigurasi jaringan lanjutan.

      Untuk antarmuka Jaringan 1, pilih Indeks kartu jaringan = 0, Indeks perangkat = 0, dan Jenis antarmuka = EFA dengan ENA.

      (Opsional) Jika Anda menggunakan jenis instans multi-kartu, seperti **`p4d.24xlarge`** atau**`p5.48xlarge`**, untuk setiap antarmuka jaringan tambahan yang diperlukan, pilih Tambahkan antarmuka jaringan, untuk indeks kartu jaringan pilih indeks berikutnya yang tidak digunakan, lalu pilih Indeks perangkat = 1 dan Jenis antarmuka = EFA dengan ENA atau EFA saja.
8. (Opsional) Di bagian Penyimpanan, konfigurasikan volume sesuai kebutuhan.
9. Di panel Ringkasan di sebelah kanan, untuk Jumlah instans, masukkan jumlah instans yang diaktifkan EFA yang ingin Anda luncurkan, lalu pilih Luncurkan instans.

Langkah 12: Mengaktifkan SSH tanpa kata sandi

Agar aplikasi Anda dapat berjalan di semua instans dalam klaster, Anda harus mengaktifkan akses SSH tanpa kata sandi dari simpul pemimpin ke simpul anggota. Simpul pemimpin adalah instans dari mana Anda menjalankan aplikasi Anda. Instans yang tersisa di klaster adalah simpul anggota.

Untuk mengaktifkan SSH tanpa kata sandi antar instans dalam klaster

1. Pilih satu instans dalam klaster sebagai simpul pemimpin, dan hubungkan ke instans tersebut.
2. Nonaktifkan `strictHostKeyChecking` dan aktifkan `ForwardAgent` pada simpul pemimpin. Buka `~/.ssh/config` menggunakan editor teks pilihan Anda dan tambahkan berikut ini.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Membuat pasangan kunci RSA.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   Pasangan kunci dibuat dalam direktori `$HOME/.ssh/`.
4. Ubah izin kunci privat pada simpul pemimpin.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Buka `~/.ssh/id_rsa.pub` menggunakan editor teks pilihan Anda dan salin kunci.
6. Untuk setiap simpul anggota di klaster, lakukan hal berikut:

   a. Hubungkan dengan instans.

   b. Buka `~/.ssh/authorized_keys` menggunakan editor teks pilihan Anda tambahkan kunci publik yang Anda salin sebelumnya.
7. Untuk menguji apakah SSH tanpa kata sandi berfungsi seperti yang diharapkan, hubungkan ke simpul pemimpin Anda dan jalankan perintah berikut.

   ```
   $ ssh member_node_private_ip
   ```

   Anda harus terhubung ke simpul anggota tanpa diminta untuk memasukkan kunci atau kata sandi.

> **Important**
>
> Ikuti Langkah 13 hanya jika Anda mengikuti Langkah 7.

Langkah 13: Uji konfigurasi EFA dan NIXL Anda di seluruh instance

Jalankan pengujian untuk memastikan bahwa instans Anda dikonfigurasi dengan benar untuk EFA dan NIXL.

Build from Docker

Untuk menguji konfigurasi EFA dan NIXL Anda di seluruh instance menggunakan Docker

1. Pilih dua host untuk menjalankan benchmark nixlbench. Gunakan alamat IP host pertama sebagai IP server ETCD untuk pertukaran metadata.
2. Mulai server ETCD di host 1.

```
$ docker run -d --name etcd-server \
    -p 2379:2379 -p 2380:2380 \
    quay.io/coreos/etcd:v3.5.18 \
    /usr/local/bin/etcd \
    --data-dir=/etcd-data \
    --listen-client-urls=http://0.0.0.0:2379 \
    --advertise-client-urls=http://0.0.0.0:2379 \
    --listen-peer-urls=http://0.0.0.0:2380 \
    --initial-advertise-peer-urls=http://0.0.0.0:2380 \
    --initial-cluster=default=http://0.0.0.0:2380
```

3. Validasi bahwa server ETCD sedang berjalan.

```
$ curl -L http://localhost:2379/health
```

```
{"health":"true"}
```

4. Jalankan benchmark nixlbench pada host 1.

```
$ docker run -it --gpus all --network host nixlbench:latest \
    nixlbench --etcd_endpoints http://localhost:2379 \
    --backend LIBFABRIC \
```

```
    --initiator_seg_type VRAM
```

5. Jalankan benchmark nixlbench pada host 2.

```
$ docker run -it --gpus all --network host nixlbench:latest \
    nixlbench --etcd_endpoints http://ETCD_SERVER_IP:2379 \
    --backend LIBFABRIC \
    --initiator_seg_type VRAM
```

Build from source

> **Important**
>
> Ikuti tab ini hanya jika Anda memilih Build from source di Langkah 6.

Untuk menguji konfigurasi EFA dan NIXL Anda di seluruh instance

1. Pilih dua host untuk menjalankan benchmark nixlbench. Gunakan alamat IP host pertama sebagai IP server ETCD untuk pertukaran metadata.
2. Luncurkan server ETCD di host 1.

```
$ etcd --listen-client-urls "http://0.0.0.0:2379" \
    --advertise-client-urls "http://localhost:2379" &
```

3. Validasi bahwa server ETCD sedang berjalan.

```
$ curl -L http://localhost:2379/health
```

```
{"health":"true"}
```

4. Jalankan benchmark nixlbench pada host 1.

```
$ export NIXL_LOG_LEVEL=INFO
$ export LD_LIBRARY_PATH=$HOME/nixl/lib/x86_64-linux-gnu:$LD_LIBRARY_PATH

$ nixlbench \
    --etcd-endpoints http://localhost:2379 \
    --backend LIBFABRIC \
```

```
    --initiator_seg_type VRAM
```

5. Jalankan benchmark nixlbench pada host 2.

```
$ export NIXL_LOG_LEVEL=INFO
$ export LD_LIBRARY_PATH=$HOME/nixl/lib/x86_64-linux-gnu:$LD_LIBRARY_PATH

$ nixlbench \
    --etcd-endpoints http://ETCD_SERVER_IP:2379 \
    --backend LIBFABRIC \
    --initiator_seg_type VRAM
```

Langkah 14: Uji penyajian inferensi terpilah melalui VllM (Opsional)

Setelah NIXL diinstal, Anda dapat menggunakan NIXL melalui inferensi LLM dan kerangka kerja penyajian seperti VllM,, dan TensorRT-LLM. SGLang

Untuk melayani beban kerja inferensi Anda menggunakan VllM

1. Instal Vllm.

```
$ pip install vllm
```

2. Mulai server VLLM dengan NIXL. Contoh perintah berikut membuat satu prefill (producer) dan satu decode (consumer) instance untuk koneksi handshake NIXL, konektor KV, peran KV, dan backend transport. Untuk contoh dan skrip terperinci, lihat Panduan NIXLConnector Penggunaan.

   Untuk menggunakan NIXL dengan EFA, atur variabel lingkungan berdasarkan kasus penyiapan dan penggunaan Anda.

   - Konfigurasi Produser (Prefiller)

```
$ vllm serve your-application \
    --port 8200 \
    --enforce-eager \
    --kv-transfer-config
 '{"kv_connector":"NixlConnector","kv_role":"kv_both","kv_buffer_device":"cuda","kv_conne
{"backends":["LIBFABRIC"]}}'
```

   - Konfigurasi konsumen (Decoder)

```
$ vllm serve your-application \
    --port 8200 \
    --enforce-eager \
    --kv-transfer-config
 '{"kv_connector":"NixlConnector","kv_role":"kv_both","kv_buffer_device":"cuda","kv_conne
{"backends":["LIBFABRIC"]}}'
```

Konfigurasi sampel sebelumnya menetapkan hal berikut:

- `kv_role`untuk`kv_both`, yang memungkinkan fungsionalitas simetris di mana konektor dapat bertindak sebagai produsen dan konsumen. Ini memberikan fleksibilitas untuk pengaturan eksperimental dan skenario di mana perbedaan peran tidak ditentukan sebelumnya.
- `kv_buffer_device`untuk`cuda`, yang memungkinkan menggunakan memori GPU.
- NIXL backend ke`LIBFABRIC`, yang memungkinkan lalu lintas NIXL melewati EFA.

Maksimalkan bandwidth jaringan pada instans Amazon EC2 dengan beberapa kartu jaringan

Banyak jenis contoh yang mendukung EFA juga memiliki beberapa kartu jaringan. Untuk informasi selengkapnya, lihat Kartu jaringan. Jika Anda berencana untuk menggunakan EFA dengan salah satu jenis instans ini, kami merekomendasikan konfigurasi dasar berikut:

- Untuk antarmuka jaringan utama (indeks kartu jaringan`0`, indeks perangkat`0`), buat antarmuka ENA. Anda tidak dapat menggunakan antarmuka jaringan khusus EFA sebagai antarmuka jaringan utama.
- Jika indeks kartu jaringan 0 mendukung EFA, buat antarmuka jaringan khusus EFA untuk indeks kartu jaringan`0`, indeks perangkat. 1
- Untuk setiap antarmuka jaringan tambahan, gunakan indeks kartu jaringan yang tidak digunakan berikutnya, indeks perangkat`0`, untuk antarmuka jaringan khusus EFA, indeks and/or perangkat 1 untuk antarmuka jaringan ENA tergantung pada kasus penggunaan Anda, seperti persyaratan bandwidth ENA atau ruang alamat IP. Misalnya kasus penggunaan, lihatKonfigurasi EFA untuk instans P5 dan P5e.

> **Note**
>
> Instans P5 memerlukan antarmuka jaringan untuk dikonfigurasi dengan cara tertentu untuk mengaktifkan bandwidth jaringan maksimum. Untuk informasi selengkapnya, lihat Konfigurasi EFA untuk instans P5 dan P5e.

Contoh berikut menunjukkan cara meluncurkan instance berdasarkan rekomendasi ini.

Instance launch

Untuk menentukan EFAs selama peluncuran instance menggunakan wizard instance peluncuran

1. Di bagian Pengaturan jaringan, pilih Edit.
2. Perluas Konfigurasi jaringan lanjutan.
3. Untuk antarmuka jaringan utama (indeks kartu jaringan`0`, indeks perangkat`0`), buat antarmuka ENA. Anda tidak dapat menggunakan antarmuka jaringan khusus EFA sebagai antarmuka jaringan utama.
4. Jika indeks kartu jaringan 0 mendukung EFA, buat antarmuka jaringan khusus EFA untuk indeks kartu jaringan`0`, indeks perangkat. 1
5. Untuk setiap antarmuka jaringan tambahan, gunakan indeks kartu jaringan yang tidak digunakan berikutnya, indeks perangkat`0`, untuk antarmuka jaringan khusus EFA, indeks and/or perangkat 1 untuk antarmuka jaringan ENA tergantung pada kasus penggunaan Anda, seperti persyaratan bandwidth ENA atau ruang alamat IP. Misalnya kasus penggunaan, lihatKonfigurasi EFA untuk instans P5 dan P5e.

Untuk menentukan EFAs selama peluncuran instance menggunakan perintah run-instance

Untuk`--network-interfaces`, tentukan jumlah antarmuka jaringan yang diperlukan. Untuk antarmuka jaringan utama, tentukan`NetworkCardIndex=0`,`DeviceIndex=0`, dan`InterfaceType=interface`. Jika indeks kartu jaringan 0 mendukung EFA, tentukan, `NetworkCardIndex=0``DeviceIndex=1`, dan`InterfaceType=efa-only`. Untuk antarmuka jaringan tambahan, untuk `NetworkCardIndex` tentukan indeks berikutnya yang tidak digunakan, `DeviceIndex=0` untuk`InterfaceType=efa-only`, and/or `DeviceIndex=1` untuk. `InterfaceType=interface`

Contoh cuplikan perintah berikut menunjukkan permintaan dengan 32 perangkat EFA dan satu perangkat ENA.

```
$ aws ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami-0abcdef1234567890 \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 \
"NetworkCardIndex=0,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
```

```
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=17,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=18,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=19,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=20,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=21,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=22,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=23,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=24,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=25,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=26,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=27,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=28,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=29,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=30,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=31,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only"
...
```

Launch templates

Untuk menambahkan EFA ke template peluncuran menggunakan konsol Amazon EC2

1. Di bagian Pengaturan jaringan, perluas Konfigurasi jaringan lanjutan.
2. Untuk antarmuka jaringan utama (indeks kartu jaringan`0`, indeks perangkat`0`), buat antarmuka ENA. Anda tidak dapat menggunakan antarmuka jaringan khusus EFA sebagai antarmuka jaringan utama.

3. Jika indeks kartu jaringan 0 mendukung EFA, buat antarmuka jaringan khusus EFA untuk indeks kartu jaringan`0`, indeks perangkat. 1
4. Untuk setiap antarmuka jaringan tambahan, gunakan indeks kartu jaringan yang tidak digunakan berikutnya, indeks perangkat`0`, untuk antarmuka jaringan khusus EFA, indeks and/or perangkat 1 untuk antarmuka jaringan ENA tergantung pada kasus penggunaan Anda, seperti persyaratan bandwidth ENA atau ruang alamat IP. Misalnya kasus penggunaan, lihatKonfigurasi EFA untuk instans P5 dan P5e.

Untuk EFAs menambah template peluncuran menggunakan create-launch-templateperintah

Untuk`NetworkInterfaces`, tentukan jumlah antarmuka jaringan yang diperlukan. Untuk antarmuka jaringan utama, tentukan`NetworkCardIndex=0`,`DeviceIndex=0`, dan`InterfaceType=interface`. Jika indeks kartu jaringan 0 mendukung EFA, tentukan, `NetworkCardIndex=0``DeviceIndex=1`, dan`InterfaceType=efa-only`. Untuk antarmuka jaringan tambahan, untuk `NetworkCardIndex` tentukan indeks berikutnya yang tidak digunakan, `DeviceIndex=0` untuk`InterfaceType=efa-only`, and/or `DeviceIndex=1` untuk. `InterfaceType=interface`

Cuplikan berikut menunjukkan contoh dengan 3 antarmuka jaringan dari kemungkinan 32 antarmuka jaringan.

```
"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "interface",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 0,
  "DeviceIndex": 1,
  "InterfaceType": "efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
```

```
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
  "DeviceIndex": 0,
  "InterfaceType": "efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 0,
  "InterfaceType": "efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 3,
  "DeviceIndex": 0,
  "InterfaceType": "efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
}
...
```

Konfigurasi EFA untuk instans P5 dan P5e

`p5.48xlarge`dan `p5e.48xlarge` contoh mendukung 32 kartu jaringan dan memiliki total kapasitas bandwidth jaringan 3.200 Gbps, yang hingga 800 Gbps dapat digunakan untuk lalu lintas jaringan IP. Karena lalu lintas jaringan EFA dan IP berbagi sumber daya dasar yang sama, bandwidth yang digunakan oleh satu akan mengurangi bandwidth yang tersedia untuk yang lain. Ini berarti Anda dapat mendistribusikan bandwidth jaringan antara lalu lintas EFA dan lalu lintas IP dalam kombinasi apa pun, selama total bandwidth tidak melebihi 3.200 Gbps dan bandwidth IP tidak melebihi 800

Gbps. Misalnya, jika Anda menggunakan 400 Gbps untuk bandwidth IP, Anda dapat mencapai bandwidth EFA hingga 2.800 Gbps secara bersamaan.

Kasus penggunaan 1: Simpan alamat IP dan hindari potensi masalah IP Linux

Konfigurasi ini menyediakan bandwidth jaringan EFA hingga 3200 Gbps dan bandwidth jaringan IP hingga 100 Gbps dengan satu alamat IP pribadi. Konfigurasi ini juga membantu menghindari potensi masalah IP Linux, seperti penetapan otomatis alamat IP publik yang tidak diizinkan dan tantangan perutean IP (masalah pemetaan nama host ke alamat IP dan ketidakcocokan alamat IP sumber), yang dapat muncul jika sebuah instance memiliki beberapa antarmuka jaringan.

- Untuk antarmuka jaringan utama (indeks kartu jaringan 0, indeks perangkat 0), gunakan antarmuka ENA.
- Untuk indeks kartu jaringan 0, indeks perangkat 1, buat antarmuka jaringan khusus EFA.
- Untuk antarmuka jaringan yang tersisa (indeks kartu jaringan 1-31, indeks perangkat 0), gunakan antarmuka jaringan khusus EFA.

Kasus penggunaan 2: Bandwidth jaringan EFA dan IP maksimum

Konfigurasi ini menyediakan bandwidth jaringan EFA hingga 3200 Gbps dan bandwidth jaringan IP hingga 800 Gbps dengan 8 alamat IP pribadi. Anda tidak dapat menetapkan alamat IP publik secara otomatis dengan konfigurasi ini. Namun, Anda dapat melampirkan alamat IP Elastis ke antarmuka jaringan utama (indeks kartu jaringan 0, indeks perangkat 0) setelah peluncuran untuk konektivitas internet.

- Untuk antarmuka jaringan utama (indeks kartu jaringan 0, indeks perangkat 0), gunakan antarmuka jaringan ENA.
- Untuk antarmuka yang tersisa, lakukan hal berikut:
  - Tentukan antarmuka jaringan khusus EFA pada indeks kartu jaringan 0 indeks perangkat 1, dan untuk indeks kartu jaringan 1, 2, dan 3, gunakan indeks perangkat 0.
  - Tentukan satu antarmuka jaringan ENA dan empat antarmuka jaringan khusus EFA di masing-masing subset indeks kartu jaringan berikut, dan gunakan indeks perangkat 1 untuk antarmuka jaringan ENA dan indeks perangkat 0 untuk antarmuka jaringan khusus EFA:
    - [4,5,6,7]
    - [8,9,10,11]
    - [12,13,14,15]

- [16,17,18,19]
- [20,21,22,23]
- [24,25,26,27]
- [28,29,30,31]

Contoh berikut menggambarkan konfigurasi ini:

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=0,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
```

```
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=17,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=18,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=19,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=20,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=21,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=22,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=23,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=24,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=25,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=26,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=27,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
```

```
"NetworkCardIndex=28,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=29,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=30,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=31,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only"
...
```

Konfigurasi EFA untuk instans P6-B200

Instans P6-B200 memiliki total kapasitas bandwidth jaringan 3.200 Gbps, dimana hingga 1600 Gbps dapat digunakan untuk ENA. Mereka memiliki 8 GPUs dan 8 kartu jaringan, di mana setiap kartu jaringan mendukung bandwidth EFA hingga 400 Gbps dan bandwidth ENA 200 Gbps. Karena lalu lintas EFA dan ENA berbagi sumber daya dasar yang sama, bandwidth yang digunakan oleh satu akan mengurangi bandwidth yang tersedia untuk yang lain.

Kasus penggunaan 1: Simpan alamat IP

Konfigurasi ini menggunakan setidaknya satu alamat IP pribadi per instance dan mendukung bandwidth EFA hingga 3200 Gbps dan bandwidth ENA 200 Gbps.

- Untuk antarmuka jaringan utama (indeks kartu jaringan 0, indeks perangkat 0), gunakan antarmuka ENA.
- Untuk indeks kartu jaringan 0, indeks perangkat 1, buat antarmuka jaringan khusus EFA.
- Untuk 7 kartu jaringan yang tersisa (indeks kartu jaringan 1-7, indeks perangkat 0), gunakan antarmuka jaringan khusus EFA.

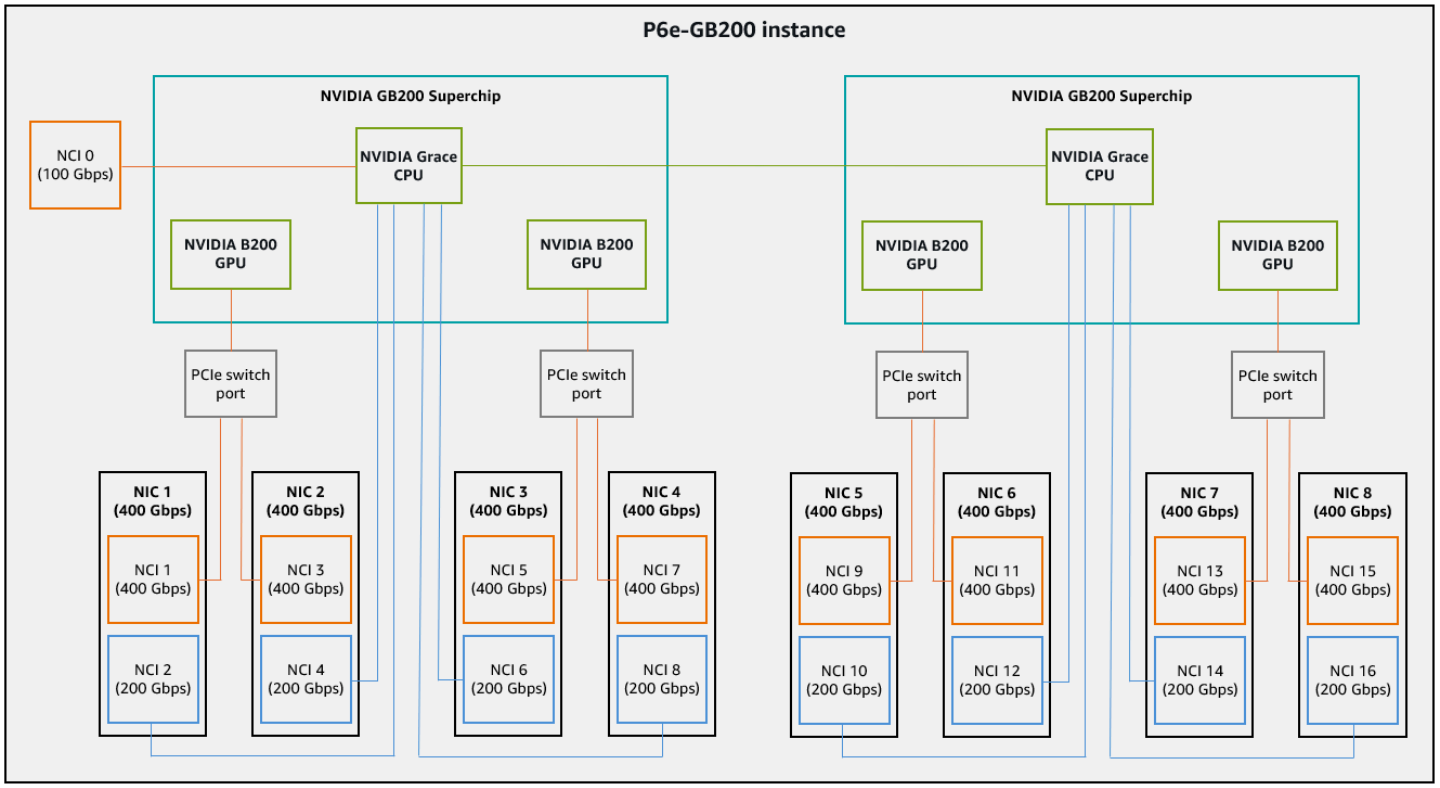
Kasus penggunaan 2: Bandwidth EFA dan ENA maksimum

Konfigurasi ini menggunakan setidaknya 8 alamat IP pribadi per instans dan mendukung bandwidth EFA hingga 3200 Gbps dan bandwidth ENA 1600 Gbps.

- Untuk antarmuka jaringan utama (indeks kartu jaringan 0, indeks perangkat 0), gunakan antarmuka ENA.
- Untuk indeks kartu jaringan 0, indeks perangkat 1, buat antarmuka jaringan khusus EFA.
- Untuk 7 kartu jaringan yang tersisa (indeks kartu jaringan 1-7), buat antarmuka jaringan khusus EFA pada indeks perangkat 0 dan antarmuka jaringan ENA pada indeks perangkat 1.

Konfigurasi EFA untuk instance P6e- GB200

P6e- GB200 instance dapat dikonfigurasi dengan hingga 17 kartu jaringan. Gambar berikut menunjukkan tata letak kartu antarmuka jaringan fisik (NIC) untuk GB200 instance P6e-, bersama dengan pemetaan indeks kartu jaringan (). NCIs



NCI utama (indeks 0) mendukung bandwidth ENA hingga 100 Gbps. NCIs dengan indeks berikut mendukung antarmuka jaringan khusus EFA dan bandwidth EFA 400 Gbps: [1, 3, 5, 7, 9, 11, 13, 15]. NCIs dengan indeks berikut mendukung hingga 200 Gbps ENA atau bandwidth EFA: [2, 4, 6, 8, 10, 12, 14, 16].

NCIs Dalam kelompok berikut berbagi NIC fisik yang mendasarinya pada host:

- [1 dan 2]
- [3 dan 4]
- [5 dan 6]
- [7 dan 8]
- [9 dan 10]
- [11 dan 12]
- [13 dan 14]

- [15 dan 16]

Setiap NIC fisik mendukung bandwidth hingga 400 Gbps. Karena NCIs dalam kelompok-kelompok ini berbagi NIC fisik dasar yang sama, bandwidth yang digunakan oleh satu akan mengurangi bandwidth yang tersedia untuk yang lain. Misalnya, jika NCI 2 menggunakan bandwidth ENA 200 Gbps, NCI 1 dapat menggunakan bandwidth EFA hingga 200 Gbps secara bersamaan.

Setiap GPU yang mendasari pada host dapat mengirim lalu lintas secara langsung melalui pasangan berikut: NCIs

- [1 dan 3]
- [5 dan 7]
- [9 dan 11]
- [13 dan 15]

Setiap GPU mendukung bandwidth EFA hingga 400 Gbps. Karena kartu jaringan dalam kelompok ini berbagi GPU yang sama, bandwidth yang digunakan oleh satu akan mengurangi bandwidth yang tersedia untuk yang lain. Misalnya, jika NCI 1 menggunakan bandwidth EFA 200 Gbps, NCI 3 dapat menggunakan bandwidth EFA hingga 200 Gbps secara bersamaan. Oleh karena itu, untuk mencapai kinerja EFA maksimum, kami menyarankan Anda melakukan salah satu hal berikut untuk mencapai total bandwidth EFA 1.600 Gbps:

- Tambahkan antarmuka jaringan khusus EFA ke hanya satu NCI di setiap grup untuk mencapai 400 Gbps per antarmuka jaringan (4 antarmuka jaringan EFA x 400 Gbps).
- Tambahkan antarmuka jaringan khusus EFA ke setiap NCI di setiap grup untuk mencapai 200 Gbps per antarmuka jaringan (8 antarmuka jaringan EFA x 200 Gbps).

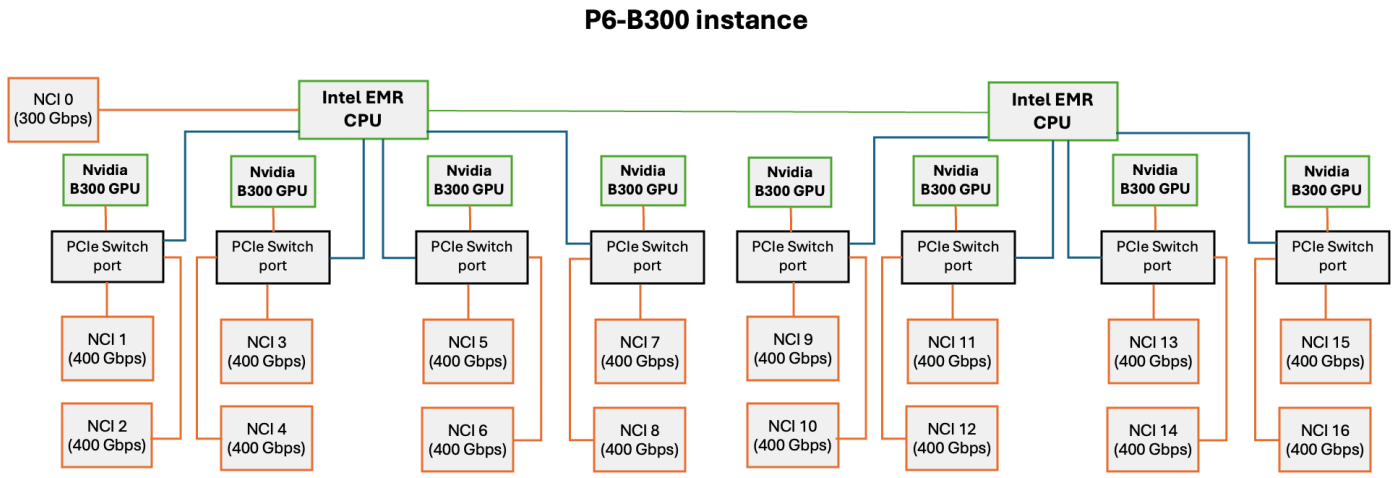
Misalnya, konfigurasi berikut menyediakan bandwidth EFA hingga 1.600 Gbps menggunakan antarmuka jaringan khusus EFA tunggal di setiap grup NCI, dan bandwidth jaringan ENA hingga 100 Gbps hanya menggunakan NCI utama (indeks 0).

- Untuk NCI utama (indeks kartu jaringan 0, indeks perangkat 0), gunakan antarmuka jaringan ENA.
- Tambahkan antarmuka jaringan khusus EFA ke yang berikut ini:
  - NCI 1, indeks perangkat 0
  - NCI 5, indeks perangkat 0

- NCI 9, indeks perangkat 0
- NCI 13, indeks perangkat 0

Konfigurasi EFA untuk instans P6-B300

Instans P6-B300 memiliki total kapasitas bandwidth jaringan hingga 6400 Gbps untuk lalu lintas EFA, dan hingga 3870 Gbps untuk lalu lintas ENA. Mereka memiliki 8 GPUs dan 17 kartu jaringan, di mana kartu jaringan utama hanya mendukung antarmuka jaringan ENA dengan bandwidth hingga 350 Gbps. Kartu jaringan sekunder mendukung hingga 400 Gbps EFA dan bandwidth ENA hingga 220 Gbps. Karena lalu lintas EFA dan ENA berbagi sumber daya dasar yang sama, bandwidth yang digunakan oleh satu akan mengurangi bandwidth yang tersedia untuk yang lain.



Kasus penggunaan 1: Simpan alamat IP

Konfigurasi ini menggunakan setidaknya satu alamat IP pribadi per instans dan mendukung bandwidth EFA hingga 6400 Gbps dan bandwidth ENA hingga 350 Gbps.

- Untuk antarmuka jaringan utama (indeks kartu jaringan 0, indeks perangkat 0), gunakan antarmuka jaringan ENA.
- Untuk kartu jaringan yang tersisa (indeks kartu jaringan 1-16, indeks perangkat 0), gunakan antarmuka jaringan khusus EFA.

```
--network-interfaces \
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
```

```
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only"
```

Kasus penggunaan 2: Bandwidth EFA dan ENA maksimum

Konfigurasi ini menggunakan setidaknya 17 alamat IP pribadi per instans dan mendukung bandwidth EFA hingga 6400 Gbps dan bandwidth ENA hingga 3870 Gbps.

- Untuk antarmuka jaringan utama (indeks kartu jaringan 0, indeks perangkat 0) gunakan antarmuka jaringan ENA.
- Untuk kartu jaringan yang tersisa, buat antarmuka khusus EFA (indeks kartu jaringan 1-16 indeks perangkat 0) dan kartu jaringan antarmuka ENA mengindeks 1-16 indeks perangkat 1).

```
--network-interfaces \
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
```

```
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
```

Membuat dan melampirkan Adaptor Kain Elastis ke instans Amazon EC2

Anda dapat membuat EFA dan melampirkannya ke instans Amazon EC2 seperti halnya antarmuka elastic network lainnya di Amazon EC2. Namun, tidak seperti antarmuka jaringan elastis, tidak EFAs dapat dilampirkan atau dilepaskan dari instance dalam keadaan. `running`

Pertimbangan-pertimbangan

- Anda dapat mengubah grup keamanan yang terkait dengan EFA. Untuk mengaktifkan fungsi bypass OS, EFA harus merupakan anggota grup keamanan yang memungkinkan semua lalu lintas masuk dan keluar ke dan dari grup keamanan itu sendiri. Untuk informasi selengkapnya, lihat Langkah 1: Siapkan grup keamanan yang diaktifkan EFA.

  Anda mengubah grup keamanan yang terkait dengan EFA dalam cara yang sama dengan cara Anda mengubah grup keamanan yang terkait dengan antarmuka jaringan elastis. Untuk informasi selengkapnya, lihat the section called “Memodifikasi atribut antarmuka jaringan”.

- Anda menetapkan Elastic IP (IPv4) dan IPv6 alamat ke antarmuka jaringan EFA (EFA dengan ENA) dengan cara yang sama seperti Anda menetapkan alamat IP ke antarmuka jaringan elastis. Untuk informasi selengkapnya, lihat Mengelola alamat IP.

  Anda tidak dapat menetapkan alamat IP ke antarmuka jaringan khusus EFA.

Tugas

- Membuat AMI
- Memasang EFA ke instans yang dihentikan
- Memasang EFA saat meluncurkan instans
- Menambahkan EFA ke templat peluncuran

Membuat AMI

Anda dapat membuat EFA dalam subnet di VPC. Anda tidak dapat memindahkan EFA ke subnet lain dibuat, dan Anda hanya dapat memasangkannya untuk menghentikan instans dalam Zona Ketersediaan yang sama.

Console

Untuk membuat antarmuka jaringan EFA (EFA dengan ENA atau ENA-only)

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Antarmuka Jaringan, lalu pilih Buat antarmuka jaringan.
3. Untuk Deskripsi, masukkan nama deskriptif untuk EFA.
4. Untuk Subnet, pilih subnet untuk membuat EFA.
5. Jenis antarmuka, pilih salah satu opsi berikut:
   - EFA dengan ENA — Untuk membuat antarmuka jaringan yang mendukung perangkat ENA dan EFA.
   - EFA Only — Untuk membuat antarmuka jaringan dengan perangkat EFA saja.
6. (Untuk EFA dengan ENA saja) Konfigurasikan alamat IP dan penetapan awalan untuk antarmuka jaringan. Jenis alamat IP dan awalan yang dapat Anda tetapkan tergantung pada subnet yang dipilih. Untuk subnet IPv4 -only, Anda dapat menetapkan alamat IPv4 IP dan awalan saja. Untuk subnet IPv6 -only, Anda dapat menetapkan alamat IPv6 IP dan awalan

saja. Untuk subnet dual-stack, Anda dapat menetapkan keduanya IPv4 dan IPv6 alamat IP dan awalan.

> **Note**
>
> Anda tidak dapat menetapkan alamat IP ke antarmuka jaringan khusus EFA.

a. Untuk IPv4 alamat and/or IPv6 alamat pribadi, pilih Tetapkan otomatis agar Amazon EC2 secara otomatis menetapkan alamat IP dari subnet yang dipilih, atau pilih Kustom untuk menentukan alamat IP yang akan ditetapkan secara manual.

b. Jika Anda menetapkan IPv6 alamat, Anda dapat mengaktifkan Tetapkan IP primer secara opsional. IPv6 Melakukan hal ini memberikan alamat unicast IPv6 global primer (GUA) ke antarmuka jaringan. Menetapkan IPv6 alamat utama memungkinkan Anda untuk menghindari mengganggu lalu lintas ke instance atau. ENIs Untuk informasi selengkapnya, lihat IPv6 alamat.

c. Untuk delegasi IPv4 awalan delegasi and/or IPv6 awalan, pilih Tetapkan otomatis agar Amazon EC2 secara otomatis menetapkan awalan dari blok CIDR subnet, atau pilih Kustom untuk menentukan awalan secara manual dari blok CIDR subnet. Jika Anda menentukan awalan, AWS verifikasi bahwa itu belum ditetapkan ke sumber daya lain. Untuk informasi selengkapnya, lihat Delegasi awalan untuk antarmuka jaringan Amazon EC2

d. (Opsional) Konfigurasikan pengaturan batas waktu pelacakan koneksi Idle. Untuk informasi selengkapnya, lihat Waktu habis pelacakan koneksi idle

   - TCP menetapkan batas waktu - Periode batas waktu, dalam hitungan detik, untuk koneksi TCP idle dalam keadaan mapan. Min: 60 detik. Maks: 432000 detik (5 hari). Default: 432.000 detik. Direkomendasikan: Kurang dari 432000 detik.
   - Batas waktu UDP — Periode batas waktu, dalam hitungan detik, untuk arus UDP idle yang telah melihat lalu lintas hanya dalam satu arah atau satu transaksi permintaan-respons. Min: 30 detik. Maks: 60 detik. Default: 30 detik.
   - Batas waktu aliran UDP — Periode batas waktu, dalam hitungan detik, untuk aliran UDP idle diklasifikasikan sebagai aliran yang telah melihat lebih dari satu transaksi permintaan-respons. Min: 60 detik. Maks: 180 detik (3 menit). Default: 180 detik.

7. Untuk Grup keamanan, pilih satu atau beberapa grup keamanan.
8. Pilih Buat antarmuka jaringan.

AWS CLI

Untuk membuat EFA

Gunakan perintah create-network-interface. Untuk `--interface-type`, tentukan `efa` untuk antarmuka jaringan EFA atau `efa-only` untuk antarmuka jaringan khusus EFA.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --interface-type efa \
    --description "my efa"
```

PowerShell

Untuk membuat EFA

Gunakan New-EC2NetworkInterfacecmdlet. Untuk `-InterfaceType`, tentukan `efa` antarmuka jaringan EFA atau `efa-only` untuk antarmuka jaringan khusus EFA

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -InterfaceType efa `
    -Description "my efa"
```

Memasang EFA ke instans yang dihentikan

Anda dapat memasang EFA ke instans yang didukung yang sedang dalam keadaan `stopped`. Anda tidak dapat memasang EFA ke instans yang sedang dalam keadaan `running`. Untuk informasi lebih lanjut tentang tipe instans yang didukung, lihat Tipe instans yang didukung.

Anda memasang EFA ke instans dengan cara yang sama seperti Anda memasang antarmuka jaringan ke suatu instans. Untuk informasi selengkapnya, lihat Lampirkan antarmuka jaringan.

Memasang EFA saat meluncurkan instans

AWS CLI

Untuk melampirkan EFA yang ada saat meluncurkan instance

Gunakan perintah run-instance dengan opsi. `--network-interfaces` Untuk antarmuka jaringan utama, tentukan antarmuka jaringan EFA dan`NetworkCardIndex=0`,`DeviceIndex=0`. Untuk melampirkan beberapa antarmuka jaringan EFA, lihat. Maksimalkan bandwidth jaringan

```
--network-interfaces "NetworkCardIndex=0, \
    DeviceIndex=0, \
    NetworkInterfaceId=eni-1234567890abcdef0, \
    Groups=sg-1234567890abcdef0, \
    SubnetId=subnet-0abcdef1234567890"
```

Untuk melampirkan EFA baru saat meluncurkan instance

Gunakan perintah run-instance dengan opsi. `--network-interfaces` Untuk antarmuka jaringan utama, gunakan`NetworkCardIndex=0`,`DeviceIndex=0`, dan`InterfaceType=efa`. Jika Anda melampirkan beberapa antarmuka jaringan EFA, lihat. Maksimalkan bandwidth jaringan

```
--network-interfaces "NetworkCardIndex=0, \
    DeviceIndex=0, \
    InterfaceType=efa, \
    Groups=sg-1234567890abcdef0, \
    SubnetId=subnet-0abcdef1234567890"
```

PowerShell

Untuk melampirkan EFA yang ada saat meluncurkan instance

Gunakan New-EC2Instancecmdlet dengan parameter. `-NetworkInterfaces`

```
-NetworkInterface $networkInterface
```

Tentukan antarmuka jaringan sebagai berikut.

```
$networkInterface = New-Object
 Amazon.EC2.Model.InstanceNetworkInterfaceSpecification
$networkInterface.DeviceIndex = 0
$networkInterface.NetworkInterfaceId = "eni-1234567890abcdef0"
$networkInterface.Groups = @("sg-1234567890abcdef0")
$networkInterface.SubnetId = "subnet-0abcdef1234567890"
```

Untuk melampirkan EFA baru saat meluncurkan instance

Gunakan New-EC2Instancecmdlet dengan parameter. `-NetworkInterfaces`

```
-NetworkInterface $networkInterface
```

Tentukan antarmuka jaringan sebagai berikut.

```
$networkInterface = New-Object
 Amazon.EC2.Model.InstanceNetworkInterfaceSpecification
$networkInterface.DeviceIndex = 0
$networkInterface.InterfaceType = "efa"
$networkInterface.Groups = @("sg-1234567890abcdef0")
$networkInterface.SubnetId = "subnet-0abcdef1234567890"
```

Menambahkan EFA ke templat peluncuran

Anda dapat membuat templat peluncuran yang berisi informasi konfigurasi yang diperlukan untuk meluncurkan instans yang diaktifkan EFA. Anda dapat menentukan antarmuka jaringan khusus EFA dan EFA di template peluncuran. Untuk membuat templat peluncuran yang diaktifkan EFA, buat templat peluncuran baru dan tentukan tipe instans yang didukung, AMI yang diaktifkan EFA Anda, dan grup keamanan yang diaktifkan EFA. Untuk`NetworkInterfaces`, tentukan antarmuka jaringan EFA untuk dilampirkan. Untuk antarmuka jaringan utama, gunakan`NetworkCardIndex=0`,`DeviceIndex=0`, dan`InterfaceType=efa`. Jika Anda melampirkan beberapa antarmuka jaringan EFA, lihat. Maksimalkan bandwidth jaringan pada instans Amazon EC2 dengan beberapa kartu jaringan

Anda dapat memanfaatkan template peluncuran untuk meluncurkan instans berkemampuan EFA dengan AWS layanan lain, seperti atau. AWS BatchAWS ParallelCluster

Untuk informasi lebih lanjut tentang membuat templat peluncuran, lihat Buat template peluncuran Amazon EC2.

Lepaskan dan hapus EFA dari instans Amazon EC2

Anda dapat melepaskan EFA dari instans Amazon EC2 dan menghapusnya dengan cara yang sama seperti antarmuka network elastis lainnya di Amazon EC2.

Melepas EFA

Untuk melepas EFA dari suatu instans, Anda harus menghentikan terlebih dahulu proses tersebut. Anda tidak dapat melepas EFA dari instans yang sedang berjalan.

Anda melepas EFA dari instans dengan cara yang sama seperti cara Anda melepas antarmuka jaringan dari suatu instans. Untuk informasi selengkapnya, lihat Lepaskan antarmuka jaringan.

Menghapus EFA

Untuk menghapus EFA, Anda harus melepasnya terlebih dahulu dari instans. Anda tidak dapat menghapus EFA saat masih terpasang di suatu instans.

Anda menghapus dengan EFAs cara yang sama seperti Anda menghapus antarmuka jaringan elastis. Untuk informasi selengkapnya, lihat Menghapus antarmuka jaringan.

Pantau Adaptor Kain Elastis di Amazon EC2

Anda dapat menggunakan fitur-fitur berikut untuk memantau performa Elastic Fabric Adapters Anda.

Topik

- Metrik driver EFA untuk instans Amazon EC2
- Log alur Amazon VPC
- Amazon CloudWatch

Metrik driver EFA untuk instans Amazon EC2

Driver Elastic Fabric Adapter (EFA) menerbitkan beberapa metrik dari instans yang memiliki antarmuka EFA terpasang, secara real time. Anda dapat menggunakan metrik ini untuk memecahkan masalah kinerja aplikasi dan jaringan, memilih ukuran klaster yang tepat untuk beban kerja, merencanakan aktivitas penskalaan secara proaktif, dan benchmark aplikasi untuk menentukan apakah metrik tersebut memaksimalkan kinerja EFA yang tersedia pada sebuah instans.

Topik

- Metrik driver EFA yang tersedia
- Ambil metrik driver EFA untuk instans Anda

Metrik driver EFA yang tersedia

Driver EFA menerbitkan metrik berikut ke instans secara real time. Mereka menyediakan jumlah kumulatif kesalahan, peristiwa koneksi, dan paket atau byte yang dikirim, diterima, dikirim ulang, atau dijatuhkan oleh perangkat EFA yang terpasang sejak peluncuran instance atau reset driver terakhir.

Metrik	Deskripsi	Tipe instans yang didukung
`tx_bytes`	Jumlah byte yang ditransmisikan. Satuan: byte	Semua jenis instans yang mendukung EFA
`rx_bytes`	Jumlah byte yang diterima. Satuan: byte	Semua jenis instans yang mendukung EFA
`tx_pkts`	Jumlah paket yang ditransmisikan. Satuan: hitung	Semua jenis instans yang mendukung EFA
`rx_pkts`	Jumlah paket yang diterima. Satuan: hitung	Semua jenis instans yang mendukung EFA
`rx_drops`	Jumlah paket yang diterima dan kemudian dijatuhkan. Satuan: hitung	Semua jenis instans yang mendukung EFA
`send_bytes`	Jumlah byte yang dikirim menggunakan operasi kirim. Satuan: byte	Semua jenis instans yang mendukung EFA
`recv_bytes`	Jumlah byte yang diterima oleh operasi kirim. Satuan: byte	Semua jenis instans yang mendukung EFA
`send_wrs`	Jumlah paket yang dikirim menggunakan operasi kirim.	Semua jenis instans yang mendukung EFA

Metrik	Deskripsi	Tipe instans yang didukung
	Satuan: hitung	
`recv_wrs`	Jumlah paket yang diterima oleh operasi kirim. Satuan: hitung	Semua jenis instans yang mendukung EFA
`rdma_write_wrs`	Jumlah operasi penulisan rdma yang diselesaikan. Satuan: hitung	Semua jenis instans yang mendukung EFA
`rdma_read_wrs`	Jumlah operasi baca rdma yang selesai. Satuan: hitung	Semua jenis instans yang mendukung EFA
`rdma_write_bytes`	Jumlah byte ditulis untuk itu oleh instance lain menggunakan operasi rdma write. Satuan: byte	Semua jenis instans yang mendukung EFA
`rdma_read_bytes`	Jumlah byte yang diterima menggunak an operasi baca rdma. Satuan: byte	Semua jenis instans yang mendukung EFA
`rdma_write_wr_err`	Jumlah operasi penulisan rdma yang memiliki kesalahan lokal atau jarak jauh. Satuan: hitung	Semua jenis instans yang mendukung EFA

Metrik	Deskripsi	Tipe instans yang didukung
`rdma_read_wr_err`	Jumlah operasi baca rdma yang memiliki kesalahan lokal atau jarak jauh. Satuan: hitung	Semua jenis instans yang mendukung EFA
`rdma_read_resp_bytes`	Jumlah byte yang dikirim sebagai tanggapan terhadap operasi baca rdma. Satuan: byte	Semua jenis instans yang mendukung EFA
`rdma_write_recv_bytes`	Jumlah byte yang diterima oleh operasi penulisan rdma. Satuan: byte	Semua jenis instans yang mendukung EFA
`retrans_bytes`	Jumlah byte EFA SRD yang ditransmi sikan kembali. Satuan: hitung	Nitro v4 dan jenis instans yang lebih baru yang mendukung EFA
`retrans_pkts`	Jumlah paket EFA SRD yang ditransmi sikan kembali. Satuan: byte	Nitro v4 dan jenis instans yang lebih baru yang mendukung EFA
`retrans_timeout_events`	Jumlah waktu lalu lintas EFA SRD habis dan mengakibatkan perubahan jalur jaringan. Satuan: hitung	Nitro v4 dan jenis instans yang lebih baru yang mendukung EFA

Metrik	Deskripsi	Tipe instans yang didukung
`impaired_remote_conn_events`	Berapa kali koneksi EFA SRD memasuki keadaan terganggu, sehingga mengurangi batas tingkat throughput. Satuan: hitung	Nitro v4 dan jenis instans yang lebih baru yang mendukung EFA
`unresponsive_remote_events`	Berapa kali koneksi jarak jauh EFA SRD tidak responsif. Satuan: hitung	Nitro v4 dan jenis instans yang lebih baru yang mendukung EFA

Untuk informasi selengkapnya tentang jenis instans yang mendukung EFA, lihatTipe instans yang didukung.

Ambil metrik driver EFA untuk instans Anda

Anda dapat menggunakan alat baris perintah rdma-tool untuk mengambil metrik untuk semua antarmuka EFA yang dilampirkan ke instance sebagai berikut:

```
$ rdma -p statistic show
link rdmap0s31/1
    tx_bytes 0
    tx_pkts 0
    rx_bytes 0
    rx_pkts 0
    rx_drops 0
    send_bytes 0
    send_wrs 0
    recv_bytes 0
    recv_wrs 0
    rdma_read_wrs 0
    rdma_read_bytes 0
    rdma_read_wr_err 0
    rdma_read_resp_bytes 0
    rdma_write_wrs 0
    rdma_write_bytes 0
```

```
    rdma_write_wr_err 0
    retrans_bytes 0
    retrans_pkts 0
    retrans_timeout_events 0
    unresponsive_remote_events 0
    impaired_remote_conn_events 0
```

Atau, Anda dapat mengambil metrik untuk setiap antarmuka EFA yang dilampirkan ke instance dari file sys menggunakan perintah berikut.

```
$ more /sys/class/infiniband/device_number/ports/port_number/hw_counters/* | cat
```

Sebagai contoh

```
$ more /sys/class/infiniband/rdmap0s31/ports/1/hw_counters/* | cat
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/lifespan
::::::::::::::
12
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_resp_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_wr_err
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_recv_bytes
::::::::::::::
0
```

```
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_wr_err
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/recv_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/recv_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_drops
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_pkts
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/send_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/send_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/tx_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/tx_pkts
::::::::::::::
0
```

```
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_bytes
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_pkts
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_timeout_events
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/unresponsive_remote_events
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/impaired_remote_conn_events
::::::::::::::
0
```

Log alur Amazon VPC

Anda dapat membuat Amazon VPC Flow Log untuk menangkap informasi tentang lalu lintas ke dan dari EFA. Data log aliran dapat dipublikasikan ke Amazon CloudWatch Logs dan Amazon S3. Setelah membuat log alur, Anda dapat mengambil dan melihat datanya di tujuan yang dipilih. Untuk informasi selengkapnya, lihat Log Alur VPC di Panduan Pengguna Amazon VPC.

Anda membuat log alur untuk EFA dengan cara yang sama dengan cara Anda membuat log alur untuk antarmuka jaringan yang elastis. Untuk informasi selengkapnya, lihat Membuat log alur di Panduan Pengguna Amazon VPC.

Dalam entri log alur, lalu lintas EFA diidentifikasi oleh `srcAddress` dan `destAddress`, yang keduanya diformat sebagai alamat MAC, sebagaimana ditunjukkan dalam contoh berikut.

```
version accountId  eniId        srcAddress        destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Jika Anda menggunakan EFA di klaster Amazon EKS, Anda dapat memantau EFAs penggunaan CloudWatch Container Insights. Amazon CloudWatch Container Insights mendukung semua

metrik driver EFA, kecuali:,`retrans_bytes`,, `retrans_pktsretrans_timeout_events`, `unresponsive_remote_events` dan. `impaired_remote_conn_events`

Untuk informasi selengkapnya, lihat metrik Amazon EKS dan Kubernetes Container Insights di Panduan Pengguna Amazon. CloudWatch

Memverifikasi penginstal EFA menggunakan checksum

Anda dapat secara opsional memverifikasi tarball EFA (`.tar.gz`file) menggunakan atau checksum. MD5 SHA256 Kami menyarankan Anda melakukan hal ini untuk memverifikasi identitas penerbit perangkat lunak dan memeriksa apakah aplikasi tersebut belum diubah atau rusak sejak file tersebut diterbitkan.

Untuk memverifikasi tarball

Gunakan utilitas md5sum untuk MD5 checksum, atau utilitas sha256sum untuk checksum, dan tentukan nama file SHA256 tarball. Anda harus menjalankan perintah dari direktori tempat Anda menyimpan file tarball.

- MD5

```
$  md5sum tarball_filename.tar.gz
```

- SHA256

```
$  sha256sum tarball_filename.tar.gz
```

Perintah tersebut harus mengembalikan nilai checksum dalam format berikut.

```
checksum_value tarball_filename.tar.gz
```

Bandingkan nilai checksum yang dikembalikan oleh perintah dengan nilai checksum yang diberikan dalam tabel di bawah ini. Jika checksum cocok, skrip penginstalan dapat dijalankan dengan aman. Jika checksum tidak cocok, jangan jalankan skrip instalasi, dan hubungi Dukungan.

Misalnya, perintah berikut memverifikasi tarball EFA 1.9.4 menggunakan checksum. SHA256

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

Contoh output:

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

Tabel berikut mencantumkan checksum untuk versi EFA terbaru.

Versi	Checksum
EFA 1.47.0	MD5: c81d4caf24dabc04a6e4818590620f5f SHA256: 2df4201e046833c7dc8160907bee7f52b76ff80ed147376a2d0ed8a0dd66b2db
EFA 1.46.0	MD5: a88bbd9b71624d7ca401b54bc2fc0c19 SHA256: 8302bd7849afb95c903a875d7dcb6f85b3d7629e9a8b67d020031cfc6f4d0ee1
EFA 1.45.1	MD5: 91c3c87e16bbcaca1513252c38b771bb SHA256: 9aeb20c645135b6039cc08986d8f14e63280f7839e882a74df5e83627ffeaa17
EFA 1.45.0	MD5: 800aeddfa9d9c5f139a7b8f7c4fec627 SHA256: 25ba26a0877fe3317390dc126aad2f23e27fc461cf0b940004f032cb342fa539
EFA 1.44.0	MD5: d024f6bebe080db42745103b84ca7c43 SHA256: f129a5b44a49d593d247e55a59eb9bcb57121566e1c2e42b832a4e794fa83d8a
EFA 1.43.3	MD5: 4dbc6eeecc516760253c10cbedb6319d

Versi	Checksum
	SHA256: 6c470ebce254c71653 47b5048895ac2996c8856727164 2297f4c597738300652
EFA 1.43.2	MD5: 7287b25a07c9747c0d4001e8fc5 f59b2 SHA256: de15c5bdbc83b952af bde876110830c604ad0796680e5 157c05f7c1979a41069
EFA 1.43.1	MD5: 7cfafc8debaea51dd4966fa0b2b ba673 SHA256: 54211eda0c193138ee8ed09b5fb 41c41fc76fe0a77935fa4ec8d989466342740
EFA 1.43.0	MD5: f2b3dd7dc8670b541f7c23fd58e 5e503 SHA256: 786df3458c499237be 33bb8e50ffd4da7c18c20e25438 0ffc80fb90833d8cc73
EFA 1.42.0	MD5: 94b2b1db09da1dde08ec049db1f 24370 SHA256: 4114fe612905ee0508 3ae5cb391a00a012510f3abfecc 642d86c9a5ae4be9008
EFA 1.41.0	MD5: 086181c3ee3f8da512fc6e1c795 e8936 SHA256: 3506354cdfbe31ff55 2fe75f5d0d9bb7efd29cf79bd99 457347d29c751c38f9f

Versi	Checksum
EFA 1.40.0	MD5: f3ec6f73fbeaccba082327507581157c SHA256: 30491b0fe7c3470d4439594538855c981b05fa69862d74f8c05eb9b97912368a
EFA 1.39.0	MD5: c223d5954a85a7fbcd248c942b866e43 SHA256: 2cbc028c03064633bb990782b47c36156637769e2f48704417a9c700a7a32101
EFA 1.38.1	MD5: f112569e828ab65187777f794bab542c SHA256: 83923374afd388b1cfcf4b3a21a2b1ba7cf46a01a587f7b519b8386cb95e4f81
EFA 1.38.0	MD5: 43a2a446b33a2506f40853d55059f1ea SHA256: 4f436954f35ad53754b4d005fd8d0be63de3b4184de41a695b504bdce0fecb22
EFA 1.37.0	MD5: 6328070192bae920eca45797ad4c1db1 SHA256: 2584fc3c8bb99f29b3285e275747ff09d67c18e162c2a652e36c976b72154bfb

Versi	Checksum
EFA 1.36.0	MD5: 1bec83180fbffb23452ab6469ca21dfa SHA256: de183f333cfb58aeb7908a67bf9106985ba3ccb7f8638b851d2a0d8dbfacaec4
EFA 1.35.0	MD5: 252f03c978dca5f8e8d9f34e488b256e SHA256: 432b6ad4368ba0cd8b902729d14a908a97be7a3dcc5239422ea994a47f35a5e1
EFA 1.34.0	MD5: 5cd4b28d27a31677c16139b54c9acb45 SHA256: bd68839e741b0afd3ec2e37d50603803cfa7a279c120f0a736cc57c2ff2d7fdc
EFA 1.33.0	MD5: e2f61fccbcaa11e2ccfddd3660522276 SHA256: 0372877b87c6a7337bb7791d255e1053b907d030489fb2c3732ba70069185fce
EFA 1.32.0	MD5: db8d65cc028d8d08b5a9f2d88881c1b1 SHA256: 5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66

Versi	Checksum
EFA 1.31.0	MD5: 856352f12bef2ccbadcd75e35aa52aaf SHA256: 943325bd37902a4300ac9e5715163537d56ecb4e7b87b37827c3e547aa1897bf
EFA 1.30.0	MD5: 31f48e1a47fe93ede8ebd273fb747358 SHA256: 876ab9403e07a0c3c91a1a34685a52eced890ae052df94857f6081c5f6c78a0a
EFA 1.29.1	MD5: e1872ca815d752c1d7c2b5c175e52a16 SHA256: 178b263b8c25845b63dc93b25bcdff5870df5204ec509af26f43e8d283488744
EFA 1.29.0	MD5: 39d06a002154d94cd982ed348133f385 SHA256: 836655f87015547e733e7d9f7c760e4e24697f8bbc261bb5f3560abd4206bc36
EFA 1.28.0	MD5: 9dc13b7446665822605e66febe074035 SHA256: 2e625d2d6d3e073b5178e8e861891273d896b66d03cb1a32244fd56789f1c435

Versi	Checksum
EFA 1.27.0	MD5: 98bfb515ea3e8d93f554020f3837fa15 SHA256: 1d49a97b0bf8d964d91652a79ac851f2550e33a5bf9d0cf86ec9357ff6579aa3
EFA 1.26.1	MD5: 884e74671fdef4725501f7cd2d451d0c SHA256: c616994c924f54ebfabfab32b7fe8ac56947fae00a0ff453d975e298d174fc96
EFA 1.26.0	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11
EFA 1.25.1	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06
EFA 1.25.0	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342

Versi	Checksum
EFA 1.24.1	MD5: 211b249f39d53086f3cb0c07665f4e6f SHA256: 120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62
EFA 1.24.0	MD5: 7afe0187951e2dd2c9cc4b572e62f924 SHA256: 878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e
EFA 1.23.1	MD5: 22491e114b6ee7160a8290145dca0c28 SHA256: 5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797
EFA 1.23.0	MD5: 38a6d7c1861f5038dba4e441ca7683ca SHA256: 555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd
EFA 1.22.1	MD5: 600c0ad7cdbc06e8e846cb763f92901b SHA256: f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665

Versi	Checksum
EFA 1.22.0	MD5: 8f100c93dc8ab519c2aeb5dab89e98f8 SHA256: f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a
EFA 1.21.0	MD5: 959ccc3a4347461909ec02ed3ba7c372 SHA256: c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050
EFA 1.20.0	MD5: 7ebfbb8e85f1b94709df4ab3db47913b SHA256: aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0
EFA 1.19.0	MD5: 2fd45324953347ec5518da7e3fefa0ec SHA256: 99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709
EFA 1.18.0	MD5: fc2571a72f5d3c7b7b576ce2de38d91e SHA256: acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6

Versi	Checksum
EFA 1.17.3	MD5: `0517df4a190356ab559235147174cafd` SHA256: `5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca`
EFA 1.17.2	MD5: `a329dedab53c4832df218a24449f4c9a` SHA256: `bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099`
EFA 1.17.1	MD5: `733ae2cfc9d14b52017eaf0a2ab6b0ff` SHA256: `f29322640a88ae9279805993cb836276ea240623820848463ca686c8ce02136f`
EFA 1.17.0	MD5: `d430fc841563c11c3805c5f82a4746b1` SHA256: `75ab0cee4fb6bd38889dce313183f5d3a83bd233e0a6ef6205d8352821ea901d`
EFA 1.16.0	MD5: `399548d3b0d2e812d74dd67937b696b4` SHA256: `cecec36495a1bc6fdc82f97761a541e4fb6c9a3cbf3cfcb145acf25ea5dbd45b`

Versi	Checksum
EFA 1.15.2	MD5: 955fea580d5170b05823d51acde7ca21 SHA256: 84df4fbc1b3741b6c073176287789a601a589313accc8e6653434e8d4c20bd49
EFA 1.15.1	MD5: c4610267039f72bbe4e35d7bf53519bc SHA256: be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7
EFA 1.15.0	MD5: 9861694e1cc00d884fadac07d22898be SHA256: b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f
EFA 1.14.1	MD5: 50ba56397d359e57872fde1f74d4168a SHA256: c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7
EFA 1.14.0	MD5: 40805e7fd842c36ececb9fd7f921b1ae SHA256: 662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97

Versi	Checksum
EFA 1.13.0	MD5: c91d16556f4fd53becadbb345828221e SHA256: ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1
EFA 1.12.3	MD5: 818aee81f097918cfaebd724eddea678 SHA256: 2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172
EFA 1.12.2	MD5: 956bb1fc5ae0d6f0f87d2e481d49fccf SHA256: 083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259
EFA 1.12.1	MD5: f5bfe52779df435188b0a2874d0633ea SHA256: 5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900
EFA 1.12.0	MD5: d6c6b49fafb39b770297e1cc44fe68a6 SHA256: 28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59

Versi	Checksum
EFA 1.11.2	MD5: 2376cf18d1353a4551e35c33d269c404 SHA256: a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371
EFA 1.11.1	MD5: 026b0d9a0a48780cc7406bd51997b1c0 SHA256: 6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a
EFA 1.11.0	MD5: 7d9058e010ad65bf2e14259214a36949 SHA256: 7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa
EFA 1.10.1	MD5: 78521d3d668be22976f46c6fecc7b730 SHA256: 61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4
EFA 1.10.0	MD5: 46f73f5a7afe41b4bb918c81888fefa9 SHA256: 136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282

Versi	Checksum
EFA 1.9.5	MD5: `95edb8a209c18ba8d250409846eb6ef4` SHA256: `a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25`
EFA 1.9.4	MD5: `f26dd5c350422c1a985e35947fa5aa28` SHA256: `1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14`
EFA 1.9.3	MD5: `95755765a097802d3e6d5018d1a5d3d6` SHA256: `46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1`
EFA 1.8.4	MD5: `85d594c41e831afc6c9305263140457e` SHA256: `0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45`

Catatan rilis Adaptor Kain Elastis

Tabel berikut menjelaskan riwayat versi dan changelog untuk perangkat lunak Adaptor Kain Elastis.

Versi	Perubahan	Tanggal rilis
1.47.0	• Tingkatkan ke libfabric 2.4.0amzn1.0	Januari 29, 2026

Versi	Perubahan	Tanggal rilis
	• Manajemen refactor rekan: pindahkan titik akhir → peer hashmap ke level AV • Tambahkan penghitung pembuatan entri paket untuk mencegah masalah ABA • Terapkan pemblokiran dukungan baca CQ (fi_cq_sread) dengan objek tunggu • Perbaiki double-free dalam pemrosesan paket eager/mul req/longread RTM • Perbaiki bendera akses IBV pendaftaran MR berdasarkan kemampuan RDMA perangkat • Nonaktifkan FI_OPT_EFA_SENDRECV_IN_ORDE R_ALIGNED_128_BYTES (mengembalikan -FI_EOPNO TSUPP) • Optimalkan entri paket agar sesuai dengan dua baris cache x86 (128 byte) • Selalu berhasil efa_rdm_srx_start dan geser jendela recv pada kesalahan RTM/RTA • Putuskan tautan entri paket RX sebelum dirilis selama pembersihan titik akhir • Tingkatkan ke libnccl-ofi 1.18.0 • Dukungan P6-B300: menambahkan keputusan tuner khusus untuk P6-B300 • Peningkatan kinerja PAT pada P6-B200 dengan mengurang i jumlah saluran untuk ukuran pesan yang lebih kecil •	

Versi	Perubahan	Tanggal rilis
	Default protokol yang diubah, default ke protokol RDMA pada Trn1 dan default ke protokol SENDRECV pada g7e.8xlarge • Pemilihan platform dinamis: menambahkan fitur untuk mengaktifkan AWS pengoptimalan saat runtime berdasarkan keberadaan. AWS NICs Ini memungkinkan biner plugin tunggal untuk digunakan untuk keduanya AWS dan AWS non-platform. AWS pengoptimalan masih dapat dinonaktifkan pada waktu kompilasi. • Dukungan tetap untuk penyedia non-FI_MR_VIRT_ADDR dalam protokol RDMA • Peningkatan kecepatan PCIe tautan NIC dan pelaporan lebar ke NCCL • Model threading yang didesain ulang untuk mendukung aplikasi multi-threaded tanpa memerlukan domain Libfabric terpisah untuk setiap thread. • Dukungan tetap untuk penyedia FI_MR_ENDPOINT (hanya mendukung protokol SENDRECV) dengan membersihkan sumber daya dalam urutan yang benar • Tingkatkan ke rdma-core 61.0 • Gunakan CQ berulir tunggal jika Domain Thread disediakan • Verifikasi nomor QP pada proses CQE • Tingkatkan ke driver efa 3.0.0 • Tingkatkan penanganan kesalahan admin • Periksa kebenaran nomor QP pada jajak pendapat penyelesaian	

Versi	Perubahan	Tanggal rilis
	• Hapus backport tanpa syarat dari temuan ukuran halaman terbaik • Cetak string errno untuk pointer kesalahan • Sederhanakan kode dalam alur pembuatan CQ • Backport perubahan hulu di CQ dengan aliran pembuatan umem • Sesuaikan konfigurasi DKMS untuk versi DKMS baru • Tingkatkan ke Buka MPI 5.0.9amzn1 • Bugfix: Atur tingkat threading domain berdasarkan dukungan utas MPI • Bugfix: Minta flag FI_COMPLETION untuk memastikan penyelesaian dibuat untuk semua peristiwa transfer data • Bagikan domain antara BTL dan MTL untuk mengurangi jumlah total domain yang dibuat untuk memperbaiki kehabisan sumber daya pada sistem dengan jumlah inti yang tinggi	

Versi	Perubahan	Tanggal rilis

1.46.0	• Tambahkan Support untuk Debian 13
	• Tingkatkan ke efa-nv-peermem 1.2.3
	  • Perbaiki kesalahan dan peringatan build dengan kernel dan DKMS baru
	• Tingkatkan ke libfabric 2.3.1amzn4.0
	  • Aktifkan jalur data langsung untuk jalur protokol efa-rdm
	  • Aktifkan ROCr dukungan HMEM
	  • Opsi FI_OPT_EFA_USE_UNSOLICITED_WRITE_RECV baru untuk menonaktifkan recv tulis yang tidak diminta
	  • Optimalkan waktu pembuatan koneksi
	• Tambahkan libnccl-ofi di RHEL 9, Rocky Linux 9, dan Debian 13
		Desember 12, 2025

1.45.1	• Tingkatkan ke libfabric 2.3.1amzn3.0 • Perbaiki bug yang memotong cq_data menjadi 2 byte sementara penyedia mengiklankan dukungan untuk 4 byte	November 26, 2025

Versi	Perubahan	Tanggal rilis

1.45.0	• Tingkatkan ke rdma-core 60.amzn0
	  • Perluas kueri DV CQ untuk mengembalikan bel pintu
	• Tingkatkan ke libfabric 2.3.1amzn2.0
	  • Mendukung mode FI_RX_CQ_DATA untuk efa-direct
	  • Optimalkan posting WQE di jalur langsung jalur data
	  • Perbaiki kondisi balapan dalam kemajuan cntr
	  • Tingkatkan pencatatan untuk pesan peringatan
	  • Menangani penyelesaian RMA dengan benar untuk rekan yang dihapus
	  • Mengusir entri AH dari AV implisit ketika batas AH tercapai
	• Tingkatkan ke libnccl-ofi 1.17.2
	  • Memperbaiki kerusakan dengan NCCL v2.28.x saat inisialis asi Libfabric gagal
	  • Menambahkan dukungan untuk keluarga instance g7e
	  • Memperbaiki masalah di mana NCCL dapat secara keliru mencoba menggunakan jalur GPUDirect RDMA pada platform yang mendukung DMA-BUF
	  • Memperbaiki masalah pemesanan shutdown NICs yang memerlukan pendaftaran memori per titik akhir (Cray Slingshot)
		November 17, 2025

Versi	Perubahan	Tanggal rilis

1.44.0	• Tingkatkan ke rdma-core 59.amzn0
	  • Tambahkan dukungan untuk mengikat QPs dan CQs ke thread domain
	  • Tambahkan dukungan untuk mengalokasikan domain induk
	  • Tambahkan dukungan untuk mengalokasikan domain thread
	  • Tambahkan kueri kata kerja langsung QP dan CQ
	  • Tambahkan opsi untuk membuat CQ dengan memori eksternal`
	  • Perbaiki jajak pendapat CQ setelah QP menghancurkan
	• Tingkatkan ke libfabric 2.3.1amzn1.0
	• Tingkatkan ke Buka MPI 5.0.8amzn1
	  • Peningkatan fungsionalitas
	  • Perbaikan bug
	• Tingkatkan ke libnccl-ofi 1.17.1
	  • Mendukung NCCL v2.28.3-1 sambil mempertahankan kompatibilitas mundur dengan NCCL v2.17.1 dan yang lebih baru.
	  • Membangun dengan platform-aws membutuhkan Libfabric v1.22.0amzn4.0 atau lebih tinggi. Diuji dengan versi hingga Libfabric v2.3.1amzn1.0.
	  •
		Oktober 29, 2025

Versi	Perubahan	Tanggal rilis
	Perbaikan untuk mendukung kompatibilitas di seluruh CUDA12 dan CUDA13.	
1.43.3	• Tingkatkan ke driver efa 2.17.3 • Support P2P dengan driver NVIDIA 580 • Sesuaikan pendaftaran MR untuk 6.17 dan pada kernel	Oktober 01, 2025
1.43.2	• Tingkatkan ke libnccl-ofi 1.16.3 • Mendukung NCCL v2.27.7-1 sambil mempertahankan kompatibilitas mundur dengan NCCL v2.17.1 dan yang lebih baru. • Membangun dengan platform-aws membutuhkan Libfabric v1.22.0amzn4.0 atau lebih tinggi. Diuji dengan versi hingga Libfabric 2.1.0amzn5.0. • Aktifkan secara domain-per-thread default pada semua jenis instans Amazon EC2 untuk meningkatkan kinerja untuk beberapa aplikasi di mana NCCL membuat beberapa utas proxy	Agustus 15, 2025

Versi	Perubahan	Tanggal rilis

1.43.1	• Tingkatkan ke libnccl-ofi 1.16.2
	  • Mendukung NCCL v2.27.6-1 sambil mempertahankan kompatibilitas mundur dengan NCCL v2.17.1 dan yang lebih baru.
	  • Membangun dengan platform-aws membutuhkan Libfabric v1.22.0amzn4.0 atau lebih tinggi. Diuji dengan versi hingga Libfabric 2.1.0amzn4.0.
	  • Menambahkan konfigurasi platform baru untuk mendukung penggunaan plugin OFI NCCL pada jenis instans Amazon EC2 p5.4xlarge
	• Tingkatkan ke libfabric 2.1.0amzn5.0
		Juli 31, 2025

Versi	Perubahan	Tanggal rilis

1.43.0	• Tingkatkan ke libnccl-ofi 1.16.1
	  • Mendukung NCCL v2.27.6-1 sambil mempertahankan kompatibilitas mundur dengan NCCL v2.17.1 dan yang lebih baru.
	  • Membangun dengan platform-aws membutuhkan Libfabric v1.22.0amzn4.0 atau lebih tinggi. Diuji dengan versi hingga Libfabric 2.1.0amzn3.
	  • Perbarui format kecepatan tautan PCI yang dilaporkan dalam file topologi agar sesuai dengan kernel 5.7+
	  • Menambahkan SKIP_NICS_WITHOUT_ACCEL_AT_SAME_PCI_LEVEL untuk melewati libfabric nics yang tidak memiliki akselerator pada level pci yang sama
	• Tingkatkan ke driver efa 2.17.2
	• Tingkatkan ke efa-nv-peermem 1.2.2
	• Tingkatkan ke libfabric 2.1.0amzn4.0
	• Tingkatkan ke rdma-core 58.amzn0
	  • Perbaiki indeks permintaan kerja penggunaan ganda
	  • Tambahkan panjang WQE ke post_send tracepoint
	• Aktifkan pengoptimalan untuk platform Graviton
	• Menolak dukungan untuk Ubuntu 20.04
		Juli 25, 2025

Versi	Perubahan	Tanggal rilis

1.42.0	• Tingkatkan ke driver efa 2.15.3
	• Tingkatkan ke efa-nv-peermem 1.2.1
	• Tingkatkan ke rdma-core 57.amzn1
	  • Perbaiki indeks permintaan kerja penggunaan ganda
	• Tingkatkan ke libfabric 2.1.0amzn3.0
	• Tingkatkan ke libnccl-ofi 1.15.0
	  • Mendukung NCCL 2.26.6-1 sambil mempertahankan kompatibilitas mundur dengan (NCCL v2.17.1 dan yang lebih baru.
	  • Membangun dengan platform-aws membutuhkan Libfabric v1.22.0amzn4.0 atau lebih tinggi. Diuji dengan versi hingga Libfabric 2.1.0amzn3.
	  • Membangun sistem dan dukungan platform
	  • Menambahkan dukungan platform Amazon EC2 P6-B200
	  • Mengubah nama pustaka plugin default menjadi libnccl-net-ofi .so, dan secara default buat symlink libnccl-net-ofi dari.so ke libnccl-net.so untuk mempertah ankan kompatibilitas mundur. Hal ini memungkinkan pengguna untuk mengatur NCCL_NET_PLUGIN=OFI untuk memaksa NCCL menggunakan plugin OFI untuk komunikasi. Menentukan -- disable-nccl-net-symlink untuk mengkonfigurasi akan melewati symlink, memungkinkan beberapa plugin dipasang di wadah yang sama.
	  • Penyetelan dan peningkatan kinerja
	  • Menambahkan dukungan tuner pada P6-B200 untuk AllReduce, AllGather, dan ReduceScatter wilayah untuk 0x0 dan 0x7 bitmask
		Juni 6, 2025

Versi	Perubahan	Tanggal rilis
	• Latensi default yang diperbarui untuk platform P5en dan P6-B200 berdasarkan hasil dan analisis empiris • Update untuk menggunakan NCCL v10 API dengan dukungan parameter TrafficClass untuk prioritas lalu lintas future • Basis kode plugin yang dimigrasi dari C ke C ++ • Menambahkan dukungan untuk pekerjaan di mana jumlah NICs per GPU berbeda di seluruh sistem. Lihat dokumenta si variabel lingkungan runtime OFI_NCCL_FORCE_NUM _RAILS untuk informasi selengkapnya.	
1.41.0	• Tingkatkan ke rdma-core 57.amzn0	16 Mei 2025
1.40.0	• Tingkatkan ke libfabric 2.1.0amzn2.0 • Tingkatkan ke rdma-core 56.0 • Tingkatkan ke efa-config 1.18. • Menolak dukungan untuk Debian 10 • Tingkatkan ke libnccl-ofi 1.14.2 • Aktifkan dukungan CUDA di Libfabric di ARM untuk Ubuntu dan Amazon Linux 2023 • Tambahkan libnccl-ofi di ARM untuk Ubuntu dan Amazon Linux 2023	2 Mei 2025
1.39.0	• Tingkatkan ke libfabric 2.1.0 • Upgrade ke Open MPI 5.0.6 • Tingkatkan ke libnccl-ofi 1.14.1 • Tingkatkan ke driver efa 2.15.0	April 16, 2025
1.38.1	• Perbarui ke `Libfabric 1.22.0amzn5.0`	Maret 3, 2025
1.38.0	• Tambahkan `libnccl-ofi 1.13.2-1`	Januari 8, 2025

Versi	Perubahan	Tanggal rilis
1.37.0	• Tingkatkan ke `libfabric 1.22.0amzn4.0` • Tingkatkan ke `rdma-core 54.amzn0`	November 18, 2024
1.36.0	• Tambahkan dukungan untuk Debian 12 • Distribusikan `efa_test.sh` sebagai skrip utilitas di `/opt/amazon/efa/bin` • Tingkatkan ke driver efa 2.13.0 • Tingkatkan ke `libfabric 1.22.0amzn3.0` • Tingkatkan ke `rdma-core 54.0` • Tingkatkan ke open mpi 4.1.7	November 7, 2024
1.35.0	• Upgrade ke Open MPI 5.0.5 • Tingkatkan ke PRRTE 3.0.6 dan ganti nama paket RPM menjadi prrte-aws • Ganti nama paket Open PMIx RPM menjadi pmix-aws • Konfigurasikan opsi build untuk build dpkg dan RPM • Tingkatkan ke `Libfabric 1.22.0amzn2.0` • Tingkatkan ke driver efa 2.12.1	Oktober 14, 2024
1.34.0	• Jatuhkan dukungan untuk CentOS 7 dan RHEL 7 • Tertelan `Libfabric 1.22.0amzn1.0` • Perbarui paket efa-config ke 1,17	Agustus 6, 2024

Versi	Perubahan	Tanggal rilis
1.33.0	• Tingkatkan ke driver efa 2.10.0 • Tingkatkan ke `rdma-core 52.0` • Tingkatkan ke PRRTE 3.0.5 • Upgrade ke Open MPI 5.0.3 • Tambahkan dukungan untuk Ubuntu 24.04 LTS • Hapus dokumentasi OpenPMIx, PRRTE dan Open MPI HTML. Pengguna harus merujuk ke situs web resmi. • Jatuhkan dukungan untuk openSUSE 15.4 atau yang lebih lama	Juni 20, 2024
1.32.0	• Tingkatkan ke driver efa 2.8.0 • Tingkatkan ke efa-nv-peermem driver 1.1.1 • Tingkatkan paket efa-config ke 1,16 • Tingkatkan paket efa-profile ke 1.7 • Tingkatkan ke `rdma-core 50.0` • Tingkatkan ke `libfabric 1.21.0amzn1.0` • Tingkatkan `efa_test.sh` dengan pemilihan `fi_pingpong` port • Instal rdma-core yang lebih baru dari sistem bila diperlukan	April 18, 2024
1.31.0	• Upgrade ke Open PMIx 4.2.8 • Tingkatkan ke PRRTE 3.0.3 • Tingkatkan ke Open MPI 5.0.2, dan konversi komponen MCA ke DSO. • Tingkatkan ke `Libfabric 1.20.1amzn1.0`	7 Maret 2024

Versi	Perubahan	Tanggal rilis
1.30.0	• Sertakan Open PMIx 4.2.7, diinstal secara default `/opt/amazon/pmix` • Sertakan PRRTE 3.0.2, diinstal secara default `/opt/amazon/prrte` • Sertakan Open MPI 5.0.0, diinstal secara default `/opt/amazon/openmpi5` • Perbarui efa-profile ke 1.6	Desember 2023
1.29.1	• Tertelan `libfabric 1.19.0amzn4.0`	Desember 2023
1.29.0	• Menelan driver kernel efa 2.6.0 • Tertelan `libfabric 1.19.0amzn3.0`	November 2023
1.28.0	• Upgrade Open MPI ke 4.1.6 • Tertelan `libfabric 1.19.0amzn2.0`	Oktober 2023
1.27.0	• Tambahkan `Libfabric 1.19.0amzn1.0` ke installer • Aktifkan atom bawaan GCC untuk Open MPI 4	September 2023
1.26.1	• `efa_test.sh` : perbaiki bug coba lagi yang tak terbatas	September 2023
1.26.0	• Tambahkan dukungan untuk RHEL 9 • Perbaiki debug build pada beberapa distribusi • Tertelan `libfabric 1.18.2amzn1.0` • `efa_test.sh` : Tambahkan coba lagi untuk `fi_pingpong`	September 2023
1.25.1	• Tertelan `libfabric 1.18.1amzn1.0` • Perbarui batas waktu dalam skrip penginstal EFA	September 2023
1.25.0	• Tambahkan dukungan untuk Amazon Linux 2023 • Perbaikan bug dalam uji pasca-instalasi	Juli 2023

Versi	Perubahan	Tanggal rilis
1.24.1	• Tingkatkan libfabric ke 1.18.1 • Tingkatkan driver efa ke 2.5.0	Juli 2023
1.24.0	• Tertelan `rdma-core 46.0` • Mengkonsumsi driver efa 2.4.1 • Support Debian 11	Juni 2023
1.23.1	• Tertelan `libfabric 1.18.0amzn2.0`	Juni 2023
1.23.0	• Tambahkan dukungan untuk Debian 10 • Jatuhkan dukungan untuk Ubuntu 18.04 LTS • Tingkatkan paket efa-config ke 1,14 • Tertelan `libfabric 1.18.0amzn1.0`	Mei 2023
1.22.1	• Tingkatkan libfabric ke 1.17.1	Maret 2023
1.22.0	• Upgrade Open MPI ke 4.1.5 • Tingkatkan libfabric ke 1.17.0 • Tingkatkan paket efa-config ke 1,13	Februari 2023
1.21.0	• Tambahkan dukungan untuk Rocky Linux 9 OS • Mengkonsumsi driver efa 2.1.1 • Tertelan `libfabric 1.16.1amzn3.0` • Tingkatkan paket efa-config ke 1.12	Desember 2022
1.20.0	• Tambahkan dukungan untuk Rocky Linux 8 OS. • Menelan driver efa 2.1.0. • Menelan`rdma-core 43.0`. • Tertelan `libfabric 1.16.1amzn1.0`	November 2022
1.19.0	• Tertelan `libfabric 1.16.0` • Bangun MPI Terbuka dengan `--enable-orterun-prefix-by-default`	Oktober 2022

Versi	Perubahan	Tanggal rilis
1.18.0	• Tambahkan dukungan untuk Ubuntu22.04	Agustus 2022
1.17.3	• Perbarui libfabric ke`1.16.0~amzn4.0` . Ini ~ menunjukkan itu adalah versi pra-rilis libfabric 1.16.0. • Perpanjang batas waktu uji pingpong pasca-instalasi hingga 20 detik	Agustus 2022
1.17.2	• Perbarui libfabric ke`1.16.0~amzn3.0` . Ini ~ menunjukkan itu adalah versi pra-rilis libfabric 1.16.0.	Juli 2022
1.17.1	• Perbarui libfabric ke`1.16.0~amzn2.0` . Ini ~ menunjukkan itu adalah versi pra-rilis libfabric 1.16.0. • Nonaktifkan penyedia net eksperimental saat membangun libfabric	Juli 2022
1.17.0	• Perbarui `rdma-core` ke v41.0 • Perbarui Buka MPI ke 4.1.4 • Perbarui libfabric ke`1.16.0~amzn1.0` . Ini ~ menunjukkan itu adalah versi pra-rilis libfabric 1.16.0.	Juli 2022
1.16.0	• Perbarui libfabric ke`1.15.1amzn1.0` , berisi perubahan nama perpustakaan neuron • Tingkatkan efa-config ke 1.10 • Kecualikan penyedia opx dan rxd di libfabric build	Juni 2022
1.15.2	• Perbarui libfabric ke 1.14.1	Mei 2022
1.15.1	• Perbarui libfabric ke `1.14.0amzn1.0`	Maret 2022

Versi	Perubahan	Tanggal rilis
1.15.0	• Perbaiki bug yang menyebabkan instalasi gagal pada Open SuSE 15.3 • Jatuhkan dukungan Open SuSE 15.2 (karena Open SuSE 15.2 mencapai akhir masa pakai) • Drop Support dari CentOS 8 (saat CentOS 8 mencapai akhir hayat) • Perbarui libfabric ke 1.14.0 • Perbarui driver kernel efa ke 1.16.0 • Perbarui `rdma-core` ke v39.0 • Perbarui Buka MPI ke versi 4.1.2.	Februari 2022
1.14.1	• Perbarui libfabric ke`1.13.2amzn1.0` .	Oktober 2021
1.14.0	• Menelan driver kernel efa 1.14.2. • Jadikan `-g, --enable-gdr efa_installer.sh` sebagai opsi tanpa operasi karena driver kernel efa terbaru mengaktifkan dukungan GDR secara default. • Menelan`rdma-core v37.0`. • Menelan`libfabric 1.13.2`. • Tambahkan daftar paket dan bandingkan RPM/DEB dengan daftar selama instalasi untuk mencegah instalasi paket yang tidak dikenal. • Tambahkan tidur di skrip penginstal untuk menunggu aturan udev diterapkan setelah driver EFA memuat ulang.	Oktober 2021
1.13.0	• Perbarui `rdma-core` ke v35.0. • Perbarui `libfabric` ke v1.13.0amzn1.0. • Tambahkan dukungan EFA untuk CentOS/RHEL 8 pada platform Gravition2. • Tambahkan logika perbandingan versi dalam skrip penginstal untuk melewati instalasi paket lokal ketika ada satu yang diinstal di sistem dengan versi yang lebih tinggi.	Agustus 2021

Versi	Perubahan	Tanggal rilis
1.12.3	• Perbarui modul kernel EFA ke 1.13.0. • Perbarui paket efa-config ke versi 1.9. Tingkatkan perhitungan reservasi halaman besar untuk menangani ukuran halaman besar default yang besar.	Juli 2021
1.12.2	• Perbarui modul kernel EFA ke 1.12.3. • Bangun paket debian MPI Terbuka dengan `--with-libevent=external` dan. `--with-hwloc=external` • Bump Open MPI rpm build ID ke 2 untuk memperbaiki masalah kompatibilitas mundur HWLOC pada CentOS 8. • Hapus instalasi paket kernel-devel dan kernel-source pada dan openSUSE 15.2. SLES15 SP2	Juni 2021
1.12.1	• Perbarui Libfabric ke versi 1.11.2amzon1.1. • Perbarui modul kernel EFA ke versi 1.12.1.	Mei 2021
1.12.0	• Perbarui Buka MPI ke versi 4.1.1. • Perbarui Libfabric ke versi 1.11.2amzn1.0. • Bangun rdma-core untuk Amazon Linux 2 menggunakan konfigurasi kemasan yang sama dengan rdma-core. AL2 • Jangan memaksakan `-Wl,--enable-new-dtags` saat membangun MPI RPMs Terbuka. • Bangun MPI Terbuka dengan pustaka sistem untuk hwloc dan libevent. • Perbarui modul kernel EFA ke versi 1.12.0 • Perbarui paket efa-config ke versi 1.8. Tingkatkan perhitungan reservasi halaman besar untuk contoh berumur panjang. • Perbarui paket efa-profile ke versi 1.5. Hapus file tuning kolektif mpi terbuka yang berfungsi sebagai solusi untuk memperbaiki Open MPI 4.1.0 hang pada P4d. • Perbarui `rdma-core` ke v32.1. • Jatuhkan dukungan untuk Amazon Linux 1 dan Ubuntu 16.04.	Mei 2021

Versi	Perubahan	Tanggal rilis
1.11.2	• Perbaiki Open MPI hang saat menggunakan Open MPI pada P4d dengan mengubah algoritma default yang digunakan untuk mengimplementasikan MPI_BARRIER melalui file konfigurasi. • Nonaktifkan penggunaan atom bawaan di Open MPI di ARM via `--disable-builtin-atomics` untuk mengatasi masalah kompiler.	Februari 2021
1.11.1	• Perbarui Buka MPI ke versi 4.1.0. • Perbarui paket efa-config ke versi 1.7. Tingkatkan perhitungan jumlah reservasi halaman yang besar. • Perbarui paket efa-profile ke versi 1.3. Menghapus file keputusan kolektif yang tidak dibutuhkan sekarang setelah Open MPI 4.1.0 digunakan.	Desember 2020
1.11.0	• Tambahkan dukungan untuk platform Gravition2. • Perbarui `rdma-core` ke versi 31.2amzn. • Perbarui Libfabric ke versi 1.11.1amzn1.0. • Perbarui efa-config ke versi 1.6. • Perbarui efa-profile ke versi 1.2.	Desember 2020
1.10.1	• Tambahkan dukungan untuk CentOs/RHEL 8. • Tambahkan dukungan untuk Ubuntu 20.04. • Tambahkan dukungan untuk SUSE Linux Enterprise 15.	November 2020

Versi	Perubahan	Tanggal rilis
1.10.0	• Tambahkan dukungan GPUDirect RDMA untuk platform P4d. Gunakan opsi `--enable-gdr` penginstal untuk menginstal modul kernel dan ruang pengguna yang sadar GDR. • Perbarui modul kernel EFA ke versi 1.10.2. • Perbarui `rdma-core` ke versi 31.amzn0. • Perbarui Libfabric ke versi 1.11.1. • Perbarui Buka MPI ke versi 4.0.5. • Perbarui efa-config ke versi 1.5. • Perbarui efa-profile ke versi 1.1. Termasuk file keputusan kolektif Open MPI yang ditingkatkan.	Oktober 2020
1.9.5	• Perbarui efa-config ke versi 1.4. Memperbaiki bug dalam file keputusan kolektif MPI Terbuka.	September 2020
1.9.4	• Perbarui Buka MPI ke versi 4.0.3. • Perbarui Libfabric ke versi 1.10.1amazon1.1. • Perbarui `rdma-core` ke versi 28.amzn0.	Juli 2020
1.9.3	• Perbarui modul kernel EFA ke versi 1.6.0. • Perbarui `rdma-core` ke versi 28.amzn0. • Perbarui Libfabric ke versi 1.10.1amzn1.1. • Perbarui efa-config ke versi 1.3. Menambahkan file tuning kolektif untuk Open MPI. • Lewati instalasi dkms jika sudah diinstal. • Perbaiki mode `--skip-kmod` instalasi agar benar-benar berfungsi.	Juni 2020
1.8.4	• Pindahkan file konfigurasi ke dalam paket efa-config dan efa-profile sehingga mereka dilacak oleh manajer paket sistem operasi. • Perbarui Buka MPI ke versi 4.0.3.	April 2020

Versi	Perubahan	Tanggal rilis
1.8.3	• Perbarui modul kernel EFA ke versi 1.5.1. • DKMS terdistribusi pada beberapa platform daripada mengandalkan repositori EPEL untuk menambah keandalan instalasi. • Pada RHEL 7, instal yang RPMs dibangun di CentOS 7 RPMs alih-alih dibangun di Amazon Linux 2.	Februari 2020
1.8.2	• Kembalikan `rdma-core` ke versi 25 karena ketidakcocokan dalam penamaan perangkat antara modul kernel dan. `rdma-core`	Januari 2020
1.8.1	• Perbarui Libfabric ke versi 1.9.0amzn1.1.	Januari 2020
1.8.0	• Perbarui `rdma-core` ke versi 27.0. • Perbarui modul kernel EFA ke versi 1.5.0. • Perbarui Libfabric ke versi 1.9.0amzn1.0. • Tambahkan opsi `--minimal` untuk menginstal hanya modul kernel EFA dan`rdma-core` .	Desember 2019
1.7.1	• Perbarui Libfabric ke versi 1.8.1amzn1.3.	Desember 2019
1.7.0	• Tambahkan file modul Libfabric. • Perbarui Libfabric ke versi 1.8.1amzn1.1.	November 2019
1.6.2	• Perbarui Buka MPI ke versi 1.6.2.	Oktober 2019
1.6.1	• Perbarui Libfabric ke versi 1.8.1amzn1.0. • Perbarui Buka MPI ke versi 4.0.1. • Perbarui `rdma-core` ke versi 26.0.	Oktober 2019
1.5.4	• Perbarui modul kernel EFA ke versi 1.4.1.	September 2019

Versi	Perubahan	Tanggal rilis
1.5.3	• Perbarui modul kernel EFA ke versi 1.3.1. • Hindari menginstal `kernel-devel` atau `linux-headers` paket kecuali menginstal driver kernel.	September 2019
1.5.1	• Hanya konfigurasikan halaman besar saat perangkat EFA hadir.	Agustus 2019
1.5.0	• Perbarui Libfabric ke versi 1.8.0amzn1.1. • Perbarui `rmda-core` ke versi 25.0.	Agustus 2019
1.4.1	• Tambahkan jalur pustaka Libfabric dan Open MPI (`/opt/amazon/efa/lib64` and`/opt/amazon/efa/openmpi/lib`)`/etc/ld.so.conf.d/efa.conf` untuk memastikan pustaka bersama Open MPI dan Libfabric berada dengan benar.	Juli 2019
1.4.0	• Perbarui modul kernel EFA ke versi 1.3.0. • Perbarui Libfabric ke versi 1.8.0amzn1.0 • Rilis pertama untuk mendukung Pembaruan Intel MPI 2019 4.	Juli 2019

Topologi Amazon EC2

Topologi Amazon EC2 memberikan tampilan hierarkis tentang kedekatan relatif kapasitas komputasi Anda. Anda dapat menggunakan informasi ini untuk mengelola komputasi kinerja tinggi (HPC), pembelajaran mesin (ML), dan infrastruktur komputasi AI generatif dalam skala besar.

Tersedia APIs

Amazon EC2 menyediakan dua API untuk memahami topologi EC2 Anda:

- DescribeInstanceTopology
  - Menunjukkan lokasi instance yang sedang berjalan relatif satu sama lain dalam hierarki jaringan.
  - Membantu mengoptimalkan tempat menjalankan beban kerja Anda pada instans yang ada.
- DescribeCapacityReservationTopology

- Menunjukkan lokasi kapasitas cadangan Anda relatif terhadap satu sama lain dalam hierarki jaringan sebelum Anda meluncurkan instance.
- Membantu perencanaan kapasitas dengan memberi tahu Anda penempatan kapasitas cadangan sebelum meluncurkan instance.

Manfaat utama

Topologi EC2 memberikan manfaat utama berikut:

- Manajemen kapasitas - Optimalkan pemanfaatan sumber daya.
- Job scheduling — Membuat keputusan berdasarkan informasi tentang penempatan beban kerja.
- Peringkat node — Memahami kedekatan relatif untuk pengoptimalan kinerja pada instance yang digabungkan dengan erat.

Pertimbangan-pertimbangan

- Tampilan topologi hanya tersedia untuk:
  - Contoh di negara bagian `running`
  - Reservasi Kapasitas di `pending` atau `active` negara bagian
- Setiap tampilan topologi adalah unik per. Akun AWS
- Konsol Manajemen AWS Tidak mendukung topologi tampilan.
- Meskipun informasi topologi membantu Anda memahami penempatan instans, Anda tidak dapat menggunakannya untuk meluncurkan instance baru secara fisik dekat dengan instance yang ada. Untuk memengaruhi penempatan instans, Anda dapat membuat Reservasi Kapasitas dalam grup penempatan klaster.

Harga

Tidak ada biaya tambahan untuk menjelaskan topologi EC2 Anda.

Daftar Isi

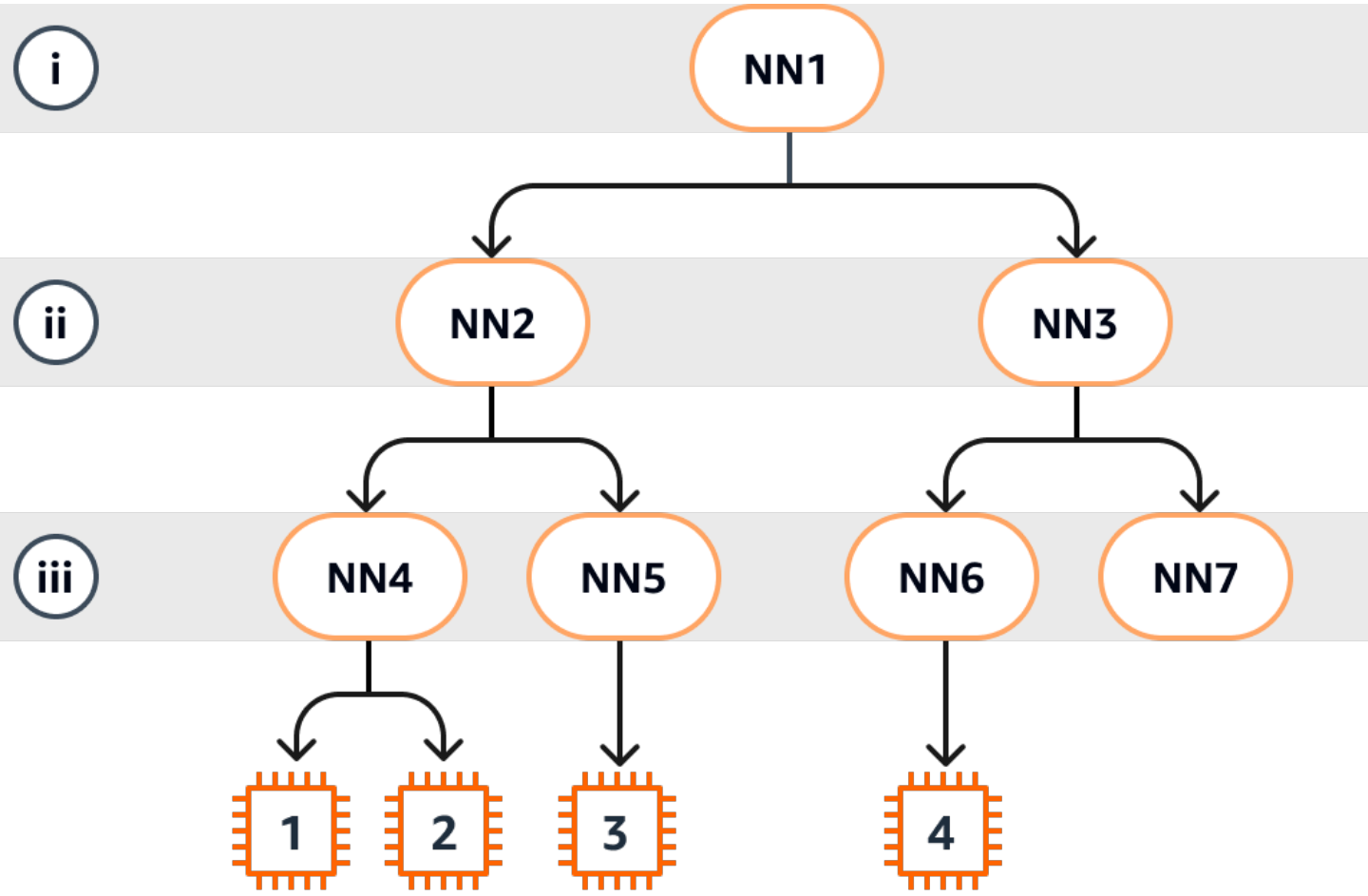
- Cara kerja topologi Amazon EC2
- Prasyarat untuk topologi Amazon EC2
- Contoh untuk topologi instans Amazon EC2

Cara kerja topologi Amazon EC2

AWS Jaringan diatur dalam hierarki lapisan. Instans EC2 terhubung ke jaringan pada atau di bawah lapisan ketiga, tergantung pada jenis instans. Topologi instance dijelaskan oleh satu set node, dengan satu node di setiap lapisan jaringan. Node yang diatur dalam respons DescribeCapacityReservationTopologyAPI DescribeInstanceTopologyatau memberikan tampilan hierarki jaringan dari atas ke bawah, dengan simpul bawah terhubung ke sebuah instance.

> **Note**
>
> Beberapa jenis contoh terdiri dari 4 node jaringan dalam satu set node yang mewakili 4 lapisan dalam jaringan, sementara yang lain terdiri dari 3 node jaringan yang mewakili 3 lapisan dalam jaringan. Untuk jenis instance yang didukung, lihatTipe instans.
> Bergantung pada jenis Reservasi Kapasitas, Anda mungkin hanya melihat 1, 2, atau 3 node jaringan.

Diagram berikut memberikan representasi visual yang dapat Anda gunakan untuk memahami topologi EC2. Node jaringan diidentifikasi sebagai NN1— NN7. Angka i, ii, dan iii mengidentifikasi lapisan jaringan. Angka 1, 2, 3, dan 4 mengidentifikasi instans EC2. Contoh terhubung ke node di lapisan bawah, diidentifikasi oleh iii dalam diagram berikut. Lebih dari satu instans dapat terhubung ke simpul yang sama.



Dalam contoh ini:

- Instance 1 terhubung ke node jaringan 4 (NN4) di lapisan iii. NN4 menghubungkan ke node jaringan 2 (NN2) di lapisan ii, dan NN2 menghubungkan ke node jaringan 1 (NN1) di lapisan i, yang merupakan bagian atas hierarki jaringan dalam contoh ini. Kumpulan node jaringan terdiri NN1,, dan NN2 NN4, diekspresikan secara hierarkis dari lapisan atas ke lapisan bawah.
- Instance 2 juga terhubung ke node jaringan 4 (NN4). Instance 1 dan instance 2 berbagi kumpulan node jaringan yang sama: NN1, NN2, dan NN4.
- Instance 3 terhubung ke node jaringan 5 (NN5). NN5 terhubung ke NN2, dan NN2 terhubung ke NN1. Node jaringan yang ditetapkan misalnya 3 adalah NN1, NN2, dan NN5.
- Instance 4 terhubung ke node jaringan 6 (NN6). Set simpul jaringannya adalah NN1, NN3, dan NN6.

Ketika mempertimbangkan kedekatan instance 1, 2, dan 3, instance 1 dan 2 lebih dekat satu sama lain karena mereka terhubung ke node jaringan yang sama (NN4), sedangkan instance 3 lebih jauh karena terhubung ke node jaringan yang berbeda (NN5).

Ketika mempertimbangkan kedekatan semua instance dalam diagram ini, instance 1, 2, dan 3 lebih dekat satu sama lain daripada instance 4 karena mereka berbagi NN2 dalam rangkaian node jaringan mereka.

Sebagai aturan umum, jika simpul jaringan yang terhubung ke dua instans adalah sama, instans ini secara fisik dekat satu sama lain, seperti halnya dengan instans 1 dan 2. Selanjutnya, makin sedikit jumlah lompatan antara simpul jaringan, makin dekat instans satu sama lain. Misalnya, instance 1 dan 3 memiliki lebih sedikit hop ke node jaringan umum (NN2) daripada yang mereka miliki ke node jaringan (NN1) yang mereka miliki bersama dengan instance 4, dan karena itu lebih dekat satu sama lain daripada instance 4.

Tidak ada instance yang berjalan di bawah node jaringan 7 (NN7) dalam contoh ini, dan oleh karena itu output API tidak akan disertakan NN7.

Bagaimana menafsirkan output DescribeInstanceTopology

Anda dapat mendeskripsikan topologi instance menggunakan API. DescribeInstanceTopology Output memberikan pandangan hierarkis dari topologi jaringan yang mendasari untuk sebuah instance.

Contoh output berikut sesuai dengan informasi topologi jaringan dari empat instans dalam diagram sebelumnya. Komentar disertakan dalam contoh output untuk keperluan contoh ini.

Informasi berikut dalam output penting untuk dicatat:

- `NetworkNodes`menggambarkan rangkaian node jaringan dari satu contoh.
- Dalam setiap set simpul jaringan, simpul jaringan terdaftar dalam urutan hierarkis dari atas ke bawah.
- Simpul jaringan yang terhubung ke instans adalah simpul jaringan terakhir dalam daftar (lapisan bawah).
- Untuk mengetahui instans mana yang dekat satu sama lain, pertama-tama temukan simpul jaringan umum di lapisan bawah. Jika tidak ada simpul jaringan umum di lapisan bawah, maka temukan simpul jaringan umum di lapisan atas.

Dalam contoh output berikut, `i-1111111111example` dan `i-2222222222example` terletak paling dekat satu sama lain dibandingkan dengan instans lain dalam contoh ini karena mereka memiliki simpul jaringan yang sama `nn-4444444444example` di lapisan bawah.

> **Note**
>
> Responsnya berisi 3 atau lebih node jaringan. Untuk informasi tentang jumlah node jaringan dalam respons untuk setiap jenis instans yang didukung, lihatTipe instans.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
 bottom layer, connected to the instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
```

```
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-5555555555example"            //Corresponds to NN5 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Bagaimana menafsirkan output DescribeCapacityReservationTopology

Anda dapat menjelaskan topologi Reservasi Kapasitas menggunakan API. DescribeCapacityReservationTopology Output memberikan pandangan hierarkis dari topologi jaringan yang mendasari untuk kapasitas cadangan.

Contoh output berikut sesuai dengan informasi topologi jaringan pada diagram sebelumnya. Komentar disertakan dalam contoh output untuk keperluan contoh ini.

Informasi berikut dalam output penting untuk dicatat:

- `NetworkNodes`menjelaskan kumpulan node jaringan dari Reservasi Kapasitas tunggal.
- Dalam setiap set simpul jaringan, simpul jaringan terdaftar dalam urutan hierarkis dari atas ke bawah.

- Node jaringan yang terhubung ke Reservasi Kapasitas adalah node jaringan terakhir dalam daftar (lapisan bawah).
- Untuk mengetahui apakah Reservasi Kapasitas akan dekat satu sama lain, pertama-tama temukan node jaringan umum di lapisan bawah pada output. Jika tidak ada simpul jaringan umum di lapisan bawah, maka temukan simpul jaringan umum di lapisan atas.

Dalam contoh output berikut, `cr-1111111111example` terletak di `nn-2222222222example` dan `cr-2222222222example` terletak din`nn-3333333333example`. Karena Reservasi Kapasitas berada di node jaringan yang berbeda`layer ii`, komunikasi dari instance dalam satu Reservasi Kapasitas ke instance di Reservasi Kapasitas lainnya tidak akan efisien.

> **Note**
>
> Respons berisi 1, 2, atau 3 node jaringan tergantung pada jenis Reservasi Kapasitas.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1111111111example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",      //Corresponds to NN1 - layer i
                "nn-2222222222example"       //Corresponds to NN2 - layer ii
                // Visibility of additional nodes requires an instance launch and
                // the DescribeInstanceTopology API
            ],
            "AvailabilityZone": "us-west-2a"
        },
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",      //Corresponds to NN1 - layer i
                "nn-3333333333example"       //Corresponds to NN3 - layer ii
                // Visibility of additional nodes requires an instance launch and
```

```
                // the DescribeInstanceTopology API
            ],
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Perbedaan antara DescribeInstanceTopology dan DescribeCapacityReservationTopology

Tabel berikut membandingkan perbedaan utama antara DescribeInstanceTopology dan DescribeCapacityReservationTopology APIs:

Titik perbandingan	DescribeInstanceTopology	DescribeCapacityReservation Topology
Fase penggunaan	Pasca-peluncuran (mode eksekusi)	Pra-peluncuran (mode perencanaan dan manajemen)
Tujuan utama	Optimalkan beban kerja pada instance yang sedang berjalan	Perencanaan kapasitas dan manajemen Reservasi Kapasitas (gabungkan, pisahkan, tetapkan) sebelum peluncuran instans
Jumlah node jaringan	Menampilkan semua node untuk instance yang sedang berjalan. Jika instance berada dalam Reservasi Kapasitas , node pertama akan cocok dengan topologi Reservasi Kapasitas yang sesuai, diikuti oleh node tambahan untuk terhubung ke instance.	Menampilkan kumpulan sebagian node, yang bervariasi berdasarkan status Reservasi Kapasitas (`pending`atau`active`) dan jenis. *

Titik perbandingan	DescribeInstanceTopology	DescribeCapacityReservationTopology
Status	Contoh harus dalam `running` keadaan	Reservasi Kapasitas harus dalam `pending` atau negara bagian `active`
Kasus penggunaan	• Optimalisasi beban kerja • Penyempurnaan performa • Analisis topologi runtime	• Perencanaan kapasitas • Manajemen Reservasi Kapasitas (merge/split/assign) • Penilaian topologi pra-peluncuran

* Untuk Blok Kapasitas untuk Ultraservers, rangkaian node jaringan sama saat menjelaskan topologi untuk Reservasi `active` Kapasitas atau instance yang sedang berjalan.

Prasyarat untuk topologi Amazon EC2

Untuk menjelaskan topologi Amazon EC2 Anda, pastikan instans dan Reservasi Kapasitas Anda memenuhi prasyarat berikut.

Prasyarat untuk:

- Wilayah AWS
- Tipe instans
- Status
- Izin IAM

Wilayah AWS

Didukung Wilayah AWS:

- AS Timur (Virginia Utara), AS Timur (Ohio), AS Barat (California Utara), AS Barat (Oregon)
- Africa (Cape Town)

- Asia Pasifik (Jakarta), Asia Pasifik (Hong Kong), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Asia Pasifik (Mumbai), Asia Pasifik (Osaka), Asia Pasifik (Seoul), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Asia Pasifik (Tokyo)
- Kanada (Pusat)
- Eropa (Frankfurt), Eropa (Irlandia), Eropa (London), Eropa (Paris), Eropa (Spanyol), Eropa (Stockholm), Eropa (Zurich)
- Israel (Tel Aviv)
- Timur Tengah (Bahrain), Timur Tengah (UEA)
- Amerika Selatan (Sao Paulo)
- AWS GovCloud (AS-Barat)

DescribeCapacityReservationTopology API tidak didukung di Israel (Tel Aviv) dan AWS GovCloud (AS-Barat).

Tipe instans

Tipe instans yang didukung:

- Mengembalikan 3* node jaringan dalam respon:
  - `g6e.xlarge` | `g6e.2xlarge` | `g6e.4xlarge` | `g6e.8xlarge` | `g6e.12xlarge` | `g6e.16xlarge` | `g6e.24xlarge` | `g6e.48xlarge` | `g7e.2xlarge` | `g7e.4xlarge` | `g7e.8xlarge` | `g7e.12xlarge` | `g7e.24xlarge` | `g7e.48xlarge`
  - `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc8a.96xlarge`
  - `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge` | `p5e.48xlarge` | `p5en.48xlarge` | `p6e-gb200.36xlarge`
  - `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge` | `trn2.48xlarge` | `trn2u.48xlarge`
- Mengembalikan 4* node jaringan dalam respon:
  - `p6-b200.48xlarge` | `p6-b300.48xlarge`

* Jumlah node jaringan yang dikembalikan hanya berlaku saat menggunakan DescribeInstanceTopology API. Untuk DescribeCapacityReservationTopology API, jumlah node jaringan yang dikembalikan akan bervariasi tergantung pada jenis dan status Reservasi Kapasitas.

Tipe instans yang tersedia berbeda-beda menurut Wilayah. Untuk informasi selengkapnya, lihat jenis instans Amazon EC2 menurut Wilayah.

Status

- Untuk `DescribeInstanceTopology` — Contoh harus di `running` negara bagian.
- Untuk `DescribeCapacityReservationTopology` — Kapasitas Reservasi harus di `pending` atau `active` negara bagian.

Anda tidak bisa mendapatkan informasi topologi untuk instance atau Reservasi Kapasitas di negara bagian lain mana pun.

Izin IAM

Identitas IAM Anda (pengguna, grup pengguna, atau peran) memerlukan izin berikut:

- `ec2:DescribeInstanceTopology`
- `ec2:DescribeCapacityReservationTopology`

Contoh untuk topologi instans Amazon EC2

Anda dapat menggunakan describe-instance-topologyperintah untuk mendeskripsikan topologi untuk instans EC2 Anda. Dan Anda dapat menggunakan describe-capacity-reservation-topologyperintah untuk menggambarkan topologi Reservasi Kapasitas Anda.

Bila Anda menggunakan `describe-capacity-reservation-topology` perintah `describe-instance-topology` atau tanpa parameter atau filter, respons mencakup semua instance atau Reservasi Kapasitas Anda (tergantung pada perintah yang digunakan) yang cocok dengan jenis instans yang didukung untuk perintah ini di Wilayah yang ditentukan. Anda dapat menentukan Wilayah dengan menyertakan parameter `--region`, atau dengan menetapkan Wilayah default. Untuk informasi selengkapnya tentang mengatur Wilayah default, lihat Pilih Wilayah untuk sumber daya Amazon EC2.

Anda dapat menyertakan parameter untuk mengembalikan instans atau Reservasi Kapasitas yang sesuai dengan contoh tertentu atau Reservasi Kapasitas IDs atau nama grup penempatan. Anda juga dapat menyertakan filter untuk mengembalikan instance atau Reservasi Kapasitas yang cocok dengan jenis instans atau keluarga instans tertentu, atau instance atau Reservasi Kapasitas di Zona

Ketersediaan atau Zona Lokal yang ditentukan. Anda dapat menyertakan satu parameter atau filter, atau kombinasi parameter dan filter.

Outputnya diberi paginasi, dengan hingga 20 instance atau Reservasi Kapasitas per halaman secara default. Anda dapat menentukan hingga 100 instance atau Reservasi Kapasitas per halaman menggunakan parameter. `--max-results`

Untuk informasi selengkapnya, lihat describe-instance-topology dan describe-reservation-topology-topology.

Izin yang diperlukan

Izin berikut diperlukan:

- `ec2:DescribeInstanceTopology`— Untuk menggambarkan topologi contoh
- `ec2:DescribeCapacityReservationTopology`— Untuk menggambarkan topologi Reservasi Kapasitas

Contoh

- Contoh 1: DescribeInstanceTopology - Instance IDs
- Contoh 2: DescribeInstanceTopology - Parameter nama grup penempatan
- Contoh 3: DescribeInstanceTopology - Filter tipe instance
  - Contoh 3a - Filter pencocokan yang tepat untuk jenis instance tertentu
  - Contoh 3b — Filter kartu liar untuk keluarga instance
  - Contoh 3c - Keluarga instance gabungan dan filter pencocokan tepat
- Contoh 4: DescribeInstanceTopology - Filter ID zona
  - Contoh 4a - Filter Availability Zone
  - Contoh 4b - Filter Zona Lokal
  - Contoh 4c - Zona Ketersediaan Gabungan dan filter Zona Lokal
- Contoh 5: DescribeInstanceTopology - Jenis instans dan filter ID zona
- Contoh 6: DescribeCapacityReservationTopology - Reservasi Kapasitas IDs
- Contoh 7: DescribeCapacityReservationTopology - Filter tipe instance

Contoh 1: DescribeInstanceTopology - Instance IDs

AWS CLI

Untuk menggambarkan topologi contoh tertentu

Gunakan describe-instance-topologyperintah dengan `--instance-ids` parameter. Outputnya hanya mencakup instance yang cocok dengan instance IDs yang ditentukan.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

Berikut ini adalah output contoh.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
```

```
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menggambarkan topologi contoh tertentu

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -InstanceId i-1111111111example, i-2222222222example
```

Contoh 2: DescribeInstanceTopology - Parameter nama grup penempatan

AWS CLI

Untuk menggambarkan topologi contoh dalam kelompok penempatan tertentu

Gunakan describe-instance-topologyperintah dengan `group-names` parameter. Output hanya mencakup instance yang ada di salah satu grup penempatan yang ditentukan.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

Berikut ini adalah output contoh.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
```

```
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menggambarkan topologi contoh dalam kelompok penempatan tertentu

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -GroupName ML-group, HPC-group
```

Contoh 3: DescribeInstanceTopology - Filter tipe instance

Anda dapat memfilter berdasarkan tipe instans tertentu (sama persis) atau memfilter menurut keluarga instans (menggunakan wildcard). Anda juga dapat menggabungkan filter tipe instans tertentu dan filter keluarga instans.

Contoh 3a - Filter pencocokan yang tepat untuk jenis instance tertentu

AWS CLI

Untuk mendeskripsikan topologi instance dengan tipe instance tertentu

Gunakan describe-instance-topologyperintah dengan `instance-type` filter. Outputnya hanya mencakup instance dengan tipe instance yang ditentukan.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

Berikut ini adalah output contoh.

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk mendeskripsikan topologi instance dengan tipe instance tertentu

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="trn1n.32xlarge"}
```

Contoh 3b — Filter kartu liar untuk keluarga instance

AWS CLI

Untuk menggambarkan topologi instance dengan keluarga instance tertentu

Gunakan describe-instance-topologyperintah dengan `instance-type` filter. Output hanya mencakup instance dengan keluarga instance tertentu.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

Berikut ini adalah output contoh.


```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
```

```
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menggambarkan topologi instance dengan keluarga instance tertentu

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="trn1*"}
```

Contoh 3c - Keluarga instance gabungan dan filter pencocokan tepat

AWS CLI

Untuk menggambarkan topologi instance dengan keluarga instance atau tipe instance

Gunakan describe-instance-topologyperintah dengan `instance-type` filter. Output hanya mencakup contoh yang memenuhi kriteria yang ditentukan.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

Berikut ini adalah output contoh.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
```

```
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-4343434343example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menggambarkan topologi instance dengan keluarga instance atau tipe instance

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="p4d*", "trn1n.32xlarge"}
```

Contoh 4: DescribeInstanceTopology - Filter ID zona

Anda dapat menggunakan filter `zone-id` untuk memfilter berdasarkan Zona Ketersediaan atau Local Zones. Anda juga dapat menggabungkan filter Zona Ketersediaan dan filter Local Zones.

Contoh 4a - Filter Availability Zone

AWS CLI

Untuk menjelaskan topologi instance di Availability Zone tertentu

Gunakan describe-instance-topologyperintah dengan `zone-id` filter. Output hanya mencakup instance di Availability Zone yang ditentukan.

```
aws ec2 describe-instance-topology \
```

```
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

Berikut ini adalah output contoh.

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menjelaskan topologi instance di Availability Zone tertentu

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-az1"}
```

Contoh 4b - Filter Zona Lokal

AWS CLI

Untuk menggambarkan topologi contoh di Zona Lokal tertentu

Gunakan describe-instance-topologyperintah dengan `zone-id` filter. Output hanya mencakup instance di Zona Lokal yang ditentukan.

```
aws ec2 describe-instance-topology \
```

```
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

Berikut ini adalah output contoh.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menggambarkan topologi contoh di Zona Lokal tertentu

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-atl2-az1"}
```

Contoh 4c - Zona Ketersediaan Gabungan dan filter Zona Lokal

AWS CLI

Untuk menggambarkan topologi contoh di zona tertentu

Gunakan describe-instance-topologyperintah dengan `zone-id` filter. Output hanya mencakup contoh yang berada di salah satu zona yang ditentukan.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Berikut ini adalah output contoh.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menggambarkan topologi contoh di zona tertentu

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-az1", "use1-atl2-az1"}
```

Contoh 5: DescribeInstanceTopology - Jenis instans dan filter ID zona

Anda dapat menggabungkan filter dalam satu perintah.

AWS CLI

Untuk menggambarkan topologi instance dengan tipe instance tertentu, keluarga instance, dan zona

Gunakan describe-instance-topologyperintah dengan `zone-id` filter `instance-type` dan. Respons berisi instance apa pun dengan salah satu jenis instance yang ditentukan dan berada di salah satu zona yang ditentukan.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" \
              "Name=zone-id,Values=use1-az1,use1-atl2-az1"
```

Berikut ini adalah output contoh.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
```

```
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menggambarkan topologi instance dengan tipe instance tertentu, keluarga instance, dan zona

Gunakan Get-EC2InstanceTopologycmdlet.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="p4d*", "trn1n.32xlarge"} `
            @{Name="zone-id"; Values="use1-az1", "use1-atl2-az1"}
```

Contoh 6: DescribeCapacityReservationTopology - Reservasi Kapasitas IDs

AWS CLI

Untuk menggambarkan topologi Reservasi Kapasitas tertentu

Gunakan describe-capacity-reservation-topologyperintah dengan `capacity-reservation-id` parameter. Output hanya mencakup Reservasi Kapasitas yang sesuai dengan Reservasi Kapasitas yang ditentukan. IDs

```
aws ec2 describe-capacity-reservation-topology \
    --region us-east-1 \
    --capacity-reservation-id cr-1111111111example cr-2222222222example
```

Berikut ini adalah output contoh.

```
{
```

```
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1111111111example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        },
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5en.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk menggambarkan topologi Reservasi Kapasitas tertentu

Gunakan Get-EC2CapacityReservationTopologycmdlet.

```
Get-EC2CapacityReservationTopology `
    -CapacityReservationId cr-1111111111example cr-2222222222example
```

Contoh 7: DescribeCapacityReservationTopology - Filter tipe instance

Anda dapat memfilter berdasarkan tipe instans tertentu (sama persis) atau memfilter menurut keluarga instans (menggunakan wildcard). Anda juga dapat menggabungkan filter tipe instans tertentu dan filter keluarga instans.

AWS CLI

Untuk mendeskripsikan topologi Reservasi Kapasitas dengan jenis instans tertentu

Gunakan describe-capacity-reservation-topologyperintah dengan `instance-type` filter. Respons berisi instance apa pun dengan tipe instance yang ditentukan.

```
aws ec2 describe-capacity-reservation-topology \
    --region us-east-1 \
    --filters Name=instance-type,Values=p5en.48xlarge
```

Berikut ini adalah output contoh.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5en.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Untuk mendeskripsikan topologi Reservasi Kapasitas dengan jenis instans tertentu

Gunakan Get-EC2CapacityReservationTopologycmdlet.

```
Get-EC2CapacityReservationTopology `
    -Filter @{Name="instance-type"; Values="p5en.48xlarge"}
```

Grup penempatan untuk EC2 instans Amazon Anda

Untuk memenuhi kebutuhan beban kerja Anda, Anda dapat meluncurkan sekelompok EC2 instance yang saling bergantung ke dalam grup penempatan untuk memengaruhi penempatan mereka.

Tergantung tipe beban kerja, Anda dapat membuat grup penempatan menggunakan salah satu strategi penempatan berikut:

- Klaster – mengemas instans saling mendekat di dalam Zona Ketersediaan. Strategi ini memungkinkan beban kerja untuk mencapai kinerja jaringan latensi rendah yang diperlukan untuk node-to-node komunikasi yang digabungkan secara ketat yang khas dari aplikasi komputasi kinerja tinggi (HPC).
- Partisi – menyebarkan instans Anda di seluruh partisi logis sehingga grup instans dalam satu partisi tidak menggunakan bersama perangkat keras yang mendasari dengan grup instans dalam partisi berbeda. Strategi ini biasanya digunakan oleh beban kerja yang terdistribusi dan direplikasi besar, seperti Hadoop, Cassandra, dan Kafka.
- Sebaran – secara ketat menempatkan sekelompok kecil instans di seluruh perangkat keras yang mendasari untuk mengurangi kegagalan yang berhubungan.

Grup penempatan adalah opsional. Jika Anda tidak meluncurkan instans Anda ke grup penempatan, cobalah untuk EC2 menempatkan instance sedemikian rupa sehingga semua instance Anda tersebar di seluruh perangkat keras yang mendasarinya untuk meminimalkan kegagalan yang berkorelasi.

Harga

Tidak ada biaya untuk membuat grup penempatan.

Aturan dan batasan

Sebelum Anda menggunakan grup penempatan, perhatikan aturan berikut ini:

- Sebuah instance dapat ditempatkan dalam satu grup penempatan pada satu waktu; Anda tidak dapat menempatkan instance di beberapa grup penempatan.
- Anda tidak dapat menggabungkan grup penempatan.
- Reservasi Kapasitas Sesuai Permintaan dan Instans Cadangan zona memungkinkan Anda memesan kapasitas untuk EC2 instans di Availability Zone. Saat Anda meluncurkan instance, jika atribut instance cocok dengan yang ditentukan oleh Reservasi Kapasitas Sesuai Permintaan atau

Instans Cadangan zona, maka kapasitas cadangan secara otomatis digunakan oleh instans. Ini juga benar jika Anda meluncurkan instance ke dalam grup penempatan.

- Anda tidak dapat meluncurkan Host Khusus di grup penempatan.
- Anda tidak dapat meluncurkan Instans Spot yang dikonfigurasi untuk menghentikan atau hibernasi saat interupsi dalam grup penempatan.

Daftar Isi

- Strategi penempatan untuk grup penempatan Anda
- Buat grup penempatan untuk EC2 instans Anda
- Ubah penempatan untuk sebuah EC2 instance
- Menghapus grup penempatan
- Grup penempatan bersama
- Grup penempatan di AWS Outposts

Strategi penempatan untuk grup penempatan Anda

Anda dapat membuat grup penempatan untuk EC2 instans Anda menggunakan salah satu strategi penempatan berikut.

Strategi penempatan

- Grup penempatan klaster
- Grup penempatan partisi
- Grup penempatan tersebar

Grup penempatan klaster

Grup penempatan klaster adalah pengelompokan logis dari instans di dalam Zona Ketersediaan. Contoh tidak diisolasi ke satu rak. Grup penempatan cluster dapat menjangkau jaringan pribadi virtual peered (VPCs) di Wilayah yang sama. Instans dalam grup penempatan cluster yang sama menikmati batas throughput per aliran yang lebih tinggi untuk TCP/IP lalu lintas dan ditempatkan di segmen bandwidth biseksi tinggi yang sama dari jaringan.

Image berikut menunjukkan instans yang ditempatkan dalam grup penempatan klaster.

Grup penempatan klaster direkomendasikan untuk aplikasi yang mendapatkan keuntungan dari latensi jaringan rendah, throughput jaringan tinggi, atau keduanya. Grup-grup itu juga direkomendasikan ketika mayoritas lalu lintas jaringan berada di antara instans dalam grup. Untuk memberikan latensi terendah dan kinerja packet-per-second jaringan tertinggi untuk grup penempatan Anda, pilih jenis instans yang mendukung jaringan yang disempurnakan. Untuk informasi lebih lanjut, lihat Jaringan yang Ditingkatkan.

Kami menyarankan Anda untuk meluncurkan instans Anda dengan cara berikut:

- Gunakan permintaan peluncuran tunggal untuk meluncurkan jumlah instans yang Anda butuhkan dalam grup penempatan.
- Gunakan tipe instans yang sama untuk semua instans di grup penempatan.

Jika Anda mencoba menambahkan lebih banyak instans ke grup penempatan nanti, atau jika Anda mencoba meluncurkan lebih dari satu tipe instans dalam grup penempatan, Anda meningkatkan peluang mendapatkan kesalahan kapasitas yang tidak cukup.

Jika Anda menghentikan satu instans dalam grup penempatan dan kemudian memulainya lagi, ini masih berjalan dalam grup penempatan. Namun demikian, momen mulai gagal jika tidak cukup kapasitas untuk instans.

Jika Anda menerima kesalahan kapasitas saat meluncurkan suatu instans dalam grup penempatan yang sudah memiliki instans, hentikan dan mulai semua instans dalam grup penempatan, dan coba luncurkan lagi. Memulai instans dapat memigrasikannya ke perangkat keras yang memiliki kapasitas untuk semua proses yang diminta.

Aturan dan batasan

Aturan berikut berlaku untuk grup penempatan klaster:

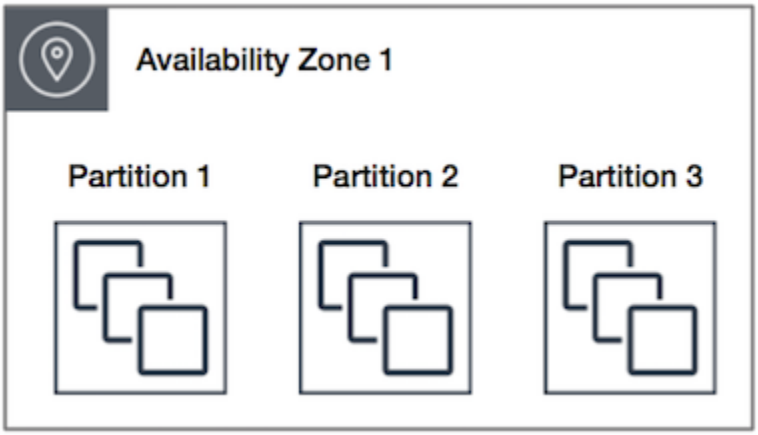
- Berikut ini adalah tipe instans yang didukung:
  - Instans generasi saat ini, kecuali instans performa burstable (misalnya, T2), instans Mac1, dan instans M7i-flex.
  - Contoh generasi sebelumnya berikut: A1, C3, C4, I2, M4, R3, dan R4.
- Grup penempatan klaster tidak dapat mencakup beberapa Zona Ketersediaan.
- Kecepatan throughput maksimum jaringan di antara dua instans dalam grup penempatan klaster dibatasi oleh pelambatan dua instans. Untuk aplikasi dengan persyaratan high-throughput, pilih tipe instans dengan sambungan jaringan yang memenuhi kebutuhan Anda.
- Untuk instans yang diaktifkan untuk jaringan yang ditingkatkan, aturan berikut berlaku:
  - Instans di dalam grup penempatan klaster dapat menggunakan hingga 10 Gbps untuk lalu lintas alur tunggal. Instans yang tidak berada di dalam grup penempatan klaster dapat menggunakan hingga 5 Gbps untuk lalu lintas alur tunggal.
  - Lalu lintas ke dan dari bucket Amazon S3 dalam Wilayah yang sama melalui ruang alamat IP publik atau melalui titik akhir VPC dapat menggunakan semua bandwidth agregat instans yang tersedia.
- Anda dapat meluncurkan beberapa tipe instans ke dalam grup penempatan klaster. Namun demikian, ini mengurangi kemungkinan bahwa jadwal yang diperlukan akan tersedia untuk peluncuran Anda agar berhasil. Kami menyarankan Anda menggunakan tipe instans yang sama untuk semua instans dalam grup penempatan klaster.
- Sebaiknya Anda memesan kapasitas secara eksplisit di grup penempatan klaster dengan membuat Reservasi Kapasitas Sesuai Permintaan di grup penempatan klaster. Perhatikan bahwa Anda tidak dapat memesan kapasitas menggunakan Instans Cadangan zona, karena mereka tidak dapat memesan kapasitas secara eksplisit dalam grup penempatan.
- Lalu lintas jaringan ke internet dan melalui Direct Connect koneksi ke sumber daya lokal dibatasi hingga 5 Gbps untuk grup penempatan klaster.

Grup penempatan partisi

Grup penempatan partisi membantu mengurangi kemungkinan kegagalan perangkat keras terkait untuk aplikasi Anda. Saat menggunakan grup penempatan partisi, Amazon EC2 membagi setiap grup menjadi segmen logis yang disebut partisi. Amazon EC2 memastikan bahwa setiap partisi dalam

grup penempatan memiliki set rak sendiri. Setiap rak IT jaringan dan sumber daya sendiri. Tidak ada dua bagian di dalam grup penempatan yang memiliki rak yang sama, yang memungkinkan Anda mengisolasi dampak kegagalan perangkat keras di dalam aplikasi Anda.

Image berikut adalah representasi visual sederhana dari grup penempatan partisi dalam satu Zona Ketersediaan. Ini menunjukkan instans yang ditempatkan ke dalam grup penempatan partisi dengan tiga partisi—Partisi 1, Partisi 2, dan Partisi 3. Setiap partisi terdiri dari beberapa instans. Instans dalam suatu partisi tidak menggunakan bersama rak dengan instans di dalam partisi lainnya, yang memungkinkan Anda untuk mencakup dampak kegagalan perangkat lunak tunggal ke hanya partisi terkait.



Grup penempatan partisi dapat digunakan untuk menyebarkan beban kerja terdistribusi dan direplikasi yang besar, seperti HDFS,, dan Cassandra HBase, di rak yang berbeda. Saat Anda meluncurkan instance ke grup penempatan partisi, Amazon EC2 mencoba mendistribusikan instance secara merata di seluruh jumlah partisi yang Anda tentukan. Anda juga dapat meluncurkan instans ke partisi tertentu untuk memiliki lebih banyak kontrol terhadap lokasi instans.

Suatu grup penempatan partisi dapat memiliki partisi pada beberapa Zona Ketersediaan di Wilayah yang sama. Grup penempatan partisi dapat memiliki maksimum tujuh partisi per Zona Ketersediaan. Jumlah instans yang dapat diluncurkan ke grup penempatan partisi hanya dibatasi oleh batas akun Anda.

Selain itu, grup penempatan partisi menawarkan visibilitas ke dalam partisi – Anda dapat melihat instans mana dan berada di partisi mana. Anda dapat membagikan informasi ini dengan aplikasi sadar topologi, seperti HDFS,, dan Cassandra. HBase Aplikasi ini menggunakan informasi ini untuk membuat keputusan replikasi data cerdas guna meningkatkan ketersediaan data durabilitas data.

Jika Anda memulai atau meluncurkan suatu instans dalam grup penempatan partisi dan tidak ada perangkat keras unik yang cukup untuk memenuhi permintaan, maka permintaan tersebut gagal. Amazon EC2 membuat perangkat keras yang lebih berbeda tersedia dari waktu ke waktu, sehingga Anda dapat mencoba permintaan Anda lagi nanti.

Aturan dan batasan

Aturan berikut berlaku untuk grup penempatan partisi:

- Grup penempatan partisi mendukung memiliki maksimum tujuh partisi per Zona Ketersediaan. Jumlah instans yang dapat diluncurkan dalam grup penempatan partisi hanya dibatasi oleh batas akun Anda.
- Saat instance diluncurkan ke grup penempatan partisi, Amazon EC2 mencoba mendistribusikan instance secara merata di semua partisi. Amazon EC2 tidak menjamin distribusi instans yang merata di semua partisi.
- Sebuah grup penempatan partisi dengan Instans Khusus bisa memiliki maksimum dua partisi.
- Reservasi Kapasitas tidak menyimpan kapasitas dalam grup penempatan partisi.

Grup penempatan tersebar

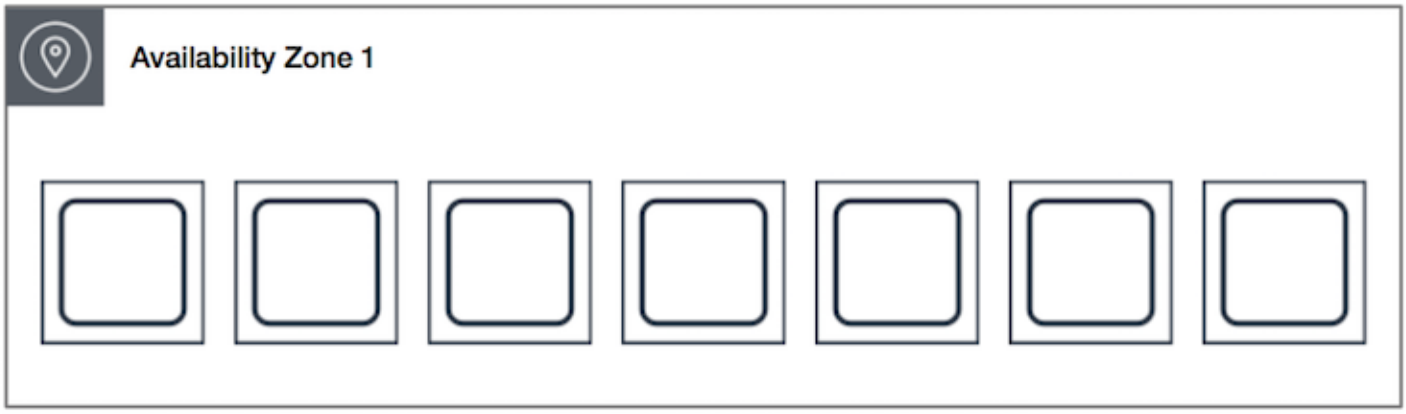
Grup penempatan sebaran adalah kelompok instans yang ditempatkan pada perangkat keras yang berbeda.

Grup penempatan sebaran direkomendasikan untuk aplikasi yang memiliki sejumlah kecil instans penting yang harus disimpan terpisah satu sama lain. Peluncuran instans dalam grup penempatan tingkat sebaran mengurangi risiko kegagalan simultan yang mungkin terjadi ketika instans memiliki peralatan yang sama. Grup penempatan tingkat tersebar menyediakan akses ke perangkat keras yang berbeda, dan oleh karena itu cocok untuk menggabungkan tipe instans atau meluncurkan instans dari waktu ke waktu.

Jika Anda memulai atau meluncurkan suatu instans dalam grup penempatan sebaran dan tidak ada perangkat keras unik yang cukup untuk memenuhi permintaan, maka permintaan tersebut gagal. Amazon EC2 membuat perangkat keras yang lebih berbeda tersedia dari waktu ke waktu, sehingga Anda dapat mencoba permintaan Anda lagi nanti. Grup penempatan dapat menyebarkan instans di seluruh rak atau host. Grup penempatan spread level rak dapat digunakan di AWS Wilayah dan seterusnya AWS Outposts. Grup penempatan spread level host AWS Outposts hanya dapat digunakan.

Grup penempatan penyebaran tingkat rak

Image berikut menunjukkan tujuh instans dalam satu Zona Ketersediaan yang ditempatkan dalam grup penempatan sebaran. Tujuh instans tersebut ditempatkan di tujuh rak yang berbeda, masing-masing rak memiliki jaringan dan sumber daya sendiri.



Grup penempatan spread level rak dapat menjangkau beberapa Availability Zone di Region yang sama. Di Wilayah, grup penempatan spread level rak dapat memiliki maksimal tujuh instance berjalan per Availability Zone per grup. Dengan Outposts, grup penempatan spread level rak dapat menampung sebanyak mungkin instance karena Anda memiliki rak di penyebaran Outpost Anda.

Grup penempatan sebaran tingkat host

Grup penempatan spread tingkat host hanya tersedia dengan AWS Outposts. Grup penempatan tingkat penyebaran host dapat menampung instance sebanyak yang Anda miliki di penyebaran Outpost Anda. Untuk informasi selengkapnya, lihat the section called “Grup penempatan di AWS Outposts”.

Aturan dan batasan

Aturan berikut berlaku untuk grup penempatan tersebar:

- Grup penempatan sebaran rak mendukung maksimal tujuh instans yang berjalan per Zona Ketersediaan. Misalnya, di Wilayah dengan tiga Zona Ketersediaan, Anda dapat menjalankan total 21 instans dalam grup, dengan tujuh instans di setiap Zona Ketersediaan. Jika Anda mencoba memulai instans kedelapan dalam Zona Ketersediaan yang sama dan dalam grup penempatan sebaran yang sama, instans tersebut tidak akan diluncurkan. Jika Anda membutuhkan lebih dari tujuh instans di Zona Ketersediaan, sebaiknya Anda menggunakan beberapa grup penempatan sebaran. Penggunaan beberapa grup penempatan sebaran tidak memberikan jaminan tentang

penyebaran instans antar grup, tetapi ini membantu memastikan penyebaran untuk tiap-tiap grup, sehingga membatasi dampak dari kelas kegagalan tertentu.

- Grup penempatan sebaran tidak didukung untuk Instans Khusus.
- Grup penempatan spread tingkat host hanya didukung untuk grup penempatan di AWS Outposts. Grup penempatan spread tingkat host dapat menampung instance sebanyak yang Anda miliki sebagai host dalam penyebaran Outpost Anda.
- Di Wilayah, grup penempatan spread level rak dapat memiliki maksimal tujuh instance berjalan per Availability Zone per grup. Dengan AWS Outposts, grup penempatan spread level rak dapat menampung sebanyak mungkin instance karena Anda memiliki rak di penyebaran Outpost Anda.
- Reservasi Kapasitas tidak menyimpan kapasitas dalam grup penempatan sebaran.

Buat grup penempatan untuk EC2 instans Anda

Anda dapat menggunakan grup penempatan untuk mengontrol penempatan instance relatif satu sama lain. Setelah membuat grup penempatan, Anda dapat meluncurkan instance di grup penempatan.

Batasan

Anda dapat membuat maksimal 500 grup penempatan per Wilayah.

Console

Untuk membuat grup penempatan

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Grup Penempatan.
3. Pilih Buat grup penempatan.
4. Tentukan nama untuk grup tersebut.
5. Pilih strategi penempatan untuk grup: Cluster, Spread, atau Partition.

   Jika Anda memilih Spread, Anda harus memilih level spread: Rack atau Host.

   Jika Anda memilih Partisi, Anda harus memasukkan jumlah partisi untuk grup.
6. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru, lalu masukkan kunci dan nilai.
7. Pilih Buat grup.

AWS CLI

Gunakan perintah create-placement-group.

Untuk membuat grup penempatan cluster

Contoh berikut membuat grup penempatan yang menggunakan strategi `cluster` penempatan, dan menerapkan tag dengan kunci `purpose` dan nilai`production`.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

Untuk membuat grup penempatan partisi

Contoh berikut membuat grup penempatan yang menggunakan strategi `partition` penempatan, dan menentukan lima partisi menggunakan parameter. `--partition-count`

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
    --partition-count 5
```

PowerShell

Gunakan New-EC2PlacementGroupcmdlet.

Untuk membuat grup penempatan cluster

Contoh berikut membuat grup penempatan cluster.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy cluster
```

Untuk membuat grup penempatan partisi

Contoh berikut membuat grup penempatan partisi.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
```

```
    -Strategy partition `
    -PartitionCount 5
```

Ubah penempatan untuk sebuah EC2 instance

Anda dapat mengubah grup penempatan suatu instans dengan cara berikut:

- Tambahkan instance ke grup penempatan
- Pindahkan satu instans dari satu grup penempatan ke grup penempatan lainnya
- Menghapus instans dari grup penempatan

Persyaratan

Sebelum Anda dapat mengubah grup penempatan untuk sebuah instance, instance harus dalam `stopped` keadaan.

Console

Untuk mengubah penempatan instance

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pilih Tindakan, Pengaturan instans, Modifikasi penempatan instans.
5. Untuk grup Penempatan, lakukan salah satu hal berikut:
   - Untuk menambahkan instance ke grup penempatan, pilih grup penempatan.
   - Untuk memindahkan instance dari satu grup penempatan ke grup penempatan lainnya, pilih grup penempatan.
   - Untuk menghapus instance dari grup penempatan, pilih Tidak Ada.
6. Pilih Simpan.

AWS CLI

Untuk memindahkan instans ke grup penempatan

Gunakan perintah berikut modify-instance-placement.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

Untuk menghapus instans dari grup penempatan

Gunakan perintah berikut modify-instance-placement. Saat Anda menentukan string kosong untuk nama grup penempatan, ini akan menghapus instance dari grup penempatan saat ini.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

PowerShell

Untuk memindahkan instans ke grup penempatan

Gunakan Edit-EC2InstancePlacementcmdlet dengan nama grup penempatan.

```
Edit-EC2InstancePlacement `
    -InstanceId i-0123a456700123456 `
    -GroupName MySpreadGroup
```

Untuk menghapus instans dari grup penempatan

Gunakan Edit-EC2InstancePlacementcmdlet dengan string kosong untuk nama grup penempatan.

```
Edit-EC2InstancePlacement `
    -InstanceId i-0123a456700123456 `
    -GroupName ""
```

Menghapus grup penempatan

Jika Anda perlu mengganti grup penempatan atau tidak lagi memerlukannya, Anda dapat menghapusnya. Sebelum Anda dapat menghapus grup penempatan, grup penempatan harus tidak berisi instans. Anda dapat menghentikan instance, memindahkannya ke grup penempatan lain, atau menghapusnya dari grup penempatan.

Console

Untuk menghapus grup penempatan

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Grup Penempatan.
3. Pilih grup penempatan dan pilih Tindakan, Hapus.
4. Saat diminta konfirmasi, masukkan **`Delete`**, lalu pilih Hapus.

AWS CLI

Untuk menghapus grup penempatan

Gunakan perintah delete-placement-group.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Untuk menghapus grup penempatan

Gunakan Remove-EC2PlacementGroupcmdlet.

```
Remove-EC2PlacementGroup -GroupName my-cluster
```

Grup penempatan bersama

Berbagi grup penempatan memungkinkan Anda memengaruhi penempatan instance yang saling bergantung yang dimiliki oleh terpisah. Akun AWS Pemilik dapat berbagi grup penempatan di beberapa Akun AWS atau di dalam organisasi mereka. Peserta dapat meluncurkan instance dalam grup penempatan yang dibagikan dengan akun mereka.

Pemilik grup penempatan dapat berbagi grup penempatan dengan:

- AWS Akun spesifik di dalam atau di luar organisasinya
- Unit organisasi di dalam organisasi -nya
- Seluruh organisasi -nya

Anda dapat menggunakan peering VPC untuk menghubungkan instans yang dimiliki oleh AWS akun terpisah dan mendapatkan manfaat latensi penuh yang ditawarkan oleh grup penempatan cluster bersama.

Daftar Isi

- Aturan dan batasan
- Izin yang diperlukan
- Berbagi di seluruh Availability Zone
- Berbagi grup penempatan
- Kelompok penempatan tidak berbagi

Aturan dan batasan

Aturan dan batasan berikut berlaku saat Anda berbagi grup penempatan atau ketika grup penempatan dibagikan dengan Anda.

- Untuk berbagi grup penempatan, Anda harus memilikinya di AWS akun Anda. Anda tidak dapat membagikan grup penempatan yang telah dibagikan dengan Anda.
- Ketika Anda berbagi partisi atau grup penempatan sebaran, batas grup penempatan tidak berubah. Grup penempatan partisi bersama mendukung maksimal tujuh partisi per Zona Ketersediaan, dan grup penempatan sebaran bersama mendukung maksimal tujuh instans yang berjalan per Zona Ketersediaan.
- Untuk berbagi grup penempatan dengan organisasi Anda atau unit organisasi di organisasi Anda, Anda harus mengaktifkan berbagi dengan AWS Organizations. Untuk informasi lebih lanjut, lihat Berbagi sumber daya AWS Anda.
- Saat menggunakan Konsol Manajemen AWS untuk meluncurkan instance, Anda dapat memilih grup penempatan apa pun yang dibagikan dengan Anda. Saat menggunakan AWS CLI untuk meluncurkan instance, Anda harus menentukan grup penempatan bersama berdasarkan ID, bukan dengan nama. Anda dapat menggunakan nama grup penempatan hanya jika Anda adalah pemilik grup penempatan bersama.
- Anda bertanggung jawab untuk mengelola instans yang dimiliki oleh Anda dalam grup penempatan bersama.
- Anda tidak dapat melihat atau mengubah instance dan reservasi kapasitas yang terkait dengan grup penempatan bersama tetapi tidak dimiliki oleh Anda.

- Nama Sumber Daya Amazon (ARN) dari grup penempatan berisi ID akun yang memiliki grup penempatan. Anda dapat menggunakan bagian ID akun dari grup penempatan ARN untuk mengidentifikasi pemilik grup penempatan yang dibagikan dengan Anda.

Izin yang diperlukan

Untuk berbagi grup penempatan, pengguna harus memiliki izin untuk tindakan berikut:

- `ec2:PutResourcePolicy`
- `ec2:DeleteResourcePolicy`

Berbagi di seluruh Availability Zone

Untuk memastikan bahwa sumber daya didistribusikan di seluruh Zona Ketersediaan untuk suatu Wilayah, kami secara independen memetakan Zona Ketersediaan ke nama untuk setiap akun . Hal ini dapat menyebabkan perbedaan penamaan Zona Ketersediaan di seluruh akun. Misalnya, Availability Zone `us-east-1a` untuk AWS akun Anda mungkin tidak memiliki lokasi yang sama dengan AWS akun lain. `us-east-1a`

Untuk menentukan lokasi Host Khusus relatif terhadap akun Anda, Anda harus menggunakan ID Zona Ketersediaan (ID AZ). ID AZ adalah pengidentifikasi unik dan konsisten untuk Zona Ketersediaan di semua akun AWS . Misalnya, `use1-az1` adalah ID Zona Ketersediaan untuk Wilayah `us-east-1` dan lokasinya sama di setiap akun AWS . Untuk informasi lebih lanjut, lihat AZ IDs.

Berbagi grup penempatan

Untuk membagikan grup penempatan, Anda harus menambahkannya ke berbagi sumber daya. Berbagi sumber daya adalah AWS RAM sumber daya yang memungkinkan Anda berbagi sumber daya di seluruh AWS akun. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan berbagi dengan mereka.

Jika Anda adalah bagian dari organisasi dalam AWS Organizations berbagi dalam organisasi Anda diaktifkan, konsumen di organisasi Anda diberikan akses ke grup penempatan bersama.

Jika grup penempatan dibagikan dengan AWS akun di luar organisasi Anda, pemilik AWS akun akan menerima undangan untuk bergabung dengan pembagian sumber daya. Mereka dapat mengakses grup penempatan bersama setelah menerima undangan.

Anda dapat berbagi grup penempatan di seluruh AWS akun menggunakan AWS Resource Access Manager. Untuk informasi selengkapnya, lihat Membuat berbagi sumber daya di Panduan AWS RAM Pengguna.

Kelompok penempatan tidak berbagi

Pemilik grup penempatan dapat membatalkan pembagian grup penempatan bersama kapan saja. Saat Anda membatalkan pembagian grup penempatan bersama, perubahan berikut akan terjadi:

- AWS Akun yang digunakan untuk berbagi grup penempatan tidak lagi dapat meluncurkan instance atau kapasitas cadangan.
- Instance apa pun yang berjalan dalam grup penempatan bersama akan dipisahkan dari grup penempatan, tetapi mereka terus berjalan di akun Anda AWS .
- Setiap reservasi kapasitas dalam grup penempatan bersama dipisahkan dari grup penempatan, tetapi tetap tersedia untuk Anda di akun Anda. AWS

Untuk informasi selengkapnya, lihat Menghapus pembagian sumber daya di Panduan AWS RAM Pengguna.

Grup penempatan di AWS Outposts

AWS Outposts adalah layanan yang dikelola sepenuhnya yang memperluas AWS infrastruktur, layanan APIs, dan alat ke tempat pelanggan. Dengan menyediakan akses lokal ke infrastruktur AWS terkelola, AWS Outposts memungkinkan pelanggan untuk membangun dan menjalankan aplikasi di tempat menggunakan antarmuka pemrograman yang sama seperti di AWS Wilayah, sambil menggunakan sumber daya komputasi dan penyimpanan lokal untuk latensi yang lebih rendah dan kebutuhan pemrosesan data lokal.

Outpost adalah kumpulan kapasitas AWS komputasi dan penyimpanan yang digunakan di situs pelanggan. AWS mengoperasikan, memantau, dan mengelola kapasitas ini sebagai bagian dari suatu AWS Wilayah.

Anda dapat membuat grup penempatan di Outposts yang telah Anda buat di akun Anda. Hal ini memungkinkan Anda untuk menyebarkan instans di perangkat keras yang mendasarinya di Outpost di situs Anda. Anda membuat dan menggunakan grup penempatan di Outposts dengan cara yang sama seperti Anda membuat dan menggunakan grup penempatan di Zona Ketersediaan biasa. Saat Anda membuat grup penempatan dengan strategi penyebaran di Outpost, Anda dapat memilih agar

grup penempatan menyebarkan instans di seluruh host atau rak. Menyebarkan instans di seluruh host memungkinkan Anda menggunakan strategi penyebaran dengan satu rak Outpost.

Pertimbangan-pertimbangan

- Grup penempatan spread level rak dapat menampung sebanyak mungkin instance karena Anda memiliki rak di penyebaran Outpost Anda.
- Grup penempatan spread tingkat host dapat menampung instance sebanyak yang Anda miliki sebagai host dalam penyebaran Outpost Anda.

Prasyarat

Anda harus menginstal Outpost di situs Anda. Untuk informasi selengkapnya, lihat Membuat Outpost dan memesan kapasitas Outpost di Panduan Pengguna AWS Outposts .

Untuk menggunakan grup penempatan di Outpost

1. Buatlah subnet pada Outpost. Untuk informasi selengkapnya, lihat Membuat subnet di Panduan Pengguna AWS Outposts .
2. Buat grup penempatan di Wilayah terkait Outpost. Jika Anda membuat grup penempatan dengan strategi penyebaran, Anda dapat memilih spread tingkat host atau rak untuk menentukan bagaimana grup akan menyebarkan instance di seluruh perangkat keras yang mendasarinya di Outpost Anda. Untuk informasi selengkapnya, lihat the section called “Buat grup penempatan”.
3. Luncurkan instans ke dalam grup penempatan. Untuk Subnet pilih subnet yang Anda buat di Langkah 1, dan untuk Nama grup penempatan, pilih grup penempatan yang Anda buat di Langkah 2. Untuk informasi selengkapnya, lihat Meluncurkan instans pada Outpost di Panduan Pengguna AWS Outposts .

Unit transmisi maksimum jaringan (MTU) untuk instans Anda EC2

Maximum transmission unit (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang dapat diizinkan yang dapat dilewatkan melalui koneksi. Semakin besar MTU suatu koneksi, semakin banyak data yang dapat dilewatkan dalam satu paket tunggal. Paket Ethernet terdiri dari frame, atau data aktual yang Anda kirim, dan informasi overhead jaringan di sekitarnya.

Frame Ethernet bisa hadir dalam format yang berbeda, dan format yang paling umum adalah format frame Ethernet v2 standar. Ini mendukung 1500 MTU, yang merupakan ukuran paket Ethernet

terbesar yang didukung di hampir seluruh internet. MTU dengan dukungan maksimum untuk suatu instans bergantung pada tipe instans-nya.

Semua jenis EC2 instans mendukung 1500 MTU.

Daftar Isi

- Frame jumbo (9001 MTU)
- Path MTU Discovery
- Mengatur MTU untuk instans Amazon EC2 Anda
- Pemecahan Masalah

Frame jumbo (9001 MTU)

Dengan jumbo frame, Anda dapat meningkatkan ukuran payload per paket, sehingga meningkatkan persentase paket yang bukan paket overhead. Dengan bingkai jumbo, lebih sedikit paket yang diperlukan untuk mengirim jumlah data yang dapat digunakan yang sama. Namun, jenis lalu lintas tertentu tunduk pada muatan maksimum berikut:

Batas MTU 1500 byte

- Lalu lintas melalui gateway internet
- Lalu lintas melalui koneksi VPN
- Lalu lintas antar AWS Wilayah, kecuali gateway transit digunakan

Batas MTU 8500 byte

- Lalu lintas melalui koneksi peering VPC antar wilayah

Jika paket melebihi batas MTU mereka, mereka terfragmentasi, atau mereka dijatuhkan jika `Don't Fragment` bendera diatur di header IP.

Frame Jumbo harus digunakan dengan hati-hati untuk lalu lintas internet-bound atau setiap lalu lintas yang meninggalkan VPC. Paket difragmentasi oleh sistem menengah, yang memperlambat lalu lintas ini. Untuk menggunakan frame jumbo di dalam VPC dan tidak memperlambat lalu lintas yang terikat di luar VPC, Anda dapat mengonfigurasi ukuran MTU berdasarkan rute, atau menggunakan beberapa antarmuka elastic network dengan ukuran MTU yang berbeda dan rute yang berbeda.

Untuk instans-instans dengan lokasi sama dalam grup penempatan klaster, bingkai jumbo membantu mencapai throughput jaringan semaksimum mungkin, dan dianjurkan dalam kasus ini. Untuk informasi selengkapnya, lihat Grup penempatan untuk EC2 instans Amazon Anda.

Anda dapat menggunakan bingkai jumbo untuk lalu lintas antara jaringan lokal Anda VPCs dan jaringan lokal Anda. Direct ConnectUntuk informasi selengkapnya, dan cara memverifikasi kemampuan Jumbo Frame, lihat MTU untuk antarmuka virtual pribadi atau antarmuka virtual transit di Panduan Pengguna.Direct Connect

Semua jenis instans generasi saat ini mendukung bingkai jumbo. Jenis instans generasi sebelumnya berikut mendukung bingkai jumbo: A1, C3, I2, M3, dan R3.

Sumber daya terkait

- Untuk gateway NAT, lihat Dasar-dasar gateway NAT di Panduan Pengguna Amazon VPC.
- Untuk gateway transit, lihat Unit transmisi maksimum di Panduan Pengguna Gerbang Transit VPC Amazon.
- Untuk Local Zones, lihat Pertimbangan di Panduan Pengguna AWS Local Zones.
- Untuk AWS Wavelength, lihat Unit transmisi maksimum di Panduan AWS Wavelength Pengguna.
- Untuk Outposts lihat Layanan menautkan persyaratan unit transmisi maksimum di AWS Outposts Panduan Pengguna.

Path MTU Discovery

Penemuan MTU Jalur (PMTUD) digunakan untuk menentukan jalur MTU antara dua perangkat. Jalur MTU adalah ukuran paket maksimum yang didukung pada jalur antara host asal dan host penerima. Ketika ada perbedaan dalam ukuran MTU dalam jaringan antara dua host, PMTUD memungkinkan host penerima untuk menanggapi host asal dengan pesan ICMP. Pesan ICMP ini menginstruksikan host asal untuk menggunakan ukuran MTU terendah di sepanjang jalur jaringan dan untuk mengirim ulang permintaan. Tanpa negosiasi ini, paket drop dapat terjadi karena permintaan terlalu besar untuk diterima oleh host penerima.

Sebab IPv4, ketika host mengirim paket yang lebih besar dari MTU host penerima atau yang lebih besar dari MTU perangkat di sepanjang jalur, host penerima atau perangkat menjatuhkan paket, dan kemudian mengembalikan pesan ICMP berikut: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipe 3, Kode 4). Ini menginstruksikan host transmisi untuk membagi muatan menjadi beberapa paket yang lebih kecil, dan kemudian mentrasmisikannya kembali.

IPv6 Protokol tidak mendukung fragmentasi dalam jaringan. Jika suatu host mengirimkan paket yang lebih besar daripada MTU host penerima atau yang lebih besar daripada MTU perangkat di sepanjang jalur, host atau perangkat penerima menjatuhkan paket, lalu mengembalikan pesan ICMP berikut: `ICMPv6 Packet Too Big (PTB)` (Tipe 2). Ini menginstruksikan host transmisi untuk membagi muatan menjadi beberapa paket yang lebih kecil, dan kemudian mentrasmisikannya kembali.

Koneksi yang dilakukan melalui beberapa komponen, seperti gateway NAT dan penyeimbang beban, secara otomatis dilacak. Ini berarti bahwa pelacakan grup keamanan diaktifkan secara otomatis untuk upaya koneksi keluar Anda. Jika koneksi dilacak secara otomatis atau jika aturan grup keamanan Anda mengizinkan lalu lintas ICMP masuk, Anda dapat menerima respons PMTUD.

Perhatikan bahwa lalu lintas ICMP dapat diblokir bahkan jika lalu lintas diizinkan di tingkat grup keamanan, seperti jika Anda memiliki entri daftar kontrol akses jaringan yang menolak lalu lintas ICMP ke subnet.

> **Important**
>
> Path MTU Discovery tidak menjamin bahwa frame jumbo tidak akan diturunkan oleh beberapa router. Gateway internet di VPC Anda akan meneruskan paket hingga 1500 byte saja. 1500 paket MTU direkomendasikan untuk lalu lintas internet.

Untuk aturan MTU mengenai gateway NAT, lihat Unit transmisi maksimum (MTU) di Panduan Pengguna Amazon VPC. Untuk aturan MTU mengenai gateway Transit, lihat Unit transmisi maksimum (MTU) di Panduan Pengguna Gateway AWS Transit.

Mengatur MTU untuk instans Amazon EC2 Anda

Maximum transmission unit (MTU) dari koneksi jaringan adalah ukuran, dalam byte, dari paket terbesar yang dapat diizinkan yang dapat dilewatkan melalui koneksi. Semua EC2 instans Amazon mendukung frame standar (1500 MTU) dan semua jenis instans generasi saat ini mendukung jumbo frame (9001 MTU).

Anda dapat melihat MTU untuk EC2 instans Amazon, melihat jalur MTU antara instans Anda dan host lain, dan mengonfigurasi instans Anda untuk menggunakan bingkai standar atau jumbo.

Tugas

- Periksa MTU jalur di antara dua host

- Periksa MTU untuk contoh Anda
- Tetapkan MTU untuk instans Anda

Periksa MTU jalur di antara dua host

Anda dapat memeriksa jalur MTU antara EC2 instans Anda dan host lain. Anda dapat menentukan nama DNS atau alamat IP sebagai tujuan. Jika tujuan adalah EC2 contoh lain, verifikasi bahwa grup keamanannya memungkinkan lalu lintas UDP masuk.

Prosedur yang Anda gunakan tergantung pada sistem operasi instance.

Instans Linux

Jalankan tracepath perintah pada instance Anda untuk memeriksa jalur MTU antara EC2 instance Anda dan tujuan yang ditentukan. Perintah ini adalah bagian dari `iputils` paket, yang tersedia secara default di banyak distribusi Linux.

Contoh ini memeriksa jalur MTU antara EC2 instance dan`amazon.com`.

```
[ec2-user ~]$ tracepath amazon.com
```

Dalam contoh output ini, jalur MTU adalah 1500.

```
 1?: [LOCALHOST]     pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  100.64.16.241 (100.64.16.241)                              0.574ms
 5:  72.21.222.221 (72.21.222.221)                             84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                           79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                             96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                             79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                           91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

Instans Windows

Untuk memeriksa jalur MTU menggunakan mturoute

1. Unduh mturoute.exe ke EC2 instance Anda dari https://elifulkerson.com/projects/mturoute.php.
2. Buka jendela Command Prompt dan ubah ke direktori untuk mengunduh mturoute.exe.
3. Gunakan perintah berikut untuk memeriksa jalur MTU antara EC2 instance Anda dan tujuan yang ditentukan. Contoh ini memeriksa jalur MTU antara EC2 instance dan`www.elifulkerson.com`.

   ```
   .\mturoute.exe www.elifulkerson.com
   ```

   Dalam contoh output ini, jalur MTU adalah 1500.

   ```
   * ICMP Fragmentation is not permitted. *
   * Speed optimization is enabled. *
   * Maximum payload is 10000 bytes. *
   + ICMP payload of 1472 bytes succeeded.
   - ICMP payload of 1473 bytes is too big.
   Path MTU: 1500 bytes.
   ```

Periksa MTU untuk contoh Anda

Anda dapat memeriksa nilai MTU untuk instance Anda. Beberapa instans dikonfigurasi untuk menggunakan frame jumbo, dan lainnya dikonfigurasi untuk menggunakan ukuran frame standar.

Prosedur yang Anda gunakan tergantung pada sistem operasi instance.

Instans Linux

Untuk memeriksa pengaturan MTU di instans Linux

Jalankan ip perintah berikut pada EC2 instance Anda. Jika antarmuka jaringan utama tida`eth0`, ganti `eth0` dengan antarmuka jaringan Anda.

```
[ec2-user ~]$ ip link show eth0
```

Dalam contoh output ini, `mtu 9001` menunjukkan bahwa instance menggunakan jumbo frame.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
 DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

Instans Windows

Prosedur yang Anda gunakan tergantung pada driver pada instance Anda.

ENA driver

Versi 2.1.0 dan yang lebih baru

Untuk mendapatkan nilai MTU, gunakan Get-NetAdapterAdvancedProperty perintah berikut pada EC2 instance Anda. Gunakan wildcard (tanda bintang) untuk mendapatkan semua nama Ethernet. Periksa output untuk nama antarmuka`*JumboPacket`. Nilai 9015 menunjukkan bahwa bingkai Jumbo diaktifkan. Bingkai jumbo dinonaktifkan secara default.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Versi 1.5 dan sebelumnya

Untuk mendapatkan nilai MTU, gunakan Get-NetAdapterAdvancedProperty perintah berikut pada EC2 instance Anda. Periksa output untuk nama antarmuka`MTU`. Nilai 9001 menunjukkan bahwa bingkai Jumbo diaktifkan. Bingkai jumbo dinonaktifkan secara default.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Untuk mendapatkan nilai MTU, gunakan Get-NetAdapterAdvancedProperty perintah berikut pada EC2 instance Anda. Periksa entri untuk nama antarmuka `*JumboPacket`. Nilai 9014 menunjukkan bahwa bingkai Jumbo diaktifkan. (Perhatikan bahwa ukuran MTU mencakup header dan muatan.) Bingkai jumbo dinonaktifkan secara default.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Untuk mendapatkan nilai MTU, gunakan perintah berikut pada EC2 instance Anda. Nama antarmuka dapat bervariasi. Dalam output, cari entri dengan nama "Ethernet," "Ethernet 2," atau

"Local Area Connection". Anda akan memerlukan nama antarmuka untuk mengaktifkan atau menonaktifkan frame jumbo. Nilai 9001 menunjukkan bahwa bingkai Jumbo diaktifkan.

```
netsh interface ipv4 show subinterface
```

Tetapkan MTU untuk instans Anda

Anda mungkin ingin menggunakan bingkai jumbo untuk lalu lintas jaringan dalam VPC Anda dan bingkai standar untuk lalu lintas internet. Apa pun kasus penggunaan Anda, kami sarankan Anda memverifikasi bahwa instance Anda berperilaku seperti yang diharapkan.

Prosedur yang Anda gunakan tergantung pada sistem operasi instance.

Instans Linux

Untuk mengatur nilai MTU di instans Linux

1. Jalankan ip perintah berikut pada instance Anda. Ini menetapkan nilai MTU yang diinginkan ke 1500, tetapi Anda bisa menggunakan 9001 sebagai gantinya. Jika antarmuka jaringan utama tidak`eth0`, ganti `eth0` dengan antarmuka jaringan yang sebenarnya.

   ```
   [ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
   ```

2. (Opsional) Untuk mempertahankan pengaturan MTU jaringan Anda setelah reboot, modifikasi file konfigurasi berikut berdasarkan tipe sistem operasi Anda.

   - Amazon Linux 2023 - Ubah `[Link]` bagian file konfigurasi. File konfigurasi default adalah`/usr/lib/systemd/network/80-ec2.network`, atau Anda dapat memperbarui file konfigurasi khusus yang dibuat di/run/systemd/network/, di mana nama file adalah *priority* - *interface* .network. Untuk informasi selengkapnya, lihat Layanan jaringan di dokumentasi Amazon Linux.

     ```
     MTUBytes=1500
     ```

   - Amazon Linux 2 - Tambahkan baris berikut ke `/etc/sysconfig/network-scripts/ifcfg-eth0` file:

     ```
     MTU=1500
     ```

Tambahkan baris berikut ke file `/etc/dhcp/dhclient.conf`:

```
request subnet-mask, broadcast-address, time-offset, routers, domain-name,
 domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
servers;
```

- Distribusi Linux lainnya - Konsultasikan dokumentasi spesifik mereka.

3. (Opsional) Reboot instans Anda dan verifikasi bahwa pengaturan MTU benar.

Instans Windows

Prosedur yang Anda gunakan tergantung pada driver pada instance Anda.

ENA driver

Anda dapat mengubah MTU menggunakan Device Manager atau Set-NetAdapterAdvancedProperty perintah pada instance Anda.

Versi 2.1.0 dan yang lebih baru

Gunakan perintah berikut untuk mengaktifkan bingkai jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Gunakan perintah berikut untuk menonaktifkan bingkai jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Versi 1.5 dan sebelumnya

Gunakan perintah berikut untuk mengaktifkan bingkai jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Gunakan perintah berikut untuk menonaktifkan bingkai jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

Anda dapat mengubah MTU menggunakan Device Manager atau Set-NetAdapterAdvancedProperty perintah pada instance Anda.

Gunakan perintah berikut untuk mengaktifkan bingkai jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Gunakan perintah berikut untuk menonaktifkan bingkai jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

Anda dapat mengubah MTU menggunakan netsh perintah pada instance Anda. Anda tidak dapat mengubah MTU menggunakan Device Manager.

Gunakan perintah berikut untuk mengaktifkan bingkai jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Gunakan perintah berikut untuk menonaktifkan bingkai jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Pemecahan Masalah

Jika Anda mengalami masalah konektivitas antara EC2 instans dan klaster Amazon Redshift saat menggunakan bingkai jumbo, lihat Kueri tampak hang dan terkadang gagal menjangkau klaster di Panduan Manajemen Pergeseran Merah Amazon.

Virtual private cloud untuk EC2 instans Anda

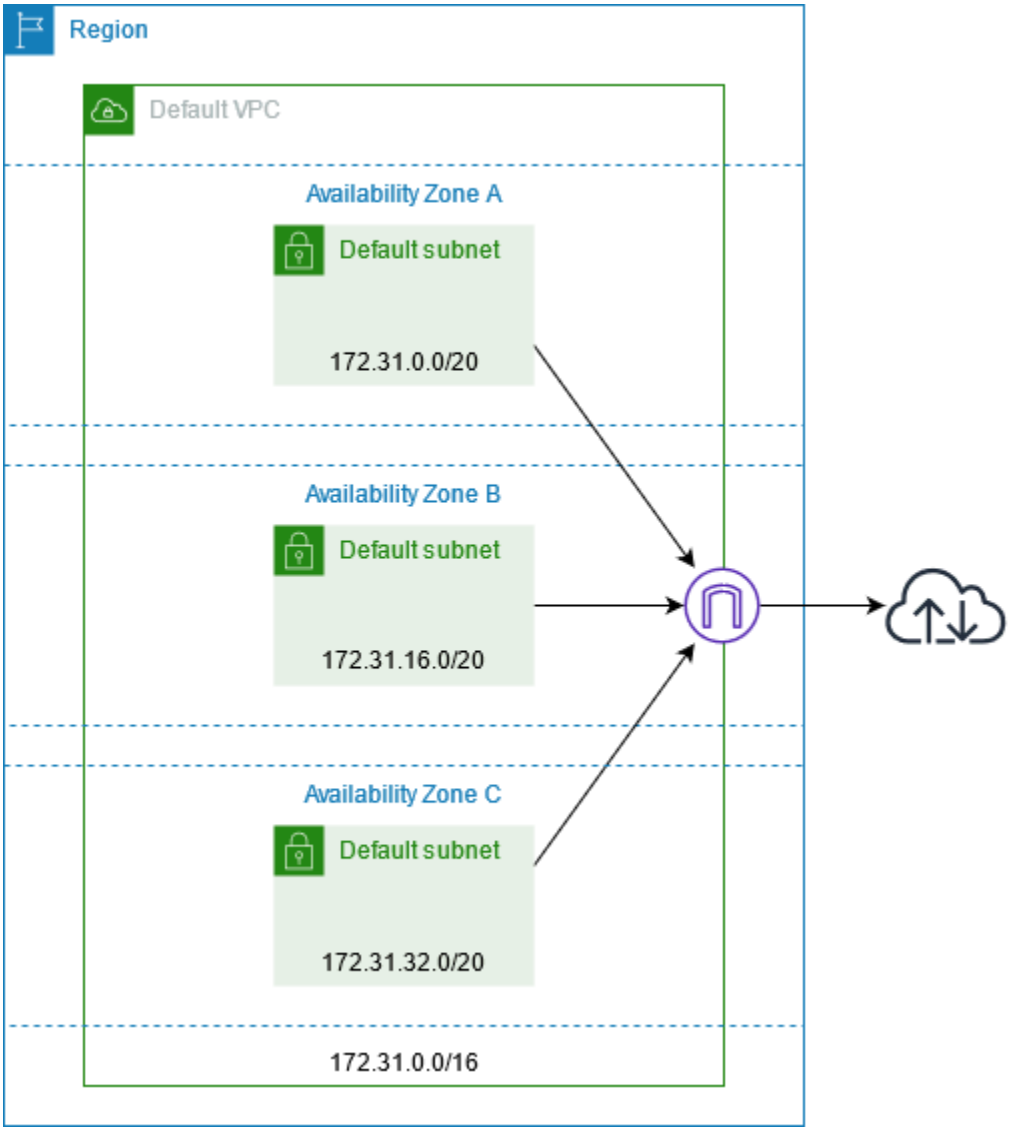
Amazon Virtual Private Cloud (Amazon VPC) memungkinkan Anda untuk menentukan jaringan virtual di area Anda sendiri yang terisolasi secara logis di dalam AWS cloud, yang dikenal sebagai cloud pribadi virtual atau VPC. Anda dapat membuat AWS sumber daya, seperti EC2 instans Amazon, ke dalam subnet VPC Anda. VPC Anda sangat menyerupai jaringan tradisional yang mungkin Anda operasikan di pusat data Anda sendiri, dengan memanfaatkan infrastruktur terukur dari AWS. Anda dapat mengonfigurasi VPC Anda; Anda dapat memilih rentang alamat IP, membuat subnet, dan mengonfigurasi tabel rute, gateway jaringan, dan pengaturan keamanan. Anda dapat menghubungkan instans dalam VPC ke internet atau ke pusat data Anda sendiri.

Daftar Isi

- Default Anda VPCs
- Tidak default VPCs
- Akses internet
- Subnet bersama
- IPv6-hanya subnet

Default Anda VPCs

Saat Anda membuat AWS akun, kami membuat VPC default di setiap Wilayah. VPC default adalah VPC yang sudah dikonfigurasi dan siap untuk Anda gunakan. Misalnya, ada subnet default untuk setiap Zona Ketersediaan di setiap VPC default, gateway internet yang terpasang ke VPC, dan ada rute di tabel rute utama yang mengirimkan semua lalu lintas (0.0.0.0/0) ke gateway internet. Anda dapat memodifikasi konfigurasi default Anda VPCs sesuai kebutuhan. Misalnya, Anda dapat menambahkan subnet dan tabel rute.



Tidak default VPCs

Alih-alih menggunakan VPC default untuk sumber daya Anda, Anda dapat membuat VPC Anda sendiri, seperti yang dijelaskan dalam Buat VPC di Panduan Pengguna Amazon VPC.

Berikut adalah beberapa hal yang perlu dipertimbangkan saat membuat VPC untuk instance Anda EC2 .

- Anda dapat menggunakan saran default untuk blok IPv4 CIDR atau memasukkan blok CIDR yang diperlukan oleh aplikasi atau jaringan Anda.
- Untuk memastikan ketersediaan tinggi, buat subnet di beberapa Availability Zone.
- Jika instans Anda harus dapat diakses dari internet, lakukan salah satu hal berikut:

- Jika instans Anda dapat berada di subnet publik, tambahkan subnet publik. Biarkan kedua opsi DNS diaktifkan. Anda dapat menambahkan subnet privat secara opsional sekarang atau nanti.
- Jika instans Anda harus dalam subnet pribadi, tambahkan hanya subnet pribadi. Anda dapat menambahkan gateway NAT untuk menyediakan akses internet ke instance di subnet pribadi. Jika instans Anda mengirim atau menerima volume lalu lintas yang signifikan di seluruh Availability Zone, buat gateway NAT di setiap Availability Zone. Jika tidak, Anda dapat membuat gateway NAT hanya di salah satu Availability Zones dan meluncurkan instance yang mengirim atau menerima lalu lintas lintas zona di Availability Zone yang sama dengan gateway NAT.

Akses internet

Instans yang diluncurkan ke subnet default di VPC default memiliki akses ke internet, karena default VPCs dikonfigurasi untuk menetapkan alamat IP publik dan nama host DNS, dan tabel rute utama dikonfigurasi dengan rute ke gateway internet yang dilampirkan ke VPC.

Untuk contoh yang Anda luncurkan di subnet nondefault dan VPCs, Anda dapat menggunakan salah satu opsi berikut untuk memastikan bahwa instance yang Anda luncurkan di subnet ini memiliki akses ke internet:

- Konfigurasi gateway internet. Untuk informasi selengkapnya, lihat Hubungkan ke internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.
- Konfigurasi gateway NAT publik. Untuk informasi selengkapnya, lihat Mengakses internet dari subnet privat di Panduan Pengguna Amazon VPC.

Subnet bersama

Saat meluncurkan EC2 instance ke subnet VPC bersama, perhatikan hal berikut:

- Peserta dapat menjalankan instance di subnet bersama dengan menentukan ID subnet bersama. Peserta harus memiliki antarmuka jaringan apa pun yang mereka tentukan.
- Peserta dapat memulai, menghentikan, menghentikan, dan menjelaskan contoh yang telah mereka buat di subnet bersama. Peserta tidak dapat memulai, menghentikan, menghentikan, atau menjelaskan contoh yang dibuat oleh pemilik VPC di subnet bersama.
- Pemilik VPC tidak dapat memulai, menghentikan, menghentikan, atau menjelaskan instance yang dibuat oleh peserta dalam subnet bersama.

- Peserta dapat terhubung ke instance di subnet bersama menggunakan EC2 Instance Connect Endpoint. Peserta harus membuat Titik Akhir EC2 Instance Connect di subnet bersama. Peserta tidak dapat menggunakan Titik Akhir EC2 Instance Connect yang dibuat oleh pemilik VPC di subnet bersama.

Untuk informasi tentang EC2 sumber daya Amazon bersama, lihat berikut ini:

- the section called “Kelola berbagi AMI dengan organisasi atau OU”
- the section called “Reservasi Kapasitas Bersama”
- the section called “Grup penempatan bersama”
- Berbagi Host Khusus Amazon EC2 lintas akun

Untuk informasi selengkapnya tentang subnet bersama, lihat Bagikan VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.

IPv6-hanya subnet

EC2 Instance yang diluncurkan di subnet IPv6 -only menerima IPv6 alamat tetapi bukan alamat. IPv4 Setiap instance yang Anda luncurkan ke subnet IPv6 -only harus instance berbasis Nitro.

Jaringan Sekunder

Secondary Networks adalah jaringan virtual yang dibangun khusus untuk kasus penggunaan jaringan khusus. Jaringan ini secara logis terisolasi dalam partisi AWS cloud. Anda dapat membuat sumber daya seperti subnet sekunder dalam jaringan sekunder Anda. Jaringan sekunder digabungkan erat dengan Amazon VPCs, sehingga instance tertentu multi-homed dan diluncurkan ke VPC dan Jaringan Sekunder.

Jaringan Sekunder saat ini tersedia untuk jenis instans tertentu dan melalui reservasi kapasitas dengan komitmen jangka panjang. Silakan hubungi tim akun Anda untuk informasi lebih lanjut jika menurut Anda jaringan sekunder mungkin bermanfaat bagi beban kerja Anda.

Daftar Isi

- Apa itu Jaringan Sekunder?
- Konsep utama
- Arsitektur

- Pertimbangan tambahan
- Memulai
- Mengelola sumber daya Jaringan Sekunder
- Praktik terbaik desain jaringan
- Pemecahan masalah
- Kuota dan batas

Apa itu Jaringan Sekunder?

Secondary Networks menyediakan jaringan logis dan terisolasi, digunakan dalam kombinasi dengan jaringan VPC, sehingga instance multi-homed menjadi dua jaringan independen. Manfaat jaringan sekunder meliputi:

- Jaringan berkinerja tinggi untuk kasus penggunaan khusus dan protokol seperti konektivitas timur-barat untuk beban kerja ML
- Dukungan multi-penyewa dengan isolasi logis
- Instans terintegrasi dengan mulus dengan VPCs dan layanan AWS

Konsep utama

Jaringan Sekunder

Konstruksi jaringan regional yang menyediakan jaringan Layer 3 logis dengan blok IPv4 CIDR (mulai dari /28 hingga /12). Jaringan Sekunder beroperasi secara independen dari VPCs infrastruktur jaringan yang dipartisi secara fisik.

Subnet Sekunder

Konstruksi khusus Zona Ketersediaan dalam Jaringan Sekunder, mirip dengan subnet VPC. Subnet Sekunder mendukung blok CIDR mulai dari /28 hingga /12.

Antarmuka Sekunder

Antarmuka jaringan yang terpasang pada kartu jaringan sekunder, menyediakan konektivitas timur-barat dalam subnet sekunder. Antarmuka ini secara fisik dan logis terpisah dari Elastic Network Interfaces ()ENIs.

Arsitektur

Instans EC2 yang mendukung Jaringan Sekunder bersifat multi-homed, yang berarti mereka dapat berkomunikasi dalam VPC dan Jaringan Sekunder secara bersamaan:

- VPC: Menyediakan TCP/IP konektivitas utara-selatan ke AWS layanan, penyimpanan, database, layanan jaringan, dan internet
- Jaringan Sekunder: Menyediakan konektivitas timur-barat antara instance khusus yang didukung

Pertimbangan tambahan

- Antarmuka sekunder dikelola melalui RunInstances dan mereka tidak dapat dibuat atau dihapus secara independen.
- Antarmuka sekunder tidak dapat dilakukan attached/detached setelah instance diluncurkan.
- Antarmuka sekunder Alamat IP tidak dapat diubah setelah diluncurkan.
- Fitur VPC seperti Grup Keamanan, NACLs, Log Aliran tidak didukung di Jaringan Sekunder.

Memulai

Prasyarat

Sebelum meluncurkan instans dengan Secondary Networks, pastikan Anda juga telah mengonfigurasi VPC Anda di wilayah yang ditargetkan dan Subnet di zona ketersediaan yang ditargetkan dari kapasitas EC2 Anda.

Langkah 1: Buat Jaringan Sekunder

Buat Jaringan Sekunder di wilayah yang sama dengan VPC Anda. Ini adalah sumber daya regional yang menyediakan isolasi logis untuk lalu lintas RDMA Anda.

```
aws ec2 create-secondary-network \
  --network-type rdma \
  --ipv4-cidr-block 172.31.0.0/16 \
  --region us-east-2
```

Parameter:

- `--network-type`: Jenis jaringan (saat ini hanya rdma yang didukung)

- `--ipv4-cidr-block`: Blok IPv4 CIDR antara /28 dan /12
- `--region`: AWS Wilayah (AS-Timur-2)

> **Note**
>
> Praktik Terbaik: Pilih blok CIDR yang tidak tumpang tindih dengan CIDR VPC Anda untuk menyederhanakan perutean di tingkat instans.

Langkah 2: Buat Subnet Sekunder

Buat Subnet Sekunder di zona ketersediaan yang sama dengan subnet VPC Anda. Ini adalah sumber daya khusus AZ.

```
aws ec2 create-secondary-subnet \
  --secondary-network-id sn-1234567890abcdef0 \
  --ipv4-cidr-block 172.31.24.0/24 \
  --availability-zone us-east-2a
```

> **Note**
>
> Reservasi Alamat IP: Seperti subnet VPC, Amazon menyimpan 4 alamat IP pertama dan alamat IP terakhir di setiap Subnet Sekunder untuk penggunaan internal.

Langkah 3: Luncurkan instans

Luncurkan instance ke subnet VPC Anda dan Subnet Sekunder. Instans akan multi-homed dengan konektivitas ke kedua jaringan.

```
aws ec2 run-instances \
  --image-id ami-12345678 \
  --count 1 \
  --instance-type <instance> \
  --key-name MyKeyPair \
  --instance-market-options '{"MarketType": "capacity-block"}' \
  --capacity-reservation-specification '{"CapacityReservationTarget": \
  {"CapacityReservationId": "cr-1234567890abcdef0"}}' \
  --network-interfaces \
```

```
    "NetworkCardIndex=0,DeviceIndex=0,Groups=sg-12345678,\
    SubnetId=subnet-0987654321fedcba0,InterfaceType=interface" \
  --secondary-interfaces \
    "NetworkCardIndex=1,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=2,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=3,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=4,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=5,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=6,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=7,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=8,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true"
```

Parameter kunci:

- `--network-interfaces`: Menentukan Nitro ENI utama untuk konektivitas VPC (Indeks Kartu Jaringan 0)
- `--secondary-interfaces`: Menentukan 8 antarmuka sekunder untuk konektivitas timur-barat dalam Subnet Sekunder (Indeks Kartu Jaringan 1-8)
- `InterfaceType=secondary`: Menunjukkan Antarmuka Sekunder

Mengelola sumber daya Jaringan Sekunder

Menggambarkan Jaringan Sekunder

Lihat detail tentang Jaringan Sekunder Anda:

```
aws ec2 describe-secondary-networks \
  --secondary-network-id sn-1234567890abcdef0
```

Menggambarkan Subnet Sekunder

Lihat detail tentang Subnet Sekunder Anda:

```
aws ec2 describe-secondary-subnets \
  --secondary-subnet-id ss-98765421yxz
```

Menjelaskan Antarmuka Sekunder

Lihat detail tentang Antarmuka Jaringan Sekunder yang dilampirkan ke instans Anda:

```
aws ec2 describe-secondary-interfaces \
  --filters "Name=attachment.instance-id,Values=i-1234567890abcdef0"
```

Menghapus sumber daya

Hapus Subnet Sekunder:

```
aws ec2 delete-secondary-subnet \
  --secondary-subnet-id ss-98765421yxz
```

Hapus Jaringan Sekunder:

```
aws ec2 delete-secondary-network \
  --secondary-network-id sn-1234567890abcdef0
```

> **Important**
>
> Anda harus menghentikan semua instance dan menghapus semua Subnet Sekunder sebelum menghapus Jaringan Sekunder.

Praktik terbaik desain jaringan

Perencanaan CIDR

Hindari Tumpang tindih CIDRs: Sementara Jaringan Sekunder secara fisik terisolasi dari VPCs, menggunakan blok CIDR yang tidak tumpang tindih menyederhanakan konfigurasi routing pada tingkat sistem operasi instance.

> **Note**
>
> Amazon mencadangkan 5 alamat IP per subnet.

Pemisahan lalu lintas

Memisahkan berdasarkan Jaringan Sekunder: Buat Jaringan Sekunder terpisah untuk proyek, tim, atau batas keamanan yang berbeda. Jaringan Sekunder memberikan isolasi logis antar instance. Instance tidak dapat berkomunikasi di berbagai Jaringan Sekunder.

Gunakan Beberapa Subnet: Dalam Jaringan Sekunder, gunakan beberapa Subnet Sekunder untuk mengelompokkan lalu lintas menurut indeks GPU, zona ketersediaan, atau jenis beban kerja. Sebagai contoh, pola arsitektur umum adalah untuk menyebarkan jaringan sekunder tunggal dengan 4 atau 8 subnet sekunder, di mana setiap subnet sekunder disejajarkan dengan sekelompok GPUs indeks umum.

Pemecahan masalah

Kegagalan peluncuran instans

Masalah: Instance gagal diluncurkan dengan antarmuka Jaringan Sekunder.

Solusi:

- Verifikasi bahwa AMI Anda menyertakan dukungan driver yang tepat
- Pastikan Subnet Sekunder Anda memiliki alamat IP yang cukup tersedia
- Konfirmasikan bahwa reservasi kapasitas Anda dalam status “aktif”
- Periksa apakah Subnet Sekunder Anda berada di zona ketersediaan yang sama dengan subnet VPC Anda

Masalah konektivitas

Masalah: Tidak dapat membuat konektivitas RDMA antar instance.

Solusi:

- Verifikasi bahwa semua instance berada di Jaringan Sekunder dan Subnet Sekunder yang sama
- Periksa apakah driver antarmuka sekunder dimuat dengan benar pada instance
- Pastikan aplikasi Anda mengikat ke antarmuka jaringan yang benar
- Instans dalam subnet sekunder yang sama dapat dicapai melalui rute langsung. Komunikasi lintas subnet tersedia melalui rute statis yang dijual melalui DHCP.

Kesalahan API

Masalah: Panggilan API untuk Jaringan Sekunder dan operasi Subnet Sekunder gagal.

Solusi:

- Verifikasi izin IAM untuk ec2:CreateSecondaryNetwork, ec2:, dll. CreateSecondarySubnet
- Periksa apakah blok CIDR berada dalam kisaran yang didukung (/28 hingga /12)
- Verifikasi bahwa Anda menggunakan wilayah dan zona ketersediaan yang benar

Kuota dan batas

Untuk meminta kenaikan kuota, gunakan AWS Service Quotas atau hubungi AWS Support.

Kuota dan batas Jaringan Sekunder

Sumber daya	Kuota	Dapat Disesuaikan
Jaringan Sekunder per wilayah	5	Ya
Subnet Sekunder untuk Jaringan Sekunder	200	Ya
Ukuran blok CIDR	/28 ke /12	Tidak

Keamanan dalam Amazon EC2

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon EC2, lihat AWS Layanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan dalam Lingkup oleh Program .
- Keamanan dalam cloud – Tanggung jawab Anda meliputi area-area berikut:
  - Mengontrol akses jaringan pada instans Anda, misalnya, dengan mengonfigurasi VPC dan grup keamanan Anda. Untuk informasi selengkapnya, lihat Mengontrol lalu lintas jaringan.
  - Mengelola kredensial yang digunakan untuk terhubung ke instans Anda.
  - Mengelola sistem operasi tamu dan perangkat lunak yang diterapkan ke sistem operasi tamu, termasuk pembaruan dan patch keamanan. Untuk informasi selengkapnya, lihat Manajemen pembaruan untuk instans Amazon EC2.
  - Mengonfigurasi IAM role yang dilampirkan pada instans dan izin yang dikaitkan peran tersebut. Untuk informasi selengkapnya, lihat IAM role untuk Amazon EC2.

Dokumentasi ini akan membantu Anda dalam memahami cara menerapkan model tanggung jawab bersama saat Anda menggunakan Amazon EC2. Dokumentasi tersebut juga menunjukkan kepada Anda cara mengonfigurasi Amazon EC2 untuk memenuhi tujuan-tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Amazon EC2 Anda.

Daftar Isi

- Perlindungan data dalam Amazon EC2
- Keamanan infrastruktur di Amazon EC2
- Ketahanan dalam Amazon EC2

- Validasi kepatuhan untuk Amazon EC2
- Manajemen identitas dan akses untuk Amazon EC2
- Manajemen pembaruan untuk instans Amazon EC2
- Praktik terbaik keamanan untuk instans Windows
- Pasangan kunci Amazon EC2 dan instans Amazon EC2
- Grup keamanan Amazon EC2 untuk instans EC2 Anda
- NitroTPM untuk instans Amazon EC2
- Pengesahan instans Amazon EC2
- Credential Guard untuk instance Windows
- Mengakses Amazon EC2 menggunakan titik akhir VPC antarmuka

Perlindungan data dalam Amazon EC2

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon Elastic Compute Cloud. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.

- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon EC2 atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau. AWS SDKs Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Daftar Isi

- Keamanan data Amazon EBS
- Enkripsi saat tidak aktif
- Enkripsi saat bergerak

Keamanan data Amazon EBS

Volume Amazon EBS disajikan kepada Anda sebagai perangkat blok mentah yang tidak terformat. Perangkat-perangkat ini adalah perangkat logis yang dibuat pada infrastruktur EBS dan layanan Amazon EBS akan memastikan bahwa perangkat-perangkat tersebut secara logis kosong (yakni bahwa, blok mentah tersebut sudah dikosongkan atau mengandung data pseudorandom secara kriptografis) sebelum digunakan atau digunakan kembali oleh pelanggan.

Jika Anda memiliki prosedur yang mengharuskan semua data dihapus menggunakan metode tertentu, baik setelah atau sebelum digunakan (atau keduanya), seperti yang dirinci dalam DoD 5220.22-M (Manual Operasi Program Keamanan Industri Nasional) atau NIST 800-88(Pedoman untuk Sanitisasi Media), Anda memiliki kemampuan untuk melakukannya di Amazon EBS. Aktivitas tingkat blok tersebut akan tercermin ke media penyimpanan yang mendasarinya dalam layanan Amazon EBS tersebut.

Enkripsi saat tidak aktif

Volume EBS

Enkripsi Amazon EBS adalah solusi enkripsi untuk volume dan snapshot EBS Anda. Ia menggunakan AWS KMS keys. Untuk informasi selengkapnya, lihat enkripsi Amazon EBS di Panduan Pengguna Amazon EBS.

[Instans Windows] Anda juga dapat menggunakan izin Microsoft EFS dan NTFS untuk enkripsi tingkat folder dan file.

Volume penyimpanan instans

Data pada volume penyimpanan NVMe instance dienkripsi menggunakan cipher XTS-AES-256, diimplementasikan pada modul perangkat keras pada instance. Kunci yang digunakan untuk mengenkripsi data yang ditulis ke perangkat NVMe penyimpanan yang terpasang secara lokal adalah per pelanggan, dan per volume. Kunci yang dihasilkan oleh, dan yang hanya berada di dalam, modul perangkat keras, yang tidak dapat diakses personil AWS . Kunci enkripsi tersebut akan dihancurkan saat instans dihentikan atau diakhiri dan tidak dapat dipulihkan. Anda tidak akan dapat menonaktifkan enkripsi ini dan Anda juga tidak dapat menyediakan kunci enkripsi Anda sendiri.

Data pada volume penyimpanan instans HDD pada instans H1, D3, dan D3en dienkripsi menggunakan XTS-AES-256 dan kunci sekali pakai.

Saat Anda menghentikan, melakukan hibernasi, atau mengakhiri instans, setiap blok penyimpanan dalam volume penyimpanan instans akan diatur ulang. Oleh karena itu, data Anda tidak dapat diakses melalui penyimpanan instans dari instans yang lain.

Memori

Enkripsi memori diaktifkan pada instans-instans berikut:

- Instans dengan AWS Graviton2 atau prosesor Graviton yang lebih baru mendukung AWS enkripsi memori yang selalu aktif. Kunci enkripsi yang secara aman dihasilkan dalam sistem host, tidak meninggalkan sistem host, dan akan hancur ketika host tersebut di-reboot atau dimatikan. Untuk informasi lainnya, lihat Prosesor AWS Graviton.
- Instans dengan prosesor Intel Xeon Scalable generasi ke-3 (Ice Lake), seperti instans M6i, dan prosesor Intel Xeon Scalable generasi ke-4 (Sapphire Rapids), seperti instans M7i. Prosesor-prosesor ini mendukung enkripsi memori yang selalu aktif menggunakan Intel Total Memory Encryption (TME).

- Instans dengan prosesor AMD EPYC generasi ke-3 (Milan), seperti instans M6a, dan prosesor AMD EPYC generasi ke-4 (Genoa), seperti instans M7a. Prosesor ini mendukung enkripsi memori yang selalu aktif menggunakan AMD Secure Memory Encryption (SME).
- AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) didukung untuk beberapa jenis instans berbasis AMD. Untuk informasi selengkapnya, lihat Temukan jenis EC2 instans yang mendukung AMD SEV-SNP.

Enkripsi saat bergerak

Enkripsi pada lapisan fisik

Semua data yang mengalir di seluruh AWS Wilayah melalui jaringan AWS global secara otomatis dienkripsi pada lapisan fisik sebelum meninggalkan fasilitas yang AWS aman. Semua lalu lintas di antaranya AZs dienkripsi. Lapisan-lapisan enkripsi tambahan, termasuk yang tercantum dalam bagian ini, dapat memberikan perlindungan tambahan.

Enkripsi disediakan oleh peering VPC Amazon dan pengintipan lintas wilayah Gateway Transit

Semua lalu lintas lintas wilayah yang menggunakan peering VPC Amazon dan peering Transit Gateway secara otomatis dienkripsi massal saat keluar dari Wilayah. Lapisan enkripsi tambahan secara otomatis disediakan di lapisan fisik untuk semua lalu lintas sebelum meninggalkan fasilitas yang AWS aman, seperti yang disebutkan sebelumnya di bagian ini.

Enkripsi antar instans

AWS menyediakan konektivitas aman dan pribadi antara instans EC2 dari semua jenis. Selain itu, beberapa tipe instans menggunakan kemampuan offload dari perangkat keras Nitro System yang mendasarinya untuk secara otomatis mengenkripsi lalu lintas dalam transit antar instans. Enkripsi ini menggunakan algoritma Authenticated Encryption with Associated Data (AEAD), dengan enkripsi 256-bit. Tidak ada dampak terhadap performa jaringan. Untuk mendukung enkripsi lalu lintas dalam transit tambahan ini antara instans, persyaratan-persyaratan berikut harus dipenuhi:

- Instans-instans tersebut menggunakan tipe instans berikut:
  - Tujuan umum: M5dn, M5n, M5Zn, M6a, M6i, M6iD, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex, M8a, M8AZN, M8g, M8GB, M8gD, M8GN, M8i, M8id, M8i-Flex, Mac-M4, Mac-M4Pro
  - Komputasi dioptimalkan: C5n, C6a, C6GN, C6i, C6id, C6in, C7a, C7g, C7gd, C7GN, C7i, C7i-flex, C8a, C8g, C8gD, C8Gn, C8i, C8id, C8i-flex

  - Memori yang dioptimalkan: R5dn, R5n, R6a, R6i, R6iD, R6iDn, R6in, R7a, R7g, R7gd, R7i, R7iZ, R8a, R8g, R8gd, R8gD, R8i, R8iD, R8i-flex, U-3tb1, U-6TB1, U-9TB1, U-12TB1, U-18tb1, U-24tb1, U7I-6TB, U7i-8tb, U7i-12tb, U7in-16TB, U7in-24TB, U7in-32TB, U7inh-32TB, X2iEDN, X2iEZN, X8g, X8AEDZ, X8i
  - Penyimpanan dioptimalkan: D3, D3en, i3en, i4G, i4i, i7i, i7ie, i8g, i8ge, iM4GN, Is4gen
  - Komputasi yang dipercepat: DL1, DL2q, F2, G4ad, G4dn, G5, G6, G6e, G6f, Gr6, Gr6f, G7e, Inf1, Inf2, P3dn, P4d, P4de, P5, P5e, P5en, P6-B200, P6-B300, P6e-, Trn1, Trn1N, Trn2, Trn2u, GB200 VT1
  - Komputasi kinerja tinggi: HPC6a, HPC6id, HPC7a, hPC7g, HPC8a
- Instans-instans tersebut berada dalam Wilayah yang sama.
- Instans berada dalam VPC atau VPCs peered yang sama, dan lalu lintas tidak melewati perangkat atau layanan jaringan virtual, seperti penyeimbang beban atau gateway transit.

Lapisan enkripsi tambahan secara otomatis disediakan di lapisan fisik untuk semua lalu lintas sebelum meninggalkan fasilitas yang AWS aman, seperti yang disebutkan sebelumnya di bagian ini.

Untuk melihat jenis instance yang mengenkripsi lalu lintas dalam transit antar instance menggunakan AWS CLI

Gunakan perintah perintah describe-instance-types berikut ini.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Enkripsi ke dan dari AWS Outposts

Outpost membuat koneksi jaringan khusus yang disebut tautan layanan ke Wilayah AWS asalnya dan, secara opsional, konektivitas pribadi ke subnet VPC yang Anda tentukan. Semua lalu lintas yang melalui koneksi tersebut sudah sepenuhnya dienkripsi. Untuk informasi selengkapnya, lihat Konektivitas melalui tautan layanan dan Enkripsi dalam transit di Panduan Pengguna AWS Outposts .

Enkripsi akses jarak jauh

Protokol SSH dan RDP menyediakan saluran komunikasi yang aman untuk akses jarak jauh ke instans Anda, baik secara langsung maupun melalui EC2 Instance Connect. Akses jarak jauh ke instans Anda menggunakan AWS Systems Manager Session Manager atau Run Command

dienkripsi menggunakan TLS 1.2, dan permintaan untuk membuat koneksi ditandatangani menggunakan SiGv4, dan diautentikasi serta diotorisasi oleh. AWS Identity and Access Management

Anda bertanggung jawab untuk menggunakan protokol enkripsi, seperti Keamanan Lapisan Pengangkutan (TLS), untuk mengenkripsi data bergerak sensitif Anda yang bergerak antara klien dan instans Amazon EC2 Anda.

(Instans Windows) Pastikan untuk hanya mengizinkan koneksi terenkripsi antara instans EC2 dan titik akhir AWS API atau layanan jaringan jarak jauh sensitif lainnya. Anda dapat menerapkan hal ini melalui grup keamanan ke luar atau aturan Windows Firewall.

Keamanan infrastruktur di Amazon EC2

Sebagai layanan terkelola, Amazon Elastic Compute Cloud dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Amazon EC2 melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Untuk informasi selengkapnya, lihat Perlindungan Infrastruktur di Pilar Keamanan — AWS Well-Architected Framework.

Isolasi jaringan

Virtual Private Cloud (VPC) adalah jaringan virtual di area Anda sendiri yang terisolasi secara logis di AWS Cloud. Gunakan terpisah VPCs untuk mengisolasi infrastruktur berdasarkan beban kerja atau entitas organisasi.

subnet adalah serangkaian alamat IP di VPC. Saat Anda meluncurkan instans, Anda meluncurkan instans tersebut ke dalam subnet dalam VPC Anda. Gunakan subnet untuk melakukan isolasi terhadap jenjang-jenjang aplikasi Anda (misalnya web, aplikasi, dan basis data) dalam satu VPC.

Gunakan subnet privat untuk instans Anda jika instan tersebut tidak dapat diakses secara langsung dari internet.

Untuk memanggil API Amazon EC2 dari VPC menggunakan alamat IP privat, gunakan AWS PrivateLink. Untuk informasi selengkapnya, lihat Mengakses Amazon EC2 menggunakan titik akhir VPC antarmuka.

Isolasi pada host fisik

Instans-instans EC2 yang beragam pada host fisik yang sama diisolasi satu sama lain seolah-olah mereka berada dalam host fisik terpisah. Hypervisor mengisolasi CPU dan memori, dan instans disediakan dalam bentuk disk virtual, bukan berupa akses ke perangkat disk mentah.

Saat Anda menghentikan atau mengakhiri instans, memori yang dialokasikan untuk instans itu dibersihkan (diatur ke nol) oleh hypervisor sebelum dialokasikan ke instans baru, dan setiap blok penyimpanan akan diatur ulang. Hal ini untuk memastikan agar data Anda tidak terekspos secara tidak sengaja ke instans lain.

Alamat MAC jaringan secara dinamis ditetapkan ke instance oleh infrastruktur AWS jaringan. Alamat IP dapat ditetapkan secara dinamis ke instans oleh infrastruktur jaringan AWS , atau ditetapkan oleh administrator EC2 melalui permintaan API terautentikasi. AWS Jaringan memungkinkan instance untuk mengirim lalu lintas hanya dari MAC dan alamat IP yang diberikan kepada mereka. Jika tidak, lalu lintas akan menurun.

Secara default, instans tidak dapat menerima lalu lintas yang tidak secara khusus ditujukan padanya. Jika Anda perlu menjalankan terjemahan alamat jaringan (NAT), perutean, atau layanan firewall pada instance Anda, Anda dapat menonaktifkan source/destination pemeriksaan antarmuka jaringan.

Mengontrol lalu lintas jaringan

Pertimbangkan opsi-opsi berikut untuk mengontrol lalu lintas jaringan pada instans EC2 Anda:

- Batasi akses ke instans Anda menggunakan grup keamanan. Konfigurasikan aturan yang memungkinkan lalu lintas jaringan minimum yang diperlukan. Misalnya, Anda dapat mengizinkan lalu lintas hanya dari rentang alamat untuk jaringan perusahaan Anda atau hanya untuk protokol tertentu, seperti HTTPS. Untuk instance Windows, izinkan lalu lintas manajemen Windows dan koneksi keluar minimal.
- Manfaatkan grup keamanan sebagai mekanisme utama untuk mengontrol akses jaringan ke instans Amazon EC2. Bila perlu, gunakan jaringan ACLs dengan hemat untuk menyediakan kontrol

jaringan butir kasar tanpa kewarganegaraan. Grup keamanan lebih fleksibel daripada jaringan ACLs karena kemampuan mereka untuk melakukan penyaringan paket stateful dan membuat aturan yang merujuk pada kelompok keamanan lainnya. Namun, jaringan ACLs dapat efektif sebagai kontrol sekunder untuk menolak subset tertentu dari lalu lintas atau menyediakan rel penjaga subnet tingkat tinggi. Juga, karena jaringan ACLs berlaku untuk seluruh subnet, mereka dapat digunakan seolah-olah sebuah instance pernah diluncurkan defense-in-depth secara tidak sengaja tanpa grup keamanan yang benar.

- [Instans Windows] Kelola pengaturan Windows Firewall secara terpusat dengan Objek Kebijakan Grup (GPO) untuk lebih meningkatkan kontrol jaringan. Para pelanggan sering menggunakan Windows Firewall untuk mendapatkan visibilitas ke dalam lalu lintas jaringan lebih jauh dan untuk melengkapi filter grup keamanan, membuat aturan-aturan lanjutan untuk memblokir aplikasi tertentu agar tidak mengakses jaringan atau untuk memfilter lalu lintas dari alamat IP subset. Sebagai contoh, Windows Firewall dapat membatasi akses ke alamat IP layanan metadata EC2 untuk pengguna atau aplikasi tertentu. Atau, layanan yang dapat diakses publik dapat menggunakan grup keamanan untuk membatasi lalu lintas ke port tertentu dan menggunakan Windows Firewall untuk memelihara daftar alamat IP yang diblokir secara eksplisit.
- Gunakan subnet privat untuk instans Anda jika instan tersebut tidak dapat diakses secara langsung dari internet. Gunakan host bastion atau gateway NAT untuk akses internet dari instans di subnet privat.
- [Instans Windows] Gunakan protokol administrasi yang aman seperti enkapsulasi RDP. SSL/TLS. The Remote Desktop Gateway Quick Start provides best practices for deploying remote desktop gateway, including configuring RDP to use SSL/TLS
- [Instans Windows] Gunakan Active Directory atau Directory Service untuk mengontrol secara ketat dan terpusat dan memantau akses pengguna dan grup interaktif ke instance Windows, dan hindari izin pengguna lokal. Selain itu, hindari penggunaan Domain Administrator dan buatlah lebih banyak akun berbasis peran yang terperinci dan spesifik untuk aplikasi. Just Enough Administration (JEA) mengizinkan perubahan-perubahan pada instans Windows dikelola tanpa akses interaktif atau administrator. Selain itu, JEA memungkinkan organisasi untuk mengunci akses administratif pada subset perintah Windows PowerShell yang diperlukan untuk administrasi instans. Untuk informasi tambahan, lihat bagian "Mengelola Akses Tingkat OS pada Amazon EC2" dalam laporan resmi Praktik Terbaik Keamanan AWS.
- [Instans Windows] Administrator Sistem harus menggunakan akun Windows dengan akses terbatas untuk melakukan aktivitas sehari-hari, dan hanya meningkatkan akses bila diperlukan untuk melakukan perubahan konfigurasi tertentu. Selain itu, akses instans Windows secara langsung hanya bila benar-benar diperlukan. Sebaliknya, manfaatkan sistem manajemen

konfigurasi pusat seperti EC2 Run Command, Systems Center Configuration Manager (SCCM), Windows PowerShell DSC, atau Amazon EC2 Systems Manager (SSM) untuk mendorong perubahan pada peladen Windows.

- Lakukan konfigurasi pada tabel rute subnet Amazon VPC dengan rute jaringan syarat minimal. Misalnya, tempatkan hanya instans Amazon EC2 yang memerlukan akses Internet langsung ke subnet dengan rute ke gateway internet, dan tempatkan hanya instans Amazon EC2 yang memerlukan akses langsung ke jaringan internal ke subnet dengan rute ke gateway pribadi virtual.
- Pertimbangkan untuk menggunakan grup keamanan tambahan atau antarmuka jaringan untuk mengontrol dan meng-audit lalu lintas pengelolaan instans Amazon EC2 secara terpisah dari lalu lintas aplikasi reguler. Pendekatan ini memungkinkan pelanggan untuk melaksanakan kebijakan IAM khusus untuk kontrol pengubahan, mempermudahnya untuk meng-audit perubahan pada aturan grup keamanan atau skrip verifikasi aturan otomatis. Menggunakan beberapa antarmuka jaringan juga menyediakan opsi tambahan untuk mengontrol lalu lintas jaringan, termasuk kemampuan untuk membuat kebijakan perutean berbasis host atau memanfaatkan aturan perutean subnet VPC yang berbeda berdasarkan subnet yang ditetapkan dari antarmuka jaringan.
- Gunakan AWS Virtual Private Network atau Direct Connect untuk membuat koneksi pribadi dari jaringan jarak jauh Anda ke jaringan Anda VPCs. Untuk informasi selengkapnya, lihat Opsi Konektivitas Network-to-Amazon VPC.
- Gunakan Log Aliran VPC untuk memantau lalu lintas yang menjangkau instans Anda.
- Gunakan Perlindungan GuardDuty Malware untuk mengidentifikasi perilaku mencurigakan yang menunjukkan perangkat lunak berbahaya pada instans Anda yang dapat membahayakan beban kerja Anda, menggunakan kembali sumber daya untuk penggunaan berbahaya, dan mendapatkan akses tidak sah ke data Anda.
- Gunakan GuardDuty Runtime Monitoring untuk mengidentifikasi dan merespons potensi ancaman terhadap instans Anda. Untuk informasi selengkapnya, lihat Cara kerja Runtime Monitoring dengan instans Amazon EC2.
- Gunakan AWS Security Hub CSPM, Reachability Analyzer, atau Network Access Analyzer untuk memeriksa aksesibilitas jaringan yang tidak diinginkan dari instans Anda.
- Gunakan EC2 Instance Connect untuk terhubung ke instans Anda menggunakan Secure Shell (SSH) tanpa perlu berbagi dan mengelola kunci SSH.
- Gunakan AWS Systems Manager Session Manager untuk mengakses instans Anda dari jarak jauh alih-alih membuka port SSH atau RDP masuk dan mengelola pasangan kunci.
- Gunakan AWS Systems Manager Run Command untuk mengotomatiskan tugas administratif umum alih-alih menghubungkan ke instance Anda.

- [Instans Windows] Banyak peran OS Windows dan aplikasi bisnis Microsoft juga menyediakan fungsionalitas yang ditingkatkan seperti pembatasan Rentang Alamat IP dalam IIS, kebijakan TCP/IP penyaringan di Microsoft SQL Server, dan kebijakan filter koneksi di Microsoft Exchange. Fungsionalitas pembatasan jaringan dalam lapisan aplikasi dapat menyediakan lapisan pertahanan tambahan untuk server aplikasi bisnis penting.

Amazon VPC mendukung kontrol keamanan jaringan tambahan, seperti gateway, server proxy, dan opsi pemantauan jaringan. Untuk informasi selengkapnya, lihat Mengontrol lalu lintas jaringan di Panduan Pengguna Amazon VPC.

Ketahanan dalam Amazon EC2

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Jika Anda harus melakukan replikasi data atau aplikasi Anda pada jarak geografis yang lebih luas, gunakan Zona Lokal AWS . Zona AWS Lokal adalah perpanjangan dari AWS Wilayah dalam kedekatan geografis dengan pengguna Anda. Zona Lokal memiliki koneksinya sendiri ke internet dan mendukung Direct Connect. Seperti semua AWS Wilayah, AWS Local Zones benar-benar terisolasi dari AWS Zona lain.

Jika Anda perlu mereplikasi data atau aplikasi Anda di Zona AWS Lokal, AWS sarankan Anda menggunakan salah satu zona berikut sebagai zona failover:

- Zona Lokal Lainnya
- Zona Ketersediaan dalam Wilayah yang bukan merupakan zona induk. Anda dapat menggunakan describe-availability-zonesperintah untuk melihat zona induk.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Amazon EC2 menawarkan fitur-fitur berikut untuk mendukung ketahanan data Anda:

- Menyalin AMIs lintas Wilayah
- Menyalin snapshot EBS di seluruh Wilayah
- Mengotomatiskan EBS yang didukung AMIs menggunakan Amazon Data Lifecycle Manager
- Menerapkan otomatisasi snapshot EBS menggunakan Amazon Data Lifecycle Manager
- Menjaga kondisi dan ketersediaan armada Anda menggunakan Amazon EC2 Auto Scaling
- Mendistribusikan lalu lintas masuk pada berbagai instans dalam satu Zona Ketersediaan atau beberapa Zona Ketersediaan menggunakan Elastic Load Balancing

Validasi kepatuhan untuk Amazon EC2

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi AWS Keamanan.

Manajemen identitas dan akses untuk Amazon EC2

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Amazon EC2. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Kredensi keamanan Anda mengidentifikasi Anda ke layanan AWS dan memberi Anda akses ke AWS sumber daya, seperti sumber daya Amazon EC2 Anda. Anda dapat menggunakan fitur Amazon EC2 dan IAM untuk memungkinkan pengguna, layanan, dan aplikasi lain menggunakan sumber daya Amazon EC2 Anda tanpa membagikan kredensil keamanan Anda. Anda dapat menggunakan IAM untuk mengontrol cara pengguna lain menggunakan sumber daya di Anda Akun AWS, dan Anda dapat menggunakan grup keamanan untuk mengontrol akses ke instans Amazon EC2 Anda. Anda dapat memilih untuk mengizinkan penggunaan penuh atau terbatas sumber daya Amazon EC2 Anda.

Jika Anda seorang pengembang, Anda dapat menggunakan peran IAM untuk mengelola kredenal keamanan yang dibutuhkan oleh aplikasi yang Anda jalankan pada instans EC2 Anda. Setelah Anda melampirkan peran IAM ke instans Anda, aplikasi yang berjalan pada instance dapat mengambil kredensil dari Layanan Metadata Instance (IMDS).

Untuk praktik terbaik untuk mengamankan AWS sumber daya Anda menggunakan IAM, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Daftar Isi

- Kebijakan berbasis identitas untuk Amazon EC2
- Contoh kebijakan untuk mengontrol akses API Amazon EC2
- Contoh kebijakan untuk mengontrol akses ke konsol Amazon EC2
- AWS kebijakan terkelola untuk Amazon EC2
- IAM role untuk Amazon EC2

Kebijakan berbasis identitas untuk Amazon EC2

Secara default, pengguna tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon EC2, atau melakukan tugas menggunakan API Amazon EC2, konsol Amazon EC2, atau CLI. Untuk memungkinkan pengguna membuat atau memodifikasi sumber daya dan melakukan tugas, Anda harus membuat kebijakan IAM yang memberikan izin kepada pengguna untuk menggunakan sumber daya serta tindakan API tertentu yang akan mereka perlukan, lalu melampirkan kebijakan tersebut ke pengguna, grup, atau peran IAM yang memerlukan izin tersebut.

Saat Anda melampirkan kebijakan ke pengguna atau grup pengguna atau peran, kebijakan tersebut akan mengizinkan atau menolak izin pengguna untuk melakukan tugas tertentu pada sumber daya tertentu. Untuk informasi umum selengkapnya tentang kebijakan IAM, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang mengelola dan membuat kebijakan IAM, lihat Mengelola kebijakan IAM.

kebijakan IAM harus mengizinkan atau menolak izin untuk menggunakan satu atau beberapa tindakan Amazon EC2. Kebijakan tersebut juga harus menentukan sumber daya yang dapat digunakan bersama dengan tindakan tersebut, yang dapat berupa semua sumber daya, atau dalam beberapa kasus, sumber daya tertentu. Kebijakan ini juga dapat mencakup syarat-syarat yang Anda terapkan pada sumber daya.

Untuk memulai, Anda dapat memeriksa apakah kebijakan AWS terkelola untuk Amazon EC2 memenuhi kebutuhan Anda. Jika tidak, Anda dapat membuat kebijakan khusus Anda sendiri. Untuk informasi selengkapnya, lihat the section called “AWS kebijakan terkelola”.

Daftar Isi

- Sintaksis kebijakan
- Tindakan-tindakan untuk Amazon EC2
- Izin tingkat sumber daya yang mendukung tindakan API Amazon EC2
- Amazon Resource Name (ARN) untuk Amazon EC2
- Kunci syarat untuk Amazon EC2
- Kontrol akses menggunakan akses berbasis atribut
- Berikan izin kepada pengguna, grup, dan peran
- Memeriksa apakah pengguna memiliki izin yang diperlukan

Sintaksis kebijakan

kebijakan IAM adalah dokumen JSON yang terdiri dari satu atau beberapa pernyataan. Masing-masing pernyataan memiliki struktur sebagai berikut.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Ada berbagai elemen yang membentuk pernyataan:

- Efek: Efek bisa berupa `Allow` atau `Deny`. Secara default, pengguna tidak memiliki izin untuk menggunakan sumber daya dan tindakan API, sehingga semua permintaan akan ditolak. izin eksplisit akan menggantikan izin default. penolakan eksplisit akan menggantikan izin apa pun.

- Tindakan: Tindakan adalah tindakan API tertentu yang Anda izinkan atau tolak. Untuk mempelajari tentang cara menentukan tindakan, lihat Tindakan-tindakan untuk Amazon EC2.
- Sumber daya: Sumber daya yang dipengaruhi oleh tindakan. Beberapa tindakan Amazon EC2 API memungkinkan Anda untuk menyertakan sumber daya tertentu dalam kebijakan Anda yang dapat dibuat atau dimodifikasi oleh tindakan tersebut. Anda dapat menentukan sumber daya menggunakan Amazon Resource Name (ARN) atau menggunakan wildcard (*) untuk menunjukkan bahwa pernyataan berlaku untuk semua sumber daya. Untuk informasi selengkapnya, lihat Izin tingkat sumber daya yang mendukung tindakan API Amazon EC2.
- Syarat: Syarat-syarat bersifat opsional. Syarat-syarat ini dapat digunakan untuk mengendalikan kapan kebijakan Anda berlaku. Untuk informasi selengkapnya tentang cara menentukan syarat untuk Amazon EC2, lihat Kunci syarat untuk Amazon EC2.

Untuk informasi selengkapnya tentang persyaratan kebijakan, lihat Referensi kebijakan IAM JSON di Panduan Pengguna IAM. Misalnya pernyataan kebijakan IAM untuk Amazon EC2, lihat Contoh kebijakan untuk mengontrol akses API Amazon EC2.

Tindakan-tindakan untuk Amazon EC2

Dalam pernyataan kebijakan IAM, Anda dapat menentukan tindakan API apa pun dari layanan apa pun yang mendukung IAM. Untuk Amazon EC2, gunakan awalan berikut ini dengan nama dari tindakan API: `ec2:`. Misalnya: `ec2:RunInstances` dan `ec2:CreateImage`.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut menggunakan koma seperti berikut:

```
"Action": ["ec2:action1", "ec2:action2"]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard. Sebagai contoh, Anda dapat menentukan semua tindakan yang namanya dimulai dengan kata “Describe” seperti berikut ini:

```
"Action": "ec2:Describe*"
```

> **Note**
>
> Saat ini, tindakan API Describe* Amazon EC2 tidak mendukung izin tingkat sumber daya. Untuk informasi selengkapnya tentang izin tingkat sumber daya untuk Amazon EC2, lihat Kebijakan berbasis identitas untuk Amazon EC2.

Untuk menentukan semua tindakan API Amazon EC2, gunakan wildcard * sebagai berikut:

```
"Action": "ec2:*"
```

Untuk melihat daftar tindakan Amazon EC2, lihat Actions defined by Amazon EC2 (Tindakan yang ditentukan oleh Amazon EC2) di Referensi Otorisasi Layanan.

Izin tingkat sumber daya yang mendukung tindakan API Amazon EC2

Izin tingkat sumber daya mengacu pada kemampuan untuk menentukan sumber daya mana yang boleh digunakan oleh para pengguna untuk melakukan tindakan. Amazon EC2 memiliki dukungan parsial untuk izin tingkat sumber daya. Artinya untuk tindakan Amazon EC2 tertentu, Anda dapat mengontrol kapan para pengguna diizinkan untuk menggunakan tindakan tersebut berdasarkan syarat yang harus dipenuhi, atau sumber daya tertentu yang diizinkan untuk digunakan oleh pengguna. Sebagai contoh, Anda dapat memberikan izin kepada para pengguna untuk meluncurkan instans, tetapi hanya untuk tipe instans tertentu, dan hanya menggunakan AMI tertentu.

Untuk menentukan sumber daya di pernyataan kebijakan IAM, gunakan Amazon Resource Name (ARN) sumber daya tersebut. Untuk informasi selengkapnya tentang cara menentukan nilai ARN, lihat Amazon Resource Name (ARN) untuk Amazon EC2. Jika tindakan API tidak mendukung individu ARNs, Anda harus menggunakan wildcard (*) untuk menentukan bahwa semua sumber daya dapat terpengaruh oleh tindakan tersebut.

Untuk melihat tabel yang mengidentifikasi tindakan API Amazon EC2 mana yang mendukung izin tingkat sumber daya, serta kunci kondisi ARNs dan yang dapat Anda gunakan dalam kebijakan, lihat Tindakan, sumber daya, dan kunci kondisi untuk Amazon EC2.

Ingatlah bahwa Anda dapat menerapkan izin tingkat sumber daya berbasis tanda dalam kebijakan IAM yang Anda gunakan untuk tindakan API Amazon EC2. Hal ini akan memberikan Anda kontrol yang lebih baik atas sumber daya yang dapat dibuat, dimodifikasi, atau digunakan oleh seorang pengguna. Untuk informasi selengkapnya, lihat Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan.

Amazon Resource Name (ARN) untuk Amazon EC2

Setiap pernyataan kebijakan IAM berlaku untuk sumber daya yang Anda tentukan menggunakan mereka ARNs.

ARN memiliki sintaksis umum sebagai berikut:

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

layanan

Layanan (contohnya, `ec2`).

wilayah

Wilayah untuk sumber daya (contohnya, `us-east-1`).

account-id

ID AWS akun, tanpa tanda hubung (misalnya,`123456789012`).

resourceType

Jenis dari sumber daya (contohnya, `instance`).

resourcePath

jalur yang mengidentifikasi sumber daya. Anda dapat menggunakan wildcard * dalam jalur Anda.

Sebagai contoh, Anda dapat mengindikasikan instans tertentu (`i-1234567890abcdef0`) dalam pernyataan Anda menggunakan ARN seperti berikut ini.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Anda dapat menentukan semua instans yang menjadi milik dari akun tertentu menggunakan wildcard * seperti berikut ini.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Anda juga dapat menentukan semua sumber daya Amazon EC2 yang menjadi milik dari akun tertentu menggunakan wildcard * seperti berikut ini.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Untuk menentukan semua sumber daya, atau jika tindakan API tertentu tidak mendukung ARNs, gunakan wildcard * dalam `Resource` elemen sebagai berikut.

```
"Resource": "*"
```

Banyak tindakan API Amazon EC2 yang melibatkan beberapa sumber daya. Misalnya, `AttachVolume` melampirkan volume Amazon EBS pada instans, sehingga pengguna harus memiliki izin untuk menggunakan volume dan instans tersebut. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARNs dengan koma, sebagai berikut.

```
"Resource": ["arn1", "arn2"]
```

Untuk melihat daftar ARN untuk sumber daya Amazon EC2, lihat Jenis sumber daya yang ditentukan oleh Amazon EC2.

Kunci syarat untuk Amazon EC2

di pernyataan kebijakan, Anda dapat secara opsional menentukan syarat yang mengontrol kapan pernyataan tersebut berlaku. Setiap syarat mengandung satu atau beberapa pasangan nilai-kunci . Kunci syarat tidak memedulikan huruf besar atau kecil. Kami telah menetapkan kunci kondisi AWS global, ditambah kunci kondisi khusus layanan tambahan.

Untuk melihat daftar kunci syarat spesifik layanan untuk Amazon EC2, lihat Kunci syarat untuk Amazon EC2. Amazon EC2 juga mengimplementasikan kunci kondisi AWS global. Untuk informasi selengkapnya, lihat Informasi yang tersedia dalam semua permintaan dalam Panduan Pengguna IAM.

Semua tindakan Amazon EC2 mendukung kunci syarat `aws:RequestedRegion` dan `ec2:Region`. Untuk informasi selengkapnya, lihat Contoh: Membatasi akses ke suatu Wilayah tertentu.

Untuk menggunakan kunci syarat dalam kebijakan IAM Anda, gunakan pernyataan `Condition`. Sebagai contoh, kebijakan berikut memberikan izin kepada para pengguna untuk menambah dan menghapus aturan ke dalam dan ke luar untuk grup keamanan apa pun. Kebijakan tersebut menggunakan kunci syarat `ec2:Vpc` untuk menentukan bahwa tindakan ini hanya dapat dilakukan pada grup keamanan di VPC tertentu.

JSON

```
{
"Version":"2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:security-group/*",
       "Condition": {
         "StringEquals": {
           "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/
vpc-11223344556677889"
         }
       }
     }
   ]
}
```

Jika Anda menentukan beberapa syarat, atau beberapa kunci dalam satu syarat, maka kami akan mengevaluasinya menggunakan operasi logika AND. Jika Anda menentukan satu syarat dengan beberapa nilai untuk satu kunci, kami akan mengevaluasi syarat tersebut menggunakan operasi logika OR. Agar izin bisa diberikan, semua syarat harus terpenuhi.

Anda juga dapat menggunakan placeholder saat menentukan syarat. Untuk informasi lebih lanjut, lihat Elemen kebijakan IAM: Variabel dan tanda dalam Panduan Pengguna IAM.

> **Important**
>
> Beberapa kunci syarat bersifat khusus untuk sumber daya, dan beberapa tindakan API menggunakan beberapa sumber daya. Jika Anda menyusun kebijakan dengan kunci syarat, gunakan elemen `Resource` dari pernyataan tersebut untuk menentukan sumber daya yang padanya kunci syarat tersebut berlaku. Jika tidak, kebijakan ini dapat membuat pengguna tidak bisa melakukan tindakan sama sekali, karena pemeriksaan syarat gagal sebab kunci syarat tidak berlaku terhadap sumber daya tersebut. Jika Anda tidak ingin menentukan sumber daya, atau jika Anda telah menyusun elemen `Action` dari kebijakan Anda untuk menyertakan beberapa tindakan API, maka Anda harus menggunakan jenis syarat `...IfExists` untuk memastikan bahwa kunci syarat diabaikan untuk sumber daya yang tidak menggunakannya. Untuk informasi lebih lanjut, lihat... IfExists Ketentuan dalam Panduan Pengguna IAM.

Kunci syarat

- Kunci syarat ec2:Attribute
- Kunci syarat ec2:ResourceID
- Kunci syarat ec2:SourceInstanceARN

Kunci syarat ec2:Attribute

Kunci syarat `ec2:Attribute` dapat digunakan untuk syarat-syarat yang memfilter akses berdasarkan atribut sumber daya.

Kunci kondisi ini hanya mendukung properti yang bertipe data primitif (seperti string atau bilangan bulat), atau AttributeValueobjek kompleks yang hanya berisi properti Value (seperti Deskripsi atau ImdsSupportobjek aksi ModifyImageAttributeAPI). Kunci kondisi tidak dapat digunakan dengan objek kompleks yang berisi beberapa properti, seperti LaunchPermissionobjek dari ModifyImageAttribute.

Misalnya, kebijakan berikut menggunakan kunci `ec2:Attribute/Description` kondisi untuk memfilter akses berdasarkan objek Description kompleks dari tindakan ModifyImageAttributeAPI. Kunci syarat hanya mengizinkan permintaan yang memodifikasi deskripsi citra ke `Production` atau `Development`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

Kebijakan contoh berikut menggunakan kunci `ec2:Attribute` kondisi untuk memfilter akses berdasarkan properti Atribut primitif dari tindakan ModifyImageAttributeAPI. Kunci syarat menolak semua permintaan yang berusaha memodifikasi deskripsi citra.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

Kunci syarat ec2:ResourceID

Saat menggunakan kunci syarat `ec2:ResourceID` berikut dengan tindakan API tertentu, nilai kunci syarat digunakan untuk menentukan sumber daya yang dihasilkan yang dibuat oleh tindakan API. Kunci syarat `ec2:ResourceID` tidak dapat digunakan untuk menentukan sumber daya sumber yang ditentukan dalam permintaan API. Jika Anda menggunakan salah satu dari kunci syarat `ec2:ResourceID` berikut dengan API tertentu, maka Anda harus selalu menentukan wildcard (*). Jika Anda menentukan nilai yang berbeda, syarat tersebut selalu diselesaikan dengan * selama runtime. Misalnya, untuk menggunakan kunci `ec2:ImageId` kondisi dengan CopyImageAPI, maka Anda harus menentukan kunci kondisi sebagai berikut:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Kami menyarankan Anda menghindari penggunaan kunci kondisi ini dengan tindakan API ini:

- `ec2:DhcpOptionsID` – `CreateDhcpOptions`
- `ec2:ImageID`—`CopyImage`,`CreateImage`,`ImportImage`, dan `RegisterImage`
- `ec2:InstanceID`— `RunInstances` dan `ImportInstance`
- `ec2:InternetGatewayID` – `CreateInternetGateway`
- `ec2:NetworkAclID` – `CreateNetworkAcl`
- `ec2:NetworkInterfaceID` – `CreateNetworkInterface`
- `ec2:PlacementGroupName` – `CreatePlacementGroup`
- `ec2:RouteTableID` – `CreateRouteTable`
- `ec2:SecurityGroupID` – `CreateSecurityGroup`
- `ec2:SnapshotID`—`CopySnapshot`,`CreateSnapshot`,`CreateSnapshots`, dan `ImportSnapshots`
- `ec2:SubnetID` – `CreateSubnet`
- `ec2:VolumeID`— `CreateVolume` dan `ImportVolume`
- `ec2:VpcID` – `CreateVpc`
- `ec2:VpcPeeringConnectionID` – `CreateVpcPeeringConnection`

Untuk memfilter akses berdasarkan sumber daya tertentu IDs, sebaiknya gunakan elemen `Resource` kebijakan sebagai berikut.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

Kunci syarat ec2:SourceInstanceARN

Gunakan `ec2:SourceInstanceARN` untuk menentukan ARN dari instance dari mana permintaan dibuat. Ini adalah kunci kondisi AWS global, yang berarti Anda dapat menggunakannya dengan layanan selain Amazon EC2. Untuk contoh kebijakan, lihatContoh: Izinkan instance tertentu untuk melihat sumber daya di AWS layanan lain.

Kontrol akses menggunakan akses berbasis atribut

Saat membuat kebijakan IAM yang memberikan izin kepada pengguna untuk menggunakan sumber daya EC2, Anda dapat menyertakan informasi tanda dalam elemen `Condition` dari kebijakan tersebut untuk mengontrol akses berdasarkan tanda. Hal ini dikenal sebagai kendali akses berbasis atribut (ABAC). ABAC memberikan Anda kendali yang lebih baik atas sumber daya mengenai sumber daya mana yang dapat diubah, digunakan, atau dihapus oleh seorang pengguna. Untuk informasi lebih lanjut, lihat Apa fungsi ABAC untuk AWS?

Sebagai contoh, Anda dapat membuat kebijakan yang memungkinkan para pengguna untuk mengakhiri instans, tetapi menolak tindakan itu jika instans tersebut memiliki tanda `environment=production`. Untuk melakukan hal ini, Anda bisa menggunakan kunci syarat `aws:ResourceTag` untuk mengizinkan atau menolak akses ke sumber daya berdasarkan tanda yang dilampirkan pada sumber daya.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Untuk mempelajari apakah tindakan API Amazon EC2 mendukung kontrol akses menggunakan kunci syarat `aws:ResourceTag`, lihat Tindakan, sumber daya, dan kunci syarat untuk Amazon EC2.

Perhatikan bahwa tindakan `Describe` tidak mendukung izin tingkat sumber daya, sehingga Anda harus menentukannya dalam pernyataan terpisah yang tidak disertai syarat.

Untuk contoh kebijakan IAM, lihat Contoh kebijakan untuk mengontrol akses API Amazon EC2.

Jika Anda mengizinkan atau menolak akses para pengguna ke sumber daya berdasarkan tanda, maka Anda harus mempertimbangkan untuk menolak secara eksplisit memberikan kemampuan kepada pengguna untuk menambahkan atau menghapus tanda tersebut dari sumber daya yang sama. Jika tidak, pengguna dapat mengakali pembatasan Anda dan mendapatkan akses atas sumber daya dengan melakukan modifikasi pada tanda dari sumber daya tersebut.

Berikan izin kepada pengguna, grup, dan peran

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Memeriksa apakah pengguna memiliki izin yang diperlukan

Setelah Anda membuat kebijakan IAM, kami merekomendasikan agar Anda memeriksa apakah kebijakan itu memberikan izin kepada para pengguna untuk menggunakan tindakan API dan sumber daya tertentu yang mereka butuhkan sebelum Anda memasukkan kebijakan tersebut ke dalam produksi.

Pertama-tama, buatlah pengguna untuk tujuan pengujian, lalu lampirkan kebijakan IAM yang Anda buat tersebut ke pengguna pengujian. Kemudian, buatlah permintaan sebagai pengguna uji.

Jika tindakan Amazon EC2 yang Anda uji membuat atau memodifikasi sumber daya, maka Anda harus mengajukan permintaan menggunakan parameter `DryRun` (atau jalankan perintah AWS CLI dengan opsi `--dry-run`). Dalam hal ini, perintah akan menyelesaikan pemeriksaan otorisasi, tetapi tidak akan menyelesaikan operasi. Sebagai contoh, Anda dapat memeriksa apakah pengguna dapat mengakhiri instans tertentu tanpa benar-benar mengakhirinya. Jika pengguna uji tersebut memiliki izin yang diperlukan, maka permintaan itu akan menampilkan `DryRunOperation`; jika tidak, `UnauthorizedOperation` yang akan ditampilkan.

Jika kebijakan tersebut tidak memberikan izin kepada pengguna seperti yang Anda harapkan, atau terlalu longgar dalam memberikan izin, maka Anda dapat menyesuaikan kebijakan itu sesuai kebutuhan Anda dan menguji ulang hingga Anda mendapatkan hasil yang Anda inginkan.

> **Important**
>
> Pengujian ini dapat memakan waktu beberapa menit sebelum perubahan terjadi pada kebijakan untuk ditransmisikan sebelum diberlakukan. Oleh karena itu, kami merekomendasikan Anda memberikan waktu lima menit sebelum Anda menguji pembaruan kebijakan Anda.

Jika pemeriksaan otorisasi gagal, maka permintaan akan menampilkan informasi berenkode yang memuat informasi diagnostik. Anda dapat melakukan dekode pada pesan tersebut menggunakan tindakan `DecodeAuthorizationMessage`. Untuk informasi selengkapnya, lihat DecodeAuthorizationMessagedi Referensi AWS Security Token Service API, dan decode-authorization-message.

Contoh kebijakan untuk mengontrol akses API Amazon EC2

Anda dapat menggunakan kebijakan IAM untuk memberi pengguna izin yang diperlukan untuk bekerja dengan Amazon EC2. Untuk step-by-step petunjuk arah, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Contoh berikut menunjukkan pernyataan kebijakan yang dapat Anda gunakan untuk memberikan izin kepada pengguna untuk menggunakan Amazon EC2. Kebijakan ini dirancang untuk permintaan yang dibuat menggunakan SDK AWS CLI atau AWS SDK. Dalam contoh berikut, ganti masing-masing *`user input placeholder`* dengan informasi Anda sendiri.

Contoh

- Contoh: Akses hanya-baca

- Contoh: Membatasi akses ke suatu Wilayah tertentu
- Cara menggunakan instans
- Luncurkan instance () RunInstances
- Cara Menggunakan Instans Spot
- Contoh: Cara Menggunakan Instans Cadangan
- Contoh: Memberi tanda pada sumber daya
- Contoh: Cara Menggunakan IAM role
- Contoh: Cara menggunakan tabel rute
- Contoh: Izinkan instance tertentu untuk melihat sumber daya di AWS layanan lain
- Contoh: Cara menggunakan templat peluncuran
- Cara menggunakan metadata instans
- Bekerja dengan volume dan snapshot Amazon EBS

Untuk contoh kebijakan yang digunakan dalam konsol Amazon EC2, lihat Contoh kebijakan untuk mengontrol akses ke konsol Amazon EC2.

Contoh: Akses hanya-baca

Kebijakan berikut memberikan izin kepada para pengguna untuk menggunakan semua tindakan API Amazon EC2 yang memiliki nama dimulai dengan `Describe`. Elemen `Resource` menggunakan wildcard untuk mengindikasikan bahwa para pengguna dapat menentukan semua sumber daya dengan tindakan API ini. Wildcard * juga Anda perlukan jika tindakan API tidak mendukung izin tingkat sumber daya. Untuk informasi selengkapnya tentang ARN mana yang dapat Anda gunakan bersama dengan tindakan API Amazon EC2 yang mana, lihat Tindakan, sumber daya, dan kunci syarat untuk Amazon EC2.

Para pengguna tidak memiliki izin untuk melakukan tindakan apa pun atas sumber daya (kecuali jika pernyataan lain memberikan mereka izin untuk melakukannya) karena mereka tidak mendapatkan izin untuk menggunakan tindakan API secara default.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Contoh: Membatasi akses ke suatu Wilayah tertentu

Kebijakan berikut menolak pemberian izin kepada para pengguna untuk menggunakan semua tindakan API Amazon EC2 kecuali Wilayah tersebut adalah Eropa (Frankfurt). Kebijakan ini menggunakan kunci syarat global `aws:RequestedRegion`, yang didukung oleh semua tindakan API Amazon EC2.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
}
```

Atau, Anda dapat menggunakan kunci syarat `ec2:Region`, yang dikhususkan untuk Amazon EC2 dan didukung oleh semua tindakan API Amazon EC2.

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Cara menggunakan instans

Contoh

- Contoh: Mendeskripsikan, meluncurkan, menghentikan, memulai, dan mengakhiri semua instans
- Contoh: Mendeskripsikan semua instans, dan menghentikan, memulai, dan mengakhiri instans tertentu saja

Contoh: Mendeskripsikan, meluncurkan, menghentikan, memulai, dan mengakhiri semua instans

Kebijakan berikut memberikan izin kepada para pengguna untuk menggunakan tindakan API yang ditentukan dalam elemen `Action`. Elemen `Resource` menggunakan wildcard * untuk mengindikasikan bahwa para pengguna dapat menentukan semua sumber daya dengan tindakan API ini. Wildcard * juga Anda perlukan jika tindakan API tidak mendukung izin tingkat sumber daya. Untuk informasi selengkapnya tentang ARN mana yang dapat Anda gunakan bersama dengan tindakan API Amazon EC2 yang mana, lihat Tindakan, sumber daya, dan kunci syarat untuk Amazon EC2.

Para pengguna tidak memiliki izin untuk menggunakan tindakan API apa pun (kecuali jika pernyataan lain memberikan mereka izin untuk melakukannya) karena para pengguna tersebut tidak mendapatkan izin untuk menggunakan tindakan API secara default.

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

Contoh: Mendeskripsikan semua instans, dan menghentikan, memulai, dan mengakhiri instans tertentu saja

Kebijakan berikut memungkinkan pengguna untuk mendeskripsikan semua instance, untuk memulai dan menghentikan hanya instance i-1234567890abcdef0 dan i-0598c7d356eba48d7, dan untuk mengakhiri hanya instance di Wilayah, dengan tag sumber daya "". `us-east-1` `purpose=test`

Pernyataan pertama menggunakan wildcard * untuk elemen `Resource` untuk mengindikasikan bahwa para pengguna dapat menentukan semua sumber daya dengan tindakan tersebut; dalam hal ini, mereka dapat mencantumkan semua instans. Wildcard * tersebut juga Anda perlukan jika tindakan API tidak mendukung izin tingkat sumber daya (dalam hal ini, `ec2:DescribeInstances`). Untuk informasi selengkapnya tentang ARN mana yang dapat Anda gunakan bersama dengan tindakan API Amazon EC2 yang mana, lihat Tindakan, sumber daya, dan kunci syarat untuk Amazon EC2.

Pernyataan kedua menggunakan izin tingkat sumber daya untuk tindakan `StopInstances` dan `StartInstances`. Contoh spesifik ditunjukkan oleh `Resource` elemen mereka ARNs .

Pernyataan ketiga memungkinkan pengguna untuk menghentikan semua instance di `us-east-1` Wilayah yang termasuk dalam AWS akun yang ditentukan, tetapi hanya jika instance memiliki tag. `"purpose=test"` Elemen `Condition` memenuhi syarat ketika pernyataan kebijakan berlaku.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:111122223333:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
      }
   }

   ]
}
```

Luncurkan instance () RunInstances

Tindakan RunInstancesAPI meluncurkan satu atau beberapa Instans Sesuai Permintaan atau satu atau beberapa Instans Spot. `RunInstances`membutuhkan AMI dan membuat instance. Para pengguna dapat menentukan pasangan kunci dan grup keamanan dalam permintaan. Peluncuran ke dalam VPC memerlukan subnet, dan akan membuat antarmuka jaringan. Peluncuran dari AMI yang

didukung Amazon EBS akan membuat volume. Oleh karena itu, para pengguna harus memiliki izin untuk menggunakan sumber daya Amazon EC2 ini. Anda dapat membuat pernyataan kebijakan yang mengharuskan pengguna menentukan parameter opsional pada `RunInstances`, atau membatasi pengguna pada nilai tertentu sebagai parameter.

Untuk informasi selengkapnya tentang izin tingkat sumber daya yang diperlukan untuk meluncurkan instans, lihat Tindakan, sumber daya, dan kunci syarat untuk Amazon EC2.

Secara default, para pengguna tidak memiliki izin untuk mendeskripsikan, memulai, menghentikan, atau mengakhiri instans yang dihasilkan. Salah satu cara untuk memberikan izin kepada para pengguna untuk mengelola instans yang dihasilkan adalah dengan membuat tanda tertentu untuk setiap instans, dan kemudian membuat pernyataan yang memungkinkan mereka mengelola instans-instans itu dengan tanda tersebut. Untuk informasi selengkapnya, lihat Cara menggunakan instans.

Sumber daya

- AMIs
- Tipe instans
- Subnet
- Volume EBS
- Tanda
- Tanda di templat peluncuran
- Elastis GPUs
- Templat peluncuran

AMIs

Kebijakan berikut memungkinkan pengguna untuk meluncurkan instance hanya menggunakan yang ditentukan AMIs, `ami-9e1670f7` dan`ami-45cf5c3c`. Pengguna tidak dapat meluncurkan instance menggunakan other AMIs (kecuali pernyataan lain memberikan izin kepada pengguna untuk melakukannya).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
```

```
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:us-east-1::image/ami-9e1670f7",
        "arn:aws:ec2:us-east-1::image/ami-45cf5c3c",
        "arn:aws:ec2:us-east-1:111122223333:instance/*",
        "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
        "arn:aws:ec2:us-east-1:111122223333:security-group/*",
        "arn:aws:ec2:us-east-1:111122223333:subnet/*",
        "arn:aws:ec2:us-east-1:111122223333:network-interface/*"
      ]
    }
   ]
}
```

Atau, kebijakan berikut memungkinkan pengguna untuk meluncurkan instans dari semua yang AMIs dimiliki oleh Amazon, atau mitra tepercaya dan terverifikasi tertentu. Elemen `Condition` dari pernyataan pertama menguji apakah `ec2:Owner` adalah `amazon`. Pengguna tidak dapat meluncurkan instance menggunakan other AMIs (kecuali pernyataan lain memberikan izin kepada pengguna untuk melakukannya).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
```

```
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
         ]
      }
   ]
}
```

Tipe instans

Kebijakan berikut memungkinkan para pengguna untuk meluncurkan instans dengan hanya menggunakan tipe instans `t2.micro` atau `t2.small`, hal ini mungkin Anda lakukan untuk mengontrol biaya. Para pengguna tidak dapat meluncurkan instans yang lebih besar karena elemen `Condition` dari pernyataan pertama menguji apakah `ec2:InstanceType` merupakan `t2.micro` atau `t2.small`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
```

```
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
         ]
      }
   ]
}
```

Atau, Anda dapat membuat kebijakan yang menolak memberikan izin kepada pengguna untuk meluncurkan instans apa pun kecuali tipe instans `t2.micro` dan `t2.small`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
```

```
            "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
            "arn:aws:ec2:us-east-1:111122223333:security-group/*"
            ]
        }
    ]
}
```

Subnet

Kebijakan berikut memungkinkan para pengguna untuk meluncurkan instans hanya menggunakan subnet yang ditentukan, `subnet-12345678`. Grup tidak dapat meluncurkan instans ke subnet lain mana pun (kecuali pernyataan lain memberikan izin kepada pengguna untuk melakukannya).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:subnet/subnet-12345678",
        "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
        "arn:aws:ec2:us-east-1:111122223333:instance/*",
        "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "arn:aws:ec2:us-east-1::image/ami-*",
        "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
        "arn:aws:ec2:us-east-1:111122223333:security-group/*"
      ]
    }
   ]
}
```

Atau, Anda dapat membuat kebijakan yang menolak memberikan izin kepada pengguna untuk meluncurkan instans ke dalam subnet lain mana pun. Pernyataan tersebut menjalankan hal ini dengan menolak memberikan izin untuk membuat antarmuka jaringan, kecuali jika subnet

`subnet-12345678` telah ditentukan. Penolakan ini akan mengabaikan kebijakan lain yang dibuat untuk memungkinkan peluncuran instans ke dalam subnet lain.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*"
      ],
      "Condition": {
         "ArnNotEquals": {
            "ec2:Subnet": "arn:aws:ec2:us-east-1:111122223333:subnet/
subnet-12345678"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
         ]
      }
   ]
}
```

Volume EBS

Kebijakan berikut memungkinkan para pengguna untuk meluncurkan instans hanya jika volume EBS untuk instans tersebut sudah dienkripsi. Pengguna harus meluncurkan instans dari AMI yang dibuat

dengan snapshot yang dienkripsi untuk memastikan volume root sudah dienkripsi. Volume tambahan apa pun yang dilampirkan oleh pengguna pada instans saat dilakukan peluncuran juga harus sudah dienkripsi.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

Tanda

Memberi tanda pada instans pada saat instans dibuat

Kebijakan berikut memungkinkan para pengguna untuk meluncurkan instans dan memberi tanda pada instans saat instans sedang dibuat. Untuk tindakan-tindakan yang digunakan untuk membuat sumber daya yang menerapkan tanda, para pengguna harus memiliki izin untuk menggunakan tindakan `CreateTags`. Pernyataan kedua menggunakan kunci syarat `ec2:CreateAction` untuk memungkinkan para pengguna membuat tanda hanya dalam konteks `RunInstances`, dan hanya untuk instans. Para pengguna tidak dapat memberi tanda pada sumber daya yang sudah ada, dan para pengguna tidak dapat memberi tanda pada volume menggunakan permintaan `RunInstances`.

Untuk informasi selengkapnya, lihat Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Memberi tanda pada instans dan volume pada saat pembuatan dengan tanda tertentu

Kebijakan berikut mencakup kunci syarat `aws:RequestTag` yang mengharuskan para pengguna untuk menandai setiap instans dan volume yang dibuat oleh `RunInstances` dengan tanda `environment=production` dan `purpose=webserver`. Jika pengguna tidak meneruskan tanda tertentu ini, atau jika mereka tidak menentukan tanda sama sekali, maka permintaan itu akan gagal.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-1::image/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:us-east-1:111122223333:volume/*",
          "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:RequestTag/environment": "production" ,
            "aws:RequestTag/purpose": "webserver"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
            "ec2:CreateTags"
         ],
         "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
         "Condition": {
            "StringEquals": {
                "ec2:CreateAction" : "RunInstances"
             }
          }
      }
   ]
}
```

Memberi tanda pada instans dan volume pada saat pembuatan dengan setidaknya satu tanda tertentu

Kebijakan berikut menggunakan pemodifikasi `ForAnyValue` berdasarkan syarat `aws:TagKeys` untuk mengindikasikan bahwa setidaknya satu tanda harus ditentukan dalam permintaan, dan harus berisi kunci `environment` atau `webserver`. Tanda harus diterapkan baik untuk instans maupun volume. Nilai tanda apa pun juga dapat ditentukan dalam permintaan.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-1::image/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
            "ec2:RunInstances"
        ],
        "Resource": [
            "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "arn:aws:ec2:us-east-1:111122223333:instance/*"
        ],
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": ["environment","webserver"]
            }
         }
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction" : "RunInstances"
            }
         }
      }
    ]
}
```

Jika instans diberi tanda pada saat instans dibuat, maka instans tersebut harus diberi tanda dengan tanda tertentu

Dalam kebijakan berikut, para pengguna tidak perlu menentukan tanda dalam permintaan, tetapi jika mereka melakukannya, tanda harus berupa `purpose=test`. Tidak ada tanda lain yang diperbolehkan. Pengguna dapat menerapkan tanda ke sumber daya mana pun yang dapat diberi tanda dalam permintaan `RunInstances`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Untuk melarang siapa pun yang dipanggil tag di create for RunInstances

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
```

```
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Hanya izinkan tag tertentu untuk spot-instances-request. Inkonsistensi kejutan nomor 2 akan mempengaruhi hasilnya. Dalam keadaan normal, tidak menentukan tanda akan menghasilkan Tidak terautentikasi. Dalam hal ini spot-instances-request, kebijakan ini tidak akan dievaluasi jika tidak ada spot-instances-request tag, sehingga permintaan Spot on Run non-tag akan berhasil.

Tanda di templat peluncuran

Dalam contoh berikut ini, para pengguna dapat meluncurkan beberapa instans, tetapi hanya jika mereka menggunakan templat peluncuran tertentu (`lt-09477bcd97b0d310e`). Kunci syarat `ec2:IsLaunchTemplateResource` mencegah para pengguna untuk mengganti sumber daya apa pun yang ditentukan dalam templat peluncuran tersebut. Bagian kedua dari pernyataan ini memungkinkan para pengguna untuk memberikan tanda pada instans saat instans dibuat—bagian pernyataan ini diperlukan jika tanda ditentukan untuk instans dalam templat peluncuran.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
```

```
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/lt-09477bcd97b0d310e"
          },
          "Bool": {
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Elastis GPUs

Dalam kebijakan berikut, para pengguna dapat meluncurkan instans dan menentukan GPU elastis untuk dilampirkan ke instans. Pengguna dapat meluncurkan instans di Wilayah mana pun, tetapi mereka hanya dapat melampirkan GPU elastis saat dilakukan peluncuran dalam Wilayah `us-east-2`.

Kunci syarat `ec2:ElasticGpuType` memastikan bahwa instans menggunakan tipe GPU elastis `eg1.medium` atau `eg1.large`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
            {
           "Effect": "Allow",
```

```
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:111122223333:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:111122223333:network-interface/*",
                "arn:aws:ec2:*:111122223333:instance/*",
                "arn:aws:ec2:*:111122223333:subnet/*",
                "arn:aws:ec2:*:111122223333:volume/*",
                "arn:aws:ec2:*:111122223333:key-pair/*",
                "arn:aws:ec2:*:111122223333:security-group/*"
            ]
        }
    ]
}
```

Templat peluncuran

Dalam contoh berikut ini, para pengguna dapat meluncurkan beberapa instans, tetapi hanya jika mereka menggunakan templat peluncuran tertentu (`lt-09477bcd97b0d310e`). Para pengguna dapat mengganti parameter apa pun dalam templat peluncuran itu dengan menentukan parameter dalam tindakan `RunInstances`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

Dalam contoh berikut, para pengguna dapat meluncurkan instans hanya jika mereka menggunakan templat peluncuran. Kebijakan ini menggunakan kunci `ec2:IsLaunchTemplateResource` kondisi untuk mencegah pengguna mengganti semua yang sudah ada sebelumnya ARNs dalam template peluncuran.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
```

```
          }
       }
    }
  ]
}
```

Contoh kebijakan berikut ini memungkinkan para pengguna untuk meluncurkan instans, tetapi hanya jika mereka menggunakan templat peluncuran. Para pengguna tidak dapat mengganti parameter subnet dan antarmuka jaringan dalam permintaan; parameter-parameter ini hanya dapat ditentukan dalam templat peluncuran. Bagian pertama pernyataan menggunakan elemen NotResource untuk memungkinkan semua sumber daya kecuali subnet dan antarmuka jaringan. Bagian kedua dari pernyataan mengizinkan sumber daya subnet dan antarmuka jaringan, tetapi hanya jika sumber tersebut berasal dari templat peluncuran.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:us-east-1:111122223333:subnet/*",
                      "arn:aws:ec2:us-east-1:111122223333:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          }
       }
    },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:us-east-1:111122223333:subnet/*",
                   "arn:aws:ec2:us-east-1:111122223333:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
```

```
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

Contoh berikut ini memungkinkan para pengguna untuk meluncurkan instans hanya jika mereka menggunakan templat peluncuran, dan hanya jika templat peluncuran memiliki tanda `Purpose=Webservers`. Para pengguna tidak dapat mengganti parameter templat peluncuran dalam tindakan `RunInstances`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
         "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
```

```
        }
      }
  ]
}
```

Cara Menggunakan Instans Spot

Anda dapat menggunakan RunInstances tindakan untuk membuat permintaan Instans Spot, dan menandai permintaan Instans Spot saat membuat. Sumber daya yang akan ditentukan RunInstances adalah`spot-instances-request`.

Sumber daya `spot-instances-request` dievaluasi dalam kebijakan IAM sebagaimana berikut ini:

- Jika Anda tidak memberi tag pada permintaan Instans Spot saat dibuat, Amazon EC2 tidak mengevaluasi`spot-instances-request` sumber daya di RunInstances pernyataan.
- Jika Anda memberi tag pada permintaan Instans Spot saat dibuat, Amazon EC2 mengevaluasi`spot-instances-request` sumber daya di RunInstances pernyataan.

Oleh karena itu, untuk sumber daya `spot-instances-request`, aturan-aturan berikut berlaku untuk kebijakan IAM:

- Jika Anda menggunakan RunInstances untuk membuat permintaan Instance Spot dan Anda tidak bermaksud untuk menandai permintaan Instans Spot saat membuat, Anda tidak perlu secara eksplisit mengizinkan `spot-instances-request` sumber daya; panggilan akan berhasil.
- Jika Anda menggunakan RunInstances untuk membuat permintaan Instans Spot dan bermaksud untuk menandai permintaan Instans Spot saat membuat, Anda harus menyertakan `spot-instances-request` sumber daya dalam pernyataan RunInstances allow, jika tidak panggilan akan gagal.
- Jika Anda menggunakan RunInstances untuk membuat permintaan Instans Spot dan bermaksud untuk menandai permintaan Instans Spot saat membuat, Anda harus menentukan `spot-instances-request` sumber daya atau * wildcard dalam pernyataan CreateTags allow, jika tidak panggilan akan gagal.

Anda dapat meminta Instans Spot menggunakan RunInstances atau RequestSpotInstances. Contoh berikut kebijakan IAM hanya berlaku saat meminta Instans Spot menggunakan. RunInstances

Contoh: Minta Instans Spot menggunakan RunInstances

Kebijakan berikut memungkinkan pengguna untuk meminta Instans Spot dengan menggunakan RunInstances tindakan. Sumber `spot-instances-request` daya, yang dibuat oleh RunInstances, meminta Instans Spot.

> **Note**
>
> Untuk digunakan RunInstances untuk membuat permintaan Instans Spot, Anda dapat menghilangkan `spot-instances-request` dari `Resource` daftar jika Anda tidak bermaksud untuk menandai permintaan Instans Spot saat membuat. Hal ini dikarenakan Amazon EC2 tidak mengevaluasi sumber daya `spot-instances-request` dalam pernyataan RunInstances jika permintaan Instans Spot tidak diberi tag pada saat penciptaan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
}
```

Warning

TIDAK DIDUKUNG - Contoh: Tolak izin pengguna untuk meminta Instans Spot menggunakan RunInstances

Kebijakan berikut ini tidak mendukung sumber daya `spot-instances-request`.

Kebijakan berikut ini dimaksudkan untuk memberikan izin kepada para pengguna untuk meluncurkan Instans Sesuai Permintaan, tetapi menolak memberikan izin untuk permintaan Instans Spot. `spot-instances-request`Sumber daya, yang dibuat oleh RunInstances, adalah sumber daya yang meminta Instans Spot. Pernyataan kedua dimaksudkan untuk menolak RunInstances tindakan untuk `spot-instances-request` sumber daya. Namun, kondisi ini tidak didukung karena Amazon EC2 tidak mengevaluasi `spot-instances-request` sumber daya dalam RunInstances pernyataan jika permintaan Instans Spot tidak ditandai pada create.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequestsNOTSUPPORTEDDONOTUSE",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
```

```
        }
    ]
}
```

Contoh: Memberikan tanda pada permintaan Instans Spot pada saat dibuat

Kebijakan berikut ini memungkinkan para pengguna untuk memberikan tanda pada semua sumber daya yang dibuat saat dilakukan peluncuran instans. Pernyataan pertama memungkinkan RunInstances untuk membuat sumber daya yang terdaftar. `spot-instances-request`Sumber daya, yang dibuat oleh RunInstances, adalah sumber daya yang meminta Instans Spot. Pernyataan kedua menyediakan wildcard * untuk mengizinkan semua sumber daya diberi tanda pada saat dibuat ketika peluncuran instans.

> **Note**
>
> Jika Anda menandai permintaan Instans Spot saat membuat, Amazon EC2 akan mengevaluasi `spot-instances-request` sumber daya dalam pernyataan. RunInstances Oleh karena itu, Anda harus secara eksplisit mengizinkan `spot-instances-request` sumber daya untuk RunInstances tindakan tersebut, jika tidak panggilan akan gagal.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
```

```
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Contoh: Menolak tanda pada saat dibuat untuk permintaan Instans Spot

Kebijakan berikut ini menolak memberikan izin kepada para pengguna untuk memberikan tanda pada semua sumber daya yang dibuat saat dilakukan peluncuran instans.

Pernyataan pertama memungkinkan RunInstances untuk membuat sumber daya yang terdaftar. `spot-instances-request`Sumber daya, yang dibuat oleh RunInstances, adalah sumber daya yang meminta Instans Spot. Pernyataan kedua menyediakan wildcard `*` untuk menolak semua sumber daya yang sedang diberi tanda pada saat dibuat ketika peluncuran instans. Jika `spot-instances-request` atau sumber daya lain diberi tag pada saat penciptaan, perintah RunInstances akan gagal.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
```

```
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Warning

TIDAK DIDUKUNG - Contoh: Mengizinkan pembuatan permintaan Instans Spot hanya jika ada tanda khusus yang ditetapkan untuknya
Kebijakan berikut ini tidak mendukung sumber daya `spot-instances-request`.
Kebijakan berikut dimaksudkan untuk memberikan RunInstances izin untuk membuat permintaan Instans Spot hanya jika permintaan ditandai dengan tag tertentu.
Pernyataan pertama memungkinkan RunInstances untuk membuat sumber daya yang terdaftar.
Pernyataan kedua dimaksudkan untuk memberikan izin kepada para pengguna untuk membuat permintaan Instans Spot hanya jika permintaan itu memiliki tanda `environment=production`. Jika kondisi ini diterapkan ke sumber daya lain yang dibuat oleh RunInstances, menentukan tidak ada tag menghasilkan `Unauthenticated` kesalahan. Namun, jika tidak ada tag yang ditentukan untuk permintaan Instans Spot, Amazon EC2 tidak mengevaluasi `spot-instances-request` sumber daya dalam RunInstances pernyataan, yang menghasilkan permintaan Instans Spot yang tidak diberi tag dibuat oleh. RunInstances Perhatikan bahwa penentuan tag lain selain `environment=production` akan menghasilkan eror `Unauthenticated` karena jika pengguna memberi tag pada permintaan Instans Spot, Amazon EC2 akan mengevaluasi sumber daya`spot-instances-request` dalam pernyataan RunInstances .

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid":
 "RequestSpotInstancesOnlyIfTagIsEnvironmentProductionNOTSUPPORTEDDONOTUSE",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/
*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
```

```
}
```

Contoh: Menolak membuat permintaan Instans Spot jika ada tanda tertentu yang ditetapkan untuknya

Kebijakan berikut menolak RunInstances izin untuk membuat permintaan Instans Spot jika permintaan tersebut ditandai dengan. `environment=production`

Pernyataan pertama memungkinkan RunInstances untuk membuat sumber daya yang terdaftar.

Pernyataan kedua menolak memberikan izin kepada para pengguna untuk membuat permintaan Instans Spot jika permintaan itu memiliki tanda `environment=production`. Menentukan `environment=production` sebagai tanda akan mengakibatkan munculnya kesalahan `Unauthenticated`. Menentukan tanda lain atau tidak menentukan tanda akan mengakibatkan terciptanya permintaan Instans Spot.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
```

```
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Contoh: Cara Menggunakan Instans Cadangan

Kebijakan berikut ini memberikan izin kepada para pengguna untuk menampilkan, memodifikasi, dan membeli Instans Cadangan dalam akun Anda.

Pengaturan izin tingkat sumber daya untuk masing-masing Instans Cadangan tidak bisa dilakukan. Kebijakan ini berarti para pengguna memiliki akses ke semua Instans Cadangan dalam akun tersebut.

Elemen `Resource` menggunakan wildcard * untuk mengindikasikan bahwa para pengguna dapat menentukan semua sumber daya dengan tindakan; dalam hal ini, mereka dapat mencantumkan dan memodifikasi semua Instans Cadangan dalam akun. Mereka juga dapat membeli Instans Cadangan menggunakan kredensial akun. Wildcard * juga Anda perlukan jika tindakan API tidak mendukung izin tingkat sumber daya.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

Untuk memungkinkan para pengguna menampilkan dan memodifikasi Instans Cadangan dalam akun Anda, tetapi tidak untuk membeli Instans Cadangan baru.

JSON

```
{
  "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Contoh: Memberi tanda pada sumber daya

Kebijakan berikut ini memungkinkan para pengguna untuk menggunakan tindakan `CreateTags` untuk menerapkan tanda ke instans hanya jika tanda tersebut berisi kunci `environment` dan nilai `production`. Tidak ada tag lain yang diizinkan dan pengguna tidak dapat menandai jenis sumber daya lainnya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

Kebijakan berikut memungkinkan pengguna untuk menandai sumber daya apa pun yang dapat ditandai, yang sudah memiliki tanda dengan kunci `owner` dan nilai dari nama pengguna. Selain itu, para pengguna juga harus menentukan tanda dengan kunci `anycompany:environment-type` dan nilai dari `test` atau `prod` dalam permintaan. Para pengguna dapat menentukan tanda tambahan dalam permintaan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:RequestTag/anycompany:environment-type":
 ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

Anda dapat membuat kebijakan IAM yang memungkinkan para pengguna untuk menghapus tanda tertentu untuk sumber daya. Sebagai contoh, kebijakan berikut ini memungkinkan para pengguna untuk menghapus tanda untuk volume jika kunci tanda yang ditentukan dalam permintaan tersebut adalah `environment` atau `cost-center`. Nilai apa pun dapat ditentukan untuk tanda tetapi kunci tanda harus cocok dengan salah satu kunci dari kunci yang ditentukan.

> **Note**
>
> Jika Anda menghapus sumber daya, semua tanda yang dikaitkan dengan sumber daya tersebut juga dihapus. Para pengguna tidak memerlukan izin untuk menggunakan tindakan `ec2:DeleteTags` untuk menghapus sumber daya yang memiliki tanda; mereka hanya memerlukan izin untuk melakukan tindakan penghapusan.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
  ]
```

```
}
```

Kebijakan ini memungkinkan pengguna untuk hanya menghapus tanda `environment=prod` pada sumber daya mana pun, dan hanya jika sumber daya tersebut sudah ditandai dengan kunci `owner` dan nilai dari nama pengguna. Pengguna tidak dapat menghapus tanda lain untuk sumber daya.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Contoh: Cara Menggunakan IAM role

Kebijakan berikut ini memungkinkan para pengguna untuk melampirkan, mengganti, dan melepaskan IAM role ke instans yang memiliki tanda `department=test`. Mengganti atau melepaskan IAM role terlampir memerlukan ID asosiasi, oleh karena itu kebijakan tersebut juga memberikan izin kepada para pengguna untuk menggunakan tindakan `ec2:DescribeIamInstanceProfileAssociations`.

Pengguna harus memiliki izin untuk menggunakan tindakan `iam:PassRole` guna meneruskan peran ke instans.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::111122223333:role/DevTeam*"
    }
  ]
}
```

Kebijakan berikut ini akan memungkinkan para pengguna untuk melampirkan atau mengganti IAM role untuk instans apa pun. Para pengguna hanya dapat melampirkan atau mengganti IAM role dengan nama yang dimulai dengan `TestRole-`. Untuk tindakan `iam:PassRole`, pastikan Anda mencantumkan nama IAM role dan bukan nama profil instans (jika nama keduanya berbeda). Untuk informasi selengkapnya, lihat Profil instans.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/TestRole-*"
        }
    ]
}
```

Contoh: Cara menggunakan tabel rute

Kebijakan berikut ini memungkinkan para pengguna menambahkan, menghapus, dan mengganti rute untuk tabel rute yang dikaitkan dengan VPC `vpc-ec43eb89` saja. Untuk menentukan VPC untuk kunci syarat `ec2:Vpc`, Anda harus menentukan ARN lengkap dari VPC tersebut.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111122223333:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/vpc-
ec43eb89"
                }
            }
        }
    ]
}
```

Contoh: Izinkan instance tertentu untuk melihat sumber daya di AWS layanan lain

Berikut ini adalah contoh kebijakan yang dapat Anda lampirkan ke IAM role. Kebijakan ini memungkinkan instance untuk melihat sumber daya di berbagai AWS layanan. Ini menggunakan kunci kondisi `ec2:SourceInstanceARN` global untuk menentukan bahwa instance dari mana permintaan dibuat harus instance`i-093452212644b0dd6`. Jika IAM role yang sama dikaitkan dengan instans yang lain, maka instans lain tersebut tidak akan dapat melakukan tindakan apa pun.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0934522126440b0dd6"
                }
            }
        }
    ]
}
```

Contoh: Cara menggunakan templat peluncuran

Kebijakan berikut ini memungkinkan para pengguna untuk membuat versi templat peluncuran dan memodifikasi templat peluncuran, tetapi hanya untuk templat peluncuran tertentu (`lt-09477bcd97b0d3abc`). Para pengguna tidak dapat menggunakan templat peluncuran yang lain.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/
lt-09477bcd97b0d3abc"
    }
  ]
}
```

Kebijakan berikut ini akan memungkinkan para pengguna untuk menghapus templat peluncuran dan versi templat peluncuran, dengan ketentuan bahwa templat peluncuran tersebut memiliki tanda `Purpose=Testing`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Cara menggunakan metadata instans

Kebijakan berikut memastikan bahwa pengguna hanya dapat mengambil metadata instance menggunakan Layanan Metadata Instance Versi 2 (). IMDSv2 Anda dapat menggabungkan empat kebijakan berikut ini ke dalam satu kebijakan yang memiliki empat pernyataan. Jika digabungkan sebagai satu kebijakan, Anda dapat menggunakan kebijakan tersebut sebagai kebijakan kontrol layanan (SCP). Kebijakan tersebut dapat berfungsi dengan sama baiknya sebagai kebijakan tolak yang Anda terapkan pada kebijakan IAM yang sudah ada (menarik dan membatasi izin dengan sudah ada), atau sebagai SCP yang diterapkan secara global pada akun, unit organisasi (OU), atau keseluruhan organisasi.

> **Note**
>
> Kebijakan opsi RunInstances metadata berikut harus digunakan bersama dengan kebijakan yang memberikan izin utama untuk meluncurkan instance. RunInstances Jika kepala sekolah juga tidak memiliki RunInstances izin, ia tidak akan dapat meluncurkan instance. Untuk

informasi selengkapnya, lihat kebijakan-kebijakan yang ada dalam Cara menggunakan instans dan Luncurkan instance () RunInstances.

Important

Jika Anda menggunakan grup Auto Scaling dan Anda perlu menggunakan semua instans baru, grup Auto Scaling Anda harus menggunakan templat peluncuran. IMDSv2
Saat grup Auto Scaling menggunakan templat peluncuran, izin `ec2:RunInstances` dari prinsipal utama IAM akan diperiksa saat grup Auto Scaling baru dibuat. Izin tersebut juga akan diperiksa saat grup Auto Scaling yang sudah ada diperbarui untuk penggunaan templat peluncuran baru atau templat peluncuran versi baru.
Pembatasan penggunaan IMDSv1 pada prinsipal IAM untuk hanya `RunInstances` dicentang ketika grup Auto Scaling yang menggunakan template peluncuran, dibuat atau diperbarui. Untuk grup Auto Scaling yang dikonfigurasi untuk menggunakan templat peluncuran `Latest` atau `Default`, izin tersebut tidak diperiksa saat versi baru dari templat peluncuran tersebut dibuat. Untuk izin yang akan diperiksa, pengguna harus melakukan konfigurasi terhadap grup Auto Scaling untuk menggunakan versi tertentu dari templat peluncuran tersebut.

Untuk menerapkan penggunaan IMDSv2 pada instans yang diluncurkan oleh grup Auto Scaling, diperlukan langkah-langkah tambahan berikut:

1. Nonaktifkan penggunaan konfigurasi peluncuran untuk semua akun di organisasi Anda dengan menggunakan kebijakan kontrol layanan (SCPs) atau batas izin IAM untuk prinsip baru yang dibuat. Untuk prinsipal utama IAM yang sudah ada yang memiliki izin grup Auto Scaling, lakukan pembaruan atas kebijakan-kebijakan yang dikaitkan dengan kunci syarat ini. Untuk menonaktifkan penggunaan konfigurasi peluncuran, buatlah atau lakukan modifikasi pada SCP, batas-batas izin, atau kebijakan IAM yang relevan dengan kunci syarat `"autoscaling:LaunchConfigurationName"` dengan nilai yang ditentukan sebagai `null`.
2. Untuk templat peluncuran baru, lakukan konfigurasi pada opsi metadata instans di templat peluncuran. Untuk templat peluncuran yang sudah ada, buatlah templat peluncuran versi baru dan lakukan konfigurasi pada opsi metadata instans dalam versi baru itu.
3. Dalam kebijakan yang memberikan izin kepada setiap prinsipal utama untuk menggunakan templat peluncuran, batasi asosiasi `$latest` dan `$default` dengan menentukan `"autoscaling:LaunchTemplateVersionSpecified": "true"`. Dengan

membatasi penggunaan hanya pada templat peluncuran versi tertentu saja, Anda telah memastikan bahwa instans baru akan diluncurkan menggunakan versi di mana opsi metadata dikonfigurasi. Untuk informasi selengkapnya, lihat LaunchTemplateSpecification dalam Referensi Amazon EC2 Auto Scaling API, khususnya parameter `Version`.

4. Untuk grup Auto Scaling yang menggunakan konfigurasi peluncuran, ganti konfigurasi peluncuran itu dengan templat peluncuran. Untuk informasi selengkapnya, lihat Memigrasi grup Auto Scaling untuk meluncurkan templat di Panduan Pengguna Amazon EC2 Auto Scaling.
5. Untuk grup Auto Scaling yang menggunakan templat peluncuran, pastikan grup tersebut menggunakan templat peluncuran baru dengan opsi metadata instans yang telah dikonfigurasi, atau menggunakan templat peluncuran versi terbaru saat ini dengan opsi metadata instans yang telah dikonfigurasi. Untuk informasi selengkapnya, lihat update-auto-scaling-group.

Contoh

- Membutuhkan penggunaan IMDSv2
- Tolak opt-out IMDSv2
- Menentukan batas hop maksimum
- Batasi siapa saja yang dapat melakukan modifikasi terhadap opsi metadata instans
- Memerlukan kredensi peran untuk diambil dari IMDSv2

Membutuhkan penggunaan IMDSv2

Kebijakan berikut menetapkan bahwa Anda tidak dapat memanggil RunInstances API kecuali instans juga memilih untuk meminta penggunaan IMDSv2 (ditunjukkan oleh`"ec2:MetadataHttpTokens": "required"`). Jika Anda tidak menentukan bahwa instance memerlukan IMDSv2, Anda mendapatkan `Unauthorized0peration` kesalahan saat memanggil RunInstances API.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
```

```
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

Tolak opt-out IMDSv2

Kebijakan berikut menetapkan bahwa Anda tidak dapat memanggil `ModifyInstanceMetadataOptions` API dan mengizinkan opsi IMDSv1 atau IMDSv2. Jika Anda memanggil API `ModifyInstanceMetadataOptions`, atribut `HttpTokens` harus diatur ke `required`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
    }]
}
```

Menentukan batas hop maksimum

Kebijakan berikut menetapkan bahwa Anda tidak dapat memanggil RunInstances API kecuali Anda juga menentukan batas hop, dan batas hop tidak boleh lebih dari 3. Jika Anda gagal melakukan itu, Anda mendapatkan `Unauthorized0peration` kesalahan saat memanggil RunInstances API.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Batasi siapa saja yang dapat melakukan modifikasi terhadap opsi metadata instans

Kebijakan berikut hanya mengizinkan pengguna dengan peran `ec2-imds-admins` untuk melakukan perubahan pada opsi metadata instans. Jika ada prinsipal selain peran `ec2-imds-admins` mencoba untuk memerintahkan ModifyInstanceMetadataOptions API, eror `Unauthorized0peration` akan terjadi. Pernyataan ini dapat digunakan untuk mengontrol penggunaan ModifyInstanceMetadataOptions API; saat ini tidak ada kontrol akses (kondisi) berbutir halus untuk API. ModifyInstanceMetadataOptions

Memerlukan kredensi peran untuk diambil dari IMDSv2

Kebijakan berikut menetapkan bahwa jika kebijakan ini diterapkan pada peran, dan peran tersebut diasumsikan oleh layanan EC2 dan kredenal yang dihasilkan digunakan untuk menandatangani permintaan, maka permintaan tersebut harus ditandatangani oleh kredensi peran EC2 yang diambil dari. IMDSv2 Jika tidak, semua panggilan API akan mendapatkan kesalahan

`UnauthorizedOperation`. Pernyataan/kebijakan ini dapat diterapkan secara umum karena, jika permintaan tidak ditandatangani oleh kredensial peran EC2, maka tidak ada dampak yang terjadi.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Bekerja dengan volume dan snapshot Amazon EBS

Misalnya kebijakan untuk bekerja dengan volume dan snapshot Amazon EBS, lihat Contoh kebijakan berbasis identitas untuk Amazon EBS.

Contoh kebijakan untuk mengontrol akses ke konsol Amazon EC2

Anda dapat menggunakan kebijakan IAM untuk memberi pengguna izin yang diperlukan untuk bekerja dengan Amazon EC2. Untuk step-by-step petunjuk arah, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Konsol tersebut menggunakan tindakan-tindakan API tambahan untuk fitur-fiturnya, sehingga kebijakan-kebijakan ini mungkin tidak berjalan sesuai yang diharapkan. Sebagai contoh, seorang pengguna yang memiliki izin untuk hanya menggunakan tindakan API `DescribeVolumes` akan mendapati kesalahan saat mencoba melihat volume dalam konsol. Bagian ini akan menunjukkan kebijakan-kebijakan yang memungkinkan para pengguna untuk menggunakan bagian tertentu dari konsol. Untuk informasi tambahan tentang membuat kebijakan untuk konsol Amazon EC2, lihat

postingan Blog AWS Keamanan berikut: Memberikan Izin kepada Pengguna untuk Bekerja di Konsol Amazon EC2.

Contoh berikut menunjukkan pernyataan kebijakan yang dapat Anda gunakan untuk memberikan izin kepada pengguna untuk menggunakan Amazon EC2. Ganti masing-masing *user input placeholder* dengan informasi Anda sendiri. Kebijakan ini dirancang untuk permintaan yang dibuat menggunakan Konsol Manajemen AWS. Konsol Amazon EC2 mungkin memanggil beberapa tindakan API untuk menampilkan satu sumber daya, dan mungkin tidak jelas sampai pengguna mencoba tugas dan konsol menampilkan kesalahan. Untuk informasi selengkapnya, lihat postingan Blog AWS Keamanan berikut: Memberikan Izin kepada Pengguna untuk Bekerja di Konsol Amazon EC2.

Contoh

- Contoh: Akses hanya-baca
- Contoh: Menggunakan wizard peluncuran instans EC2
- Contoh: Cara menggunakan grup keamanan
- Contoh: Cara menggunakan alamat IP Elastis
- Contoh: Cara Menggunakan Instans Cadangan

Untuk membantu mengetahui tindakan API mana yang diperlukan untuk melakukan tugas di konsol, Anda dapat menggunakan layanan yang mencatat panggilan, seperti AWS CloudTrail. Jika kebijakan Anda tidak memberikan izin untuk membuat atau melakukan modifikasi terhadap sumber daya tertentu, maka konsol akan menampilkan pesan berenkode yang memuat informasi diagnostik. Anda dapat memecahkan kode pesan menggunakan tindakan DecodeAuthorizationMessageAPI untuk AWS STS, atau decode-authorization-messageperintah di. AWS CLI

Contoh: Akses hanya-baca

Untuk memungkinkan para pengguna menampilkan semua sumber daya dalam konsol Amazon EC2, Anda dapat menggunakan kebijakan yang sama seperti contoh berikut ini: Contoh: Akses hanya-baca. Para pengguna tidak dapat melakukan tindakan apa pun pada sumber daya tersebut atau membuat sumber daya baru, kecuali bila ada pernyataan lain yang memberikan izin kepada mereka untuk melakukan hal itu.

Lihat contoh, AMIs, dan snapshot

Atau, Anda dapat memberikan akses hanya-baca ke subset sumber daya. Untuk melakukan hal ini, ganti wildcard * dalam tindakan API `ec2:Describe` dengan tindakan `ec2:Describe`

tertentu untuk masing-masing sumber daya. Kebijakan berikut ini akan memungkinkan para pengguna untuk menampilkan semua instans, AMI, dan snapshot dalam konsol Amazon EC2. `ec2:DescribeTags`Tindakan ini memungkinkan pengguna untuk melihat publikAMIs. Konsol memerlukan informasi penandaan untuk menampilkan publik AMIs; namun, Anda dapat menghapus tindakan ini untuk memungkinkan pengguna hanya melihat pribadiAMIs.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
         "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
   }
   ]
}
```

> **Note**
>
> Tindakan API `ec2:Describe*` Amazon EC2 tidak mendukung izin tingkat sumber daya, sehingga Anda tidak dapat mengontrol sumber daya individu mana yang dapat dilihat oleh pengguna dalam konsol. Oleh karena itu, wildcard * dibutuhkan dalam elemen `Resource` pada pernyataan di atas. Untuk informasi selengkapnya tentang ARN mana yang dapat Anda gunakan bersama dengan tindakan API Amazon EC2 yang mana, lihat Tindakan, sumber daya, dan kunci syarat untuk Amazon EC2.

Lihat contoh dan metrik CloudWatch

Kebijakan berikut memungkinkan pengguna untuk melihat instans dalam konsol Amazon EC2, serta alarm dan metrik CloudWatch dalam tab Monitoring dari halaman Instances. Konsol Amazon EC2 menggunakan CloudWatch API untuk menampilkan alarm dan metrik, jadi

Anda harus memberi pengguna izin untuk menggunakan`cloudwatch:DescribeAlarms`,,, `cloudwatch:DescribeAlarmsForMetric``cloudwatch:ListMetrics`, `cloudwatch:GetMetricStatistics` dan tindakan. `cloudwatch:GetMetricData`

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
         "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
   }
   ]
}
```

Contoh: Menggunakan wizard peluncuran instans EC2

Wizard peluncuran instans Amazon EC2 adalah layar yang menampilkan opsi untuk melakukan konfigurasi dan meluncurkan instans. Kebijakan Anda harus menyertakan izin untuk menggunakan tindakan API yang memungkinkan para pengguna untuk menggunakan opsi-opsi yang ditampilkan pemandu. Jika kebijakan Anda tidak menyertakan izin untuk menggunakan tindakan tersebut, beberapa item dalam pemandu tidak akan dapat dimuat dengan benar, dan pengguna tidak akan dapat menyelesaikan peluncuran.

Akses wizard peluncuran instans dasar

Agar berhasil menyelesaikan peluncuran, para pengguna harus diberi izin untuk menggunakan tindakan API `ec2:RunInstances`, dan setidaknya tindakan-tindakan API berikut ini:

- `ec2:DescribeImages`: Untuk menampilkan dan memilih AMI.
- `ec2:DescribeInstanceTypes`: Untuk menampilkan dan memilih tipe instans.

- `ec2:DescribeVpcs`: Untuk menampilkan opsi-opsi jaringan yang tersedia.
- `ec2:DescribeSubnets`: Untuk menampilkan semua subnet yang tersedia untuk VPC yang dipilih.
- `ec2:DescribeSecurityGroups` atau `ec2:CreateSecurityGroup`: Untuk menampilkan dan memilih grup keamanan yang sudah ada, atau untuk membuat grup keamanan yang baru.
- `ec2:DescribeKeyPairs` atau `ec2:CreateKeyPair`: Untuk memilih pasangan kunci yang sudah ada, atau untuk membuat pasangan kunci yang baru.
- `ec2:AuthorizeSecurityGroupIngress`: Untuk menambahkan aturan ke dalam.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

Anda dapat menambahkan tindakan-tindakan API pada kebijakan Anda untuk menyediakan lebih banyak opsi bagi para pengguna, sebagai contoh:

- `ec2:DescribeAvailabilityZones`: Untuk menampilkan dan memilih Zona Ketersediaan tertentu.
- `ec2:DescribeNetworkInterfaces`: Untuk menampilkan dan memilih antarmuka jaringan yang sudah ada untuk subnet yang dipilih.
- Untuk menambahkan aturan-aturan ke luar untuk grup keamanan VPC, para pengguna harus mendapatkan izin untuk menggunakan tindakan API `ec2:AuthorizeSecurityGroupEgress`. Untuk melakukan modifikasi atau menghapus aturan-aturan yang sudah ada, para pengguna harus diberi izin untuk menggunakan tindakan API `ec2:RevokeSecurityGroup*` yang relevan.
- `ec2:CreateTags`: Untuk memberikan tanda pada sumber daya yang dibuat oleh `RunInstances`. Untuk informasi selengkapnya, lihat Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan. Jika pengguna tidak memiliki izin untuk menggunakan tindakan ini dan mereka berusaha untuk menerapkan tanda di halaman penandaan wizard peluncuran instans, maka peluncuran akan gagal.

  > **Important**
  >
  > Menentukan Nama saat meluncurkan instans membuat tanda dan memerlukan tindakan `ec2:CreateTags`. Anda harus berhati-hati dalam memberikan izin kepada para pengguna untuk menggunakan tindakan `ec2:CreateTags`, karena tindakan itu akan membatasi kemampuan Anda untuk menggunakan kunci syarat `aws:ResourceTag` untuk membatasi penggunaan sumber daya yang lain. Jika Anda memberikan izin kepada para pengguna untuk menggunakan tindakan `ec2:CreateTags`, mereka dapat mengubah tanda dari sumber daya untuk menembus pembatasan-pembatasan tersebut. Untuk informasi selengkapnya, lihat Kontrol akses menggunakan akses berbasis atribut.

- Untuk menggunakan parameter Systems Manager saat Anda memilih AMI, Anda harus menambahkan `ssm:DescribeParameters` dan `ssm:GetParameters` pada kebijakan. `ssm:DescribeParameters` memberikan izin kepada pengguna untuk melihat dan memilih parameter Systems Manager. `ssm:GetParameters` memberikan izin kepada pengguna untuk mendapatkan nilai dari parameter Systems Manager. Anda juga dapat membatasi akses ke parameter Systems Manager tertentu. Untuk informasi selengkapnya, lihat Membatasi akses ke parameter Systems Manager tertentu yang juga ada dalam bagian ini.

Saat ini, tindakan API `Describe*` Amazon EC2 tidak mendukung izin tingkat sumber daya, sehingga Anda tidak dapat membatasi sumber daya individu mana yang dapat dilihat dalam wizard peluncuran instans. Akan tetapi, Anda dapat menerapkan izin tingkat sumber daya pada tindakan API `ec2:RunInstances` untuk membatasi sumber daya mana yang dapat digunakan oleh para pengguna untuk meluncurkan instans. Peluncuran tersebut akan gagal jika pengguna memilih opsi-opsi yang tidak mendapatkan otorisasi untuk digunakan.

Membatasi akses ke tipe instans, subnet, dan Wilayah tertentu

Kebijakan berikut memungkinkan pengguna untuk meluncurkan instans `t2.micro` menggunakan AMIs yang dimiliki oleh Amazon, dan hanya ke dalam subnet khusus (`subnet-1a2b3c4d`). Pengguna hanya dapat meluncurkan di Wilayah yang ditentukan. Jika pengguna memilih Wilayah yang berbeda, atau memilih tipe instans, AMI, atau subnet yang berbeda dalam wizard peluncuran instans, maka peluncuran akan gagal.

Pernyataan pertama memberikan izin kepada pengguna untuk melihat opsi dalam wizard peluncuran instans atau untuk membuat yang baru, sebagaimana yang telah dijelaskan dalam contoh di atas. Pernyataan kedua memberikan izin kepada para pengguna untuk menggunakan antarmuka jaringan, volume, pasangan kunci, grup keamanan, dan sumber daya subnet untuk tindakan `ec2:RunInstances`, yang diperlukan untuk meluncurkan instans ke dalam VPC. Untuk informasi selengkapnya tentang penggunaan tindakan `ec2:RunInstances`, lihat Luncurkan instance () RunInstances. Pernyataan ketiga dan keempat memberikan izin kepada pengguna untuk menggunakan masing-masing instans dan sumber daya AMI, tetapi hanya jika instans tersebut adalah instans `t2.micro`, serta hanya jika AMI tersebut dimiliki oleh Amazon atau partner tertentu yang tepercaya dan terverifikasi.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
         "ec2:CreateKeyPair",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets", "ec2:DescribeSecurityGroups",
```

```
            "ec2:CreateSecurityGroup",
            "ec2:AuthorizeSecurityGroupIngress"
        ],
        "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action":"ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-2:111122223333:network-interface/*",
                "arn:aws:ec2:us-east-2:111122223333:volume/*",
                "arn:aws:ec2:us-east-2:111122223333:key-pair/*",
                "arn:aws:ec2:us-east-2:111122223333:security-group/*",
                "arn:aws:ec2:us-east-2:111122223333:subnet/subnet-1a2b3c4d"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-2:111122223333:instance/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:InstanceType": "t2.micro"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                    "arn:aws:ec2:us-east-2::image/ami-*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Owner": "amazon"
                }
            }
        }
        ]
}
```

Membatasi akses ke parameter Systems Manager tertentu

Kebijakan berikut ini memberikan akses untuk menggunakan parameter-parameter Systems Manager yang memiliki nama tertentu.

Pernyataan pertama memberikan izin kepada pengguna untuk menampilkan parameter Systems Manager saat memilih AMI dalam wizard peluncuran instans. Pernyataan kedua memberikan izin kepada para pengguna untuk menggunakan parameter yang mempunyai nama `prod-*`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123456:parameter/prod-*"
   }
   ]
}
```

Contoh: Cara menggunakan grup keamanan

Menampilkan grup keamanan dan menambah serta menghapus aturan

Kebijakan berikut ini memberikan izin kepada para pengguna untuk menampilkan grup keamanan di konsol Amazon EC2, untuk menambahkan dan menghapus aturan ke dalam dan ke luar, dan untuk mencantumkan serta melakukan modifikasi terhadap deskripsi aturan untuk grup keamanan yang sudah ada yang memiliki tanda `Department=Test`.

Dalam pernyataan pertama, tindakan `ec2:DescribeTags` akan memungkinkan para pengguna untuk menampilkan tanda dalam konsol, yang dapat mempermudah para pengguna untuk mengidentifikasi grup keamanan yang diizinkan untuk dimodifikasi.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:AuthorizeSecurityGroupIngress",
         "ec2:RevokeSecurityGroupIngress",
         "ec2:AuthorizeSecurityGroupEgress",
         "ec2:RevokeSecurityGroupEgress",
         "ec2:ModifySecurityGroupRules",
         "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
         "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-2:111122223333:security-group/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/Department": "Test"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
         "ec2:ModifySecurityGroupRules"
      ],
```

```
      "Resource": [
         "arn:aws:ec2:us-east-2:111122223333:security-group-rule/*"
      ]
   }
]}
```

Cara menggunakan kotak dialog Buat Grup Keamanan

Anda dapat membuat kebijakan yang memungkinkan para pengguna untuk menggunakan kotak dialog Buat Grup Keamanan yang ada dalam konsol Amazon EC2. Untuk menggunakan kotak dialog ini, para pengguna harus diberi izin untuk menggunakan setidaknya tindakan-tindakan API berikut ini:

- `ec2:CreateSecurityGroup`: Untuk membuat grup keamanan yang baru.
- `ec2:DescribeVpcs`: Untuk melihat daftar yang ada VPCs di daftar VPC.

Dengan izin tersebut, para pengguna dapat membuat grup keamanan baru dengan sukses, tetapi mereka tidak akan dapat menambahkan aturan apa pun pada grup keamanan tersebut. Untuk menggunakan aturan-aturan yang ada dalam kotak dialog Buat Grup Keamanan, Anda dapat menambahkan tindakan-tindakan API berikut pada kebijakan Anda:

- `ec2:AuthorizeSecurityGroupIngress`: Untuk menambahkan aturan ke dalam.
- `ec2:AuthorizeSecurityGroupEgress`: Untuk menambahkan aturan ke luar pada grup keamanan VPC.
- `ec2:RevokeSecurityGroupIngress`: Untuk melakukan modifikasi atau membuang aturan ke dalam yang sudah ada. Tindakan-tindakan ini berguna untuk memungkinkan para pengguna menggunakan fitur Salin ke yang baru yang ada dalam konsol. Fitur ini akan membuka kotak dialog Buat Grup Keamanan dan mengisinya dengan aturan-aturan yang sama seperti grup keamanan yang sudah dipilih.
- `ec2:RevokeSecurityGroupEgress`: Untuk melakukan modifikasi atau penghapusan terhadap aturan-aturan ke luar untuk grup keamanan VPC. Hal ini berguna untuk memungkinkan para pengguna untuk melakukan modifikasi terhadap atau menghapus aturan ke luar default yang mengizinkan semua lalu lintas ke luar.
- `ec2:DeleteSecurityGroup`: Untuk melayani ketika aturan-aturan yang tidak valid tidak dapat disimpan. Pertama-tama konsol akan membuat grup keamanan, kemudian akan menambahkan aturan-aturan tertentu. Jika aturan tidak valid, maka tindakan tersebut akan gagal, dan konsol akan mencoba menghapus grup keamanan. Para pengguna akan tetap berada dalam kotak dialog

Buat Grup Keamanan sehingga mereka dapat melakukan koreksi atas aturan-aturan yang tidak valid dan mencoba membuat grup keamanan lagi. Tindakan API ini tidak diperlukan, tetapi jika seorang pengguna tidak diberikan izin untuk menggunakannya dan berusaha untuk membuat grup keamanan dengan aturan-aturan yang tidak valid, maka grup keamanan akan dibuat tanpa aturan apa pun, dan pengguna tersebut harus menambahkan aturan-aturan setelahnya.

- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: Untuk menambahkan atau memperbarui deskripsi aturan grup keamanan ingress (ke dalam).
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: Untuk menambahkan atau memperbarui deskripsi aturan grup keamanan egress (ke luar).
- `ec2:ModifySecurityGroupRules`: Untuk mengubah aturan grup keamanan.
- `ec2:DescribeSecurityGroupRules`: Untuk mencantumkan aturan grup keamanan.

Kebijakan berikut ini akan memberikan izin kepada para pengguna untuk menggunakan kotak dialog Buat Grup Keamanan dan untuk membuat aturan-aturan ke dalam dan ke luar untuk grup keamanan yang dikaitkan dengan VPC tertentu (`vpc-1a2b3c4d`). Pengguna dapat membuat grup keamanan untuk VPC, tetapi mereka tidak dapat menambahkan aturan apa pun pada grup keamanan tersebut. Demikian pula, para pengguna tidak dapat menambahkan aturan apa pun ke grup keamanan yang ada yang tidak dikaitkan dengan VPC `vpc-1a2b3c4d`. Para pengguna juga diberikan izin untuk menampilkan semua grup keamanan di konsol. Hal ini akan mempermudah para pengguna untuk mengidentifikasi grup keamanan yang padanya dapat mereka tambahkan aturan-aturan ke dalam. Kebijakan ini juga memberikan izin kepada para pengguna untuk menghapus grup keamanan yang dikaitkan dengan VPC `vpc-1a2b3c4d`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:us-east-2:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:us-east-2:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
    }
   ]
}
```

Contoh: Cara menggunakan alamat IP Elastis

Untuk memungkinkan para pengguna menampilkan alamat IP Elastis dalam konsol Amazon EC2, Anda harus memberikan izin kepada para pengguna untuk menggunakan tindakan `ec2:DescribeAddresses`.

Agar pengguna dapat menggunakan alamat IP Elastis, Anda dapat menambahkan tindakan-tindakan berikut pada kebijakan Anda.

- `ec2:AllocateAddress`: Untuk mengalokasikan alamat IP Elastis.
- `ec2:ReleaseAddress`: Untuk merilis alamat IP Elastis.
- `ec2:AssociateAddress`: Untuk mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan.
- `ec2:DescribeNetworkInterfaces` dan `ec2:DescribeInstances`: Untuk menggunakan layar Kaitkan alamat. Layar tersebut akan menampilkan instans atau antarmuka jaringan yang tersedia yang bisa Anda gunakan untuk mengaitkan alamat IP Elastis.
- `ec2:DisassociateAddress`: Untuk melepaskan pengaitan alamat IP Elastis dari instans atau antarmuka jaringan.

Kebijakan berikut ini akan memungkinkan para pengguna untuk menampilkan, mengalokasikan, dan mengaitkan alamat IP Elastis dengan instans. Para pengguna tidak dapat mengaitkan alamat IP Elastis dengan antarmuka jaringan, melepaskan pengaitan alamat IP Elastis, atau merilisnya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Cara Menggunakan Instans Cadangan

Kebijakan berikut mengizinkan pengguna untuk menampilkan dan memodifikasi Instans Terpesan dalam akun Anda, serta membeli Instans Terpesan baru dalam Konsol Manajemen AWS.

Kebijakan ini akan memungkinkan para pengguna untuk menampilkan semua Instans Cadangan, serta Instans Sesuai Permintaan, dalam akun tersebut. Pengaturan izin tingkat sumber daya untuk masing-masing Instans Cadangan tidak dapat dilakukan.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
         "ec2:PurchaseReservedInstancesOffering",
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeAvailabilityZones",
```

```
            "ec2:DescribeReservedInstancesOfferings"
        ],
        "Resource": "*"
    }
    ]
}
```

Tindakan `ec2:DescribeAvailabilityZones` dibutuhkan untuk memastikan bahwa konsol Amazon EC2 dapat menampilkan informasi tentang Zona Ketersediaan di mana Anda dapat membeli Instans Cadangan. Tindakan `ec2:DescribeInstances` tidak diperlukan, tetapi dapat memastikan bahwa pengguna dapat menampilkan instans dalam akun dan membeli cadangan agar sesuai dengan spesifikasi yang semestinya.

Anda dapat menyesuaikan tindakan API untuk membatasi akses pengguna, sebagai contoh, menghapus `ec2:DescribeInstances` dan `ec2:DescribeAvailabilityZones` artinya pengguna memiliki akses hanya-baca.

AWS kebijakan terkelola untuk Amazon EC2

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di AWS akun Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWS kebijakan terkelola: AmazonEC2FullAccess

Anda dapat melampirkan kebijakan `AmazonEC2FullAccess` ke identitas-identitas IAM Anda. Kebijakan ini akan memberikan izin yang mengizinkan akses penuh ke Amazon EC2.

Untuk melihat izin kebijakan ini, lihat AmazonEC2FullAccessdi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonEC2ReadOnlyAccess

Anda dapat melampirkan kebijakan `AmazonEC2ReadOnlyAccess` ke identitas-identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan akses hanya-baca ke Amazon EC2.

Untuk melihat izin kebijakan ini, lihat AmazonEC2ReadOnlyAccessdi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonEC2ImageReferencesAccessPolicy

Anda dapat melampirkan kebijakan `AmazonEC2ImageReferencesAccessPolicy` ke identitas IAM Anda. Kebijakan ini memberikan izin yang diperlukan untuk menggunakan DescribeImageReferences API EC2, termasuk izin untuk melihat instans EC2, template peluncuran, parameter Systems Manager, dan resep Image Builder. Kebijakan mendukung `IncludeAllResourceTypes` bendera dan akan terus berfungsi saat AWS menambahkan dukungan untuk jenis sumber daya baru, sehingga menghilangkan kebutuhan akan pembaruan kebijakan di masa mendatang.

Untuk melihat izin kebijakan ini, lihat AmazonEC2ImageReferencesAccessPolicydi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSEC2CapacityReservationFleetRolePolicy

Kebijakan ini dilampirkan pada peran terkait layanan yang diberi nama AWSServiceRoleForEC2CapacityReservationFleetuntuk memungkinkan layanan membuat, memodifikasi, dan membatalkan Reservasi Kapasitas dalam Armada Reservasi Kapasitas atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran tertaut layanan untuk Armada Reservasi Kapasitas.

Untuk melihat izin kebijakan ini, lihat AWSEC2CapacityReservationFleetRolePolicydi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSEC2FleetServiceRolePolicy

Kebijakan ini dilampirkan pada peran tertaut layanan yang mempunyai nama AWSServiceRoleForEC2Fleet untuk mengizinkan Armada EC2 meminta, meluncurkan, mengakhiri,

dan memberi tanda pada instans atas nama Anda. Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk Armada EC2.

Untuk melihat izin kebijakan ini, lihat AWSEC2FleetServiceRolePolicydi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSEC2SpotFleetServiceRolePolicy

Kebijakan ini dilampirkan pada peran tertaut layanan yang mempunyai nama AWSServiceRoleForEC2SpotFleet untuk mengizinkan Armada Spot meluncurkan dan mengelola instans atas nama Anda. Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk Armada Spot.

Untuk melihat izin kebijakan ini, lihat AWSEC2SpotFleetServiceRolePolicydi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSEC2SpotServiceRolePolicy

Kebijakan ini dilampirkan pada peran tertaut layanan yang mempunyai nama AWSServiceRoleForEC2Spot untuk mengizinkan Amazon EC2 meluncurkan dan mengelola Instans Spot atas nama Anda. Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk permintaan Instans Spot.

Untuk melihat izin kebijakan ini, lihat AWSEC2SpotServiceRolePolicydi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSEC2VssSnapshotPolicy

Anda dapat melampirkan kebijakan terkelola ini ke peran profil instans IAM yang Anda gunakan untuk instans Windows Amazon EC2. Kebijakan ini memberikan izin untuk mengizinkan Amazon EC2 membuat dan mengelola snapshot VSS atas nama Anda.

Untuk melihat izin kebijakan ini, lihat AWSEC2VssSnapshotPolicydi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: DeclarativePoliciesEC2Report

Kebijakan ini dilampirkan ke peran terkait layanan yang diberi nama `AWSServiceRoleForDeclarativePoliciesEC2Report` untuk menyediakan akses ke hanya-baca yang APIs diperlukan untuk menghasilkan laporan status akun untuk kebijakan deklaratif.

Untuk melihat izin kebijakan ini, lihat DeclarativePoliciesEC2Reportdi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: EC2FastLaunchFullAccess

Anda dapat melampirkan `EC2FastLaunchFullAccess` kebijakan ke profil instans atau peran IAM lainnya. Kebijakan ini memberikan akses penuh ke tindakan Peluncuran Cepat EC2, dan izin yang ditargetkan sebagai berikut.

Detail izin

- Peluncuran Cepat EC2 — Akses administratif diberikan, sehingga peran dapat mengaktifkan atau menonaktifkan Peluncuran Cepat EC2, dan menggambarkan gambar Peluncuran Cepat EC2.
- Amazon EC2 — Akses diberikan untuk operasi Amazon RunInstances EC2CreateTags,, Jelaskan, dan Buat dan Ubah Peluncuran Template. Akses juga diberikan untuk membuat sumber daya jaringan dan grup keamanan, mengotorisasi aturan masuk, dan menghapus sumber daya yang dibuat oleh Peluncuran Cepat EC2.
- IAM — Akses diberikan untuk mendapatkan dan menggunakan profil instance yang namanya berisi `ec2fastlaunch` untuk membuat peran EC2FastLaunchServiceRolePolicy terkait layanan.
- CloudFormation— Akses diberikan untuk EC2 Fast Launch untuk mendeskripsikan dan membuat CloudFormation tumpukan, dan untuk menghapus tumpukan yang dibuatnya.

Untuk melihat izin kebijakan ini, lihat EC2FastLaunchFullAccessdi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSEC2CapacityManagerServiceRolePolicy

Kebijakan ini dilampirkan pada peran terkait layanan yang diberi nama AWSServiceRoleForEC2CapacityManageruntuk memungkinkan Manajer Kapasitas EC2 mengelola sumber daya kapasitas dan berintegrasi dengan AWS Organizations atas nama Anda. Untuk informasi selengkapnya, lihat Peran terkait layanan untuk Manajer Kapasitas EC2.

Untuk melihat izin kebijakan ini, lihat AWSEC2CapacityManagerServiceRolePolicydi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: EC2FastLaunchServiceRolePolicy

Kebijakan ini dilampirkan ke peran terkait layanan yang diberi nama AWSServiceRoleForEC2FastLaunchuntuk memungkinkan Amazon EC2 membuat dan mengelola

sekumpulan snapshot yang telah disediakan sebelumnya yang mengurangi waktu yang diperlukan untuk meluncurkan instans dari AMI berkemampuan Peluncuran Cepat EC2 Anda. Untuk informasi selengkapnya, lihat the section called “Peran tertaut layanan”.

Untuk melihat izin kebijakan ini, lihat EC2FastLaunchServiceRolePolicydi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: Ec2InstanceConnect

Anda dapat melampirkan kebijakan `Ec2InstanceConnect` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan pelanggan memanggil EC2 Instance Connect untuk mempublikasikan kunci sementara ke instans EC2 mereka dan terhubung melalui ssh atau CLI Instans Connect EC2.

Untuk melihat izin kebijakan ini, lihat Ec2InstanceConnectdi Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: Ec2InstanceConnectEndpoint

Kebijakan ini dilampirkan ke peran terkait layanan yang diberi nama AWSServiceRoleForEC2InstanceConnectuntuk mengizinkan Titik Akhir Koneksi Instans EC2 melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk EC2 Instance Connect Endpoint.

Untuk melihat izin kebijakan ini, lihat Ec2InstanceConnectEndpointdi Referensi Kebijakan AWS Terkelola. Untuk penjelasan tentang pembaruan kebijakan ini, lihatPembaruan Amazon EC2 ke AWS kebijakan terkelola.

Pembaruan Amazon EC2 ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon EC2 sejak layanan ini mulai melacak perubahan ini.

Ubah	Deskripsi	Date
AWSEC2CapacityManagerServiceRolePolicy – Kebijakan baru	Amazon EC2 menambahkan kebijakan ini untuk memungkinkan Anda mengelola sumber daya kapasitas dan berintegrasi dengan AWS Organizations atas nama Anda.	Oktober 15, 2025

Ubah	Deskripsi	Date
AmazonEC2ImageReferencesAccessPolicy – Kebijakan baru	Amazon EC2 menambahkan kebijakan ini untuk memberikan izin untuk memindai semua jenis sumber daya yang didukung oleh API DescribeImageReferences EC2.	Agustus 26, 2025
Ec2InstanceConnectEndpoint— Kebijakan yang diperbarui	Untuk mendukung modifikasi Titik Akhir Instance Connect yang ada, Amazon EC2 memperbarui kebijakan ini untuk menambahkan izin untuk menetapkan dan membatalkan penetapan alamat IPv6 serta memodifikasi grup keamanan pada antarmuka jaringan yang dibuat oleh EC2 Instance Connect Endpoint. Amazon EC2 juga memperbarui kebijakan ini untuk mengganti operator `Null` kondisi dengan operator `StringLike` kondisi.	Juli 31, 2025

Ubah	Deskripsi	Date
EC2FastLaunchServiceRolePolicy— Kebijakan yang diperbarui	Untuk membantu mencegah sumber daya yatim piatu, Amazon EC2 memperbarui kebijakan ini untuk menambahkan izin untuk mendeskripsikan volume, atribut volume, dan antarmuka jaringan, serta menghapus volume dan antarmuka jaringan yang dibuat oleh Peluncuran Cepat EC2.	Juli 17, 2025
EC2FastLaunchFullAccess— Kebijakan yang diperbarui	Amazon EC2 memperbarui kebijakan ini untuk menyertakan operasi Buat dan Ubah Peluncuran Template, untuk membuat sumber daya jaringan dan grup keamanan, mengotorisasi aturan masuk, dan menghapus sumber daya yang dibuat oleh Peluncuran Cepat EC2. Ini juga dapat menggambarkan dan membuat CloudFormation tumpukan, dan menghapus tumpukan yang dibuat oleh Peluncuran Cepat EC2.	14 Mei 2025

Ubah	Deskripsi	Date
EC2FastLaunchServiceRolePolicy— Kebijakan yang diperbarui	Amazon EC2 memperbarui kebijakan ini untuk menambahkan EventBridge akses Amazon untuk membuat dan mengelola aturan acara untuk Peluncuran Cepat EC2. Selain itu, EC2 Fast Launch sekarang dapat menjelaskan CloudFormation tumpukan, meluncurkan instance dari AMI yang terkait dengannya AWS License Manager, mendapatkan daftar AWS KMS hibah yang dibuatnya yang dapat dihentikan, dan menghapus template peluncuran yang dibuatnya.	14 Mei 2025
AWSEC2CapacityReservationFleetRolePolicy— Izin yang diperbarui	Amazon EC2 memperbarui kebijakan `AWSEC2CapacityReservationFleetRolePolicy` terkelola untuk menggunakan operator `ArnLike` kondisi, bukan operator `StringLike` kondisi.	Maret 03, 2025
AmazonEC2ReadOnlyAccess— Izin Ditambahkan	Amazon EC2 menambahkan izin yang memungkinkan Anda mengambil grup keamanan menggunakan operasi. `GetSecurityGroupsForVpc`	Desember 27, 2024

Ubah	Deskripsi	Date
EC2FastLaunchFullAccess – Kebijakan baru	Amazon EC2 menambahkan kebijakan ini untuk melakukan tindakan API yang terkait dengan fitur Peluncuran Cepat EC2 dari instans. Kebijakan ini dapat dilampirkan ke profil instans untuk instance yang diluncurkan dari AMI yang diaktifkan Peluncuran Cepat EC2.	14 Mei 2024
AWSEC2VssSnapshotPolicy – Kebijakan baru	Amazon EC2 menambahkan `AWSEC2VssSnapshotPolicy` kebijakan yang berisi izin untuk membuat dan menambahkan tag ke Amazon Machine Images (AMIs) dan snapshot EBS.	Maret 28, 2024
Ec2InstanceConnectEndpoint – Kebijakan baru	Amazon EC2 menambahkan kebijakan. `Ec2InstanceConnectEndpoint` Kebijakan ini dilampirkan ke peran AWSServiceRoleForEC2InstanceConnectterkait layanan, untuk memungkinkan Amazon EC2 melakukan tindakan atas nama Anda saat Anda membuat Titik Akhir Koneksi Instans EC2.	Januari 24, 2023

Ubah	Deskripsi	Date
EC2FastLaunchServiceRolePolicy – Kebijakan baru	Amazon EC2 menambahkan fitur Peluncuran Cepat EC2 untuk memungkinkan Windows AMIs meluncurkan instans lebih cepat dengan membuat serangkaian snapshot yang telah disediakan sebelumnya.	26 November 2021
Amazon EC2 mulai melakukan pelacakan perubahan	Amazon EC2 mulai melacak perubahan pada kebijakan yang dikelola AWS	1 Maret 2021

IAM role untuk Amazon EC2

Aplikasi harus menandatangani permintaan API mereka dengan AWS kredensialnya. Oleh karena itu, jika Anda adalah seorang developer aplikasi, Anda membutuhkan strategi untuk mengelola kredensial untuk aplikasi-aplikasi Anda yang berjalan pada instans EC2. Sebagai contoh, Anda dapat mendistribusikan kredensial AWS Anda dengan aman ke instans, yang mana hal itu akan memungkinkan aplikasi-aplikasi pada instans tersebut untuk menggunakan kredensial Anda untuk menandatangani permintaan, sekaligus melindungi kredensial Anda dari pengguna lain. Namun, sulit untuk mendistribusikan kredensil secara aman ke setiap instans, terutama yang AWS dibuat atas nama Anda, seperti Instans Spot atau instans di grup Auto Scaling. Anda juga harus dapat memperbarui kredensional pada setiap instance ketika Anda memutar kredensional Anda. AWS

Kami merancang IAM role agar aplikasi-aplikasi Anda dapat membuat permintaan API dengan aman dari instans Anda, tanpa mengharuskan Anda mengelola kredensial keamanan yang digunakan oleh aplikasi-aplikasi tersebut. Alih-alih membuat dan mendistribusikan AWS kredensional Anda, Anda dapat mendelegasikan izin untuk membuat permintaan API menggunakan peran IAM sebagai berikut:

1. Buat peran IAM.
2. Tentukan akun atau AWS layanan mana yang dapat mengambil peran.
3. Tentukan tindakan dan sumber daya API mana yang dapat digunakan oleh aplikasi setelah peran tersebut diambil.

4. Tentukan peran saat Anda meluncurkan instans Anda, atau lampirkan peran tersebut ke instans yang sudah ada.
5. Buatlah aplikasi tersebut mengambil satu set kredensial sementara lalu gunakan kredensial tersebut.

Sebagai contoh, Anda dapat menggunakan IAM role untuk memberikan izin ke aplikasi-aplikasi yang berjalan pada instans Anda yang harus menggunakan bucket dalam Amazon Simple Storage Service (Amazon S3). Anda dapat menentukan izin untuk IAM role dengan membuat kebijakan dalam format JSON. Peran ini mirip dengan kebijakan yang Anda buat untuk pengguna. Jika Anda mengubah peran, maka perubahan itu akan disebarkan ke semua instans.

> **Note**
>
> Kredensi peran Amazon EC2 IAM tidak tunduk pada durasi sesi maksimum yang dikonfigurasi dalam peran. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Saat Anda membuat IAM role, kaitkan kebijakan IAM dengan hak akses paling rendah yang membatasi akses ke panggilan API tertentu yang diperlukan oleh aplikasi. Untuk Windows-to-Windows komunikasi, gunakan grup dan peran Windows yang terdefinisi dengan baik dan terdokumentasi dengan baik untuk memberikan akses tingkat aplikasi antara instance Windows. Grup dan peran memungkinkan pelanggan untuk menentukan izin aplikasi dengan hak akses paling rendah dan izin tingkat folder NTFS untuk membatasi akses ke persyaratan spesifik aplikasi.

Anda hanya dapat melampirkan satu IAM role saja ke instans, tapi Anda dapat melampirkan peran yang sama ke banyak instans. Untuk informasi selengkapnya tentang cara membuat dan menggunakan IAM role, lihat Peran dalam Panduan Pengguna IAM.

Anda dapat menerapkan izin tingkat sumber daya pada kebijakan IAM Anda untuk mengontrol kemampuan pengguna dalam melampirkan, mengganti, atau melepaskan IAM role yang dilampirkan ke instans. Untuk informasi selengkapnya, lihat Izin tingkat sumber daya yang mendukung tindakan API Amazon EC2 dan contoh berikut ini: Contoh: Cara Menggunakan IAM role.

Daftar Isi

- Profil instans
- Izin untuk kasus penggunaan Anda

- Mengambil kredensial keamanan dari metadata instans
- Berikan izin untuk melampirkan peran IAM ke instance
- Melampirkan IAM role ke instans
- Peran identitas instans untuk instans Amazon EC2

Profil instans

Amazon EC2 menggunakan profil instans sebagai kontainer untuk IAM role. Saat Anda membuat IAM role menggunakan konsol IAM, konsol akan membuat profil instans secara otomatis dan memberikan nama yang sama sesuai dengan perannya. Jika Anda menggunakan konsol Amazon EC2 untuk meluncurkan instans dengan IAM role atau untuk melampirkan IAM role ke instans, Anda dapat memilih peran tersebut berdasarkan daftar nama profil instans.

Jika Anda menggunakan API AWS CLI, atau AWS SDK untuk membuat peran, Anda membuat profil peran dan instance sebagai tindakan terpisah, dengan nama yang berpotensi berbeda. Jika Anda kemudian menggunakan AWS CLI, API, atau AWS SDK untuk meluncurkan instance dengan peran IAM atau melampirkan peran IAM ke instance, tentukan nama profil instance.

profil instans hanya dapat berisi satu IAM role saja. Anda dapat menyertakan peran IAM dalam beberapa profil instans.

Untuk memperbarui izin untuk sebuah instance, ganti profil instance-nya. Kami tidak menyarankan untuk menghapus peran dari profil instance, karena ada penundaan hingga satu jam sebelum perubahan ini berlaku.

Untuk informasi selengkapnya, lihat Menggunakan profil instans di Panduan Pengguna IAM.

Izin untuk kasus penggunaan Anda

Ketika Anda pertama kali membuat IAM role untuk aplikasi-aplikasi Anda, terkadang Anda mungkin harus memberikan izin melebihi yang diperlukan. Sebelum meluncurkan aplikasi Anda di lingkungan produksi Anda, Anda dapat membuat kebijakan IAM yang berbasis aktivitas akses untuk IAM role. IAM Access Analyzer meninjau AWS CloudTrail log Anda dan menghasilkan templat kebijakan yang berisi izin yang telah digunakan oleh peran dalam rentang tanggal yang ditentukan. Anda dapat menggunakan templat tersebut untuk membuat kebijakan terkelola dengan izin yang sangat terperinci dan kemudian melampirkan kebijakan itu ke IAM role. Dengan begitu, Anda hanya memberikan izin yang diperlukan peran untuk berinteraksi dengan AWS sumber daya untuk kasus

penggunaan spesifik Anda. Hal ini akan membantu Anda untuk lebih mematuhi praktik terbaik dalam memberikan hak akses paling rendah. Untuk informasi selengkapnya, lihat pembuatan kebijakan IAM Access Analyzer di Panduan Pengguna IAM.

Mengambil kredensial keamanan dari metadata instans

aplikasi pada instans akan mengambil kredensial keamanan yang disediakan oleh peran dari item metadata instans `iam/security-credentials/`role-name. Aplikasi ini diberi izin untuk tindakan-tindakan dan sumber daya yang telah Anda tentukan untuk peran tersebut melalui kredensial keamanan yang dikaitkan dengan peran tersebut. Kredensial keamanan ini bersifat sementara dan kami memutar kredensial tersebut secara otomatis. Kami menyediakan kredensial yang baru setidaknya lima menit sebelum kredensial lama kedaluwarsa.

Untuk informasi selengkapnya tentang metadata instans, lihat Gunakan metadata instans untuk mengelola instans EC2.

> **Warning**
>
> Jika Anda menggunakan layanan-layanan yang menggunakan metadata instans dengan IAM role, pastikan Anda tidak mengekspos kredensial Anda saat layanan-layanan tersebut melakukan panggilan HTTP atas nama Anda. Jenis layanan yang dapat mengekspos kredensil Anda termasuk proxy HTTP, layanan HTML/CSS validator, dan prosesor XHTML yang mendukung inklusi XHTML.

Untuk beban kerja Amazon EC2, sebaiknya Anda mengambil kredensial sesi menggunakan metode yang dijelaskan di bawah ini. Kredensial ini harus memungkinkan beban kerja Anda membuat permintaan API AWS , tanpa perlu menggunakan `sts:AssumeRole` untuk mengambil peran yang sama yang sudah dikaitkan dengan instans. Kecuali jika Anda perlu meneruskan tanda sesi untuk kontrol akses berbasis atribut (ABAC) atau meneruskan kebijakan sesi guna membatasi izin peran lebih lanjut, panggilan pengambilan peran tersebut tidak diperlukan karena panggilan tersebut membuat kumpulan baru kredensial sesi peran sementara yang sama.

Jika beban kerja menggunakan peran untuk mengambil dirinya sendiri, Anda harus membuat kebijakan kepercayaan yang secara eksplisit memungkinkan peran tersebut untuk mengambil dirinya sendiri. Jika Anda tidak membuat kebijakan kepercayaan, Anda mendapatkan `AccessDenied` kesalahan. Untuk informasi selengkapnya, lihat Memperbarui kebijakan kepercayaan peran di Panduan Pengguna IAM.

IMDSv2

Linux

Jalankan perintah berikut dari instance Linux Anda untuk mengambil kredensi keamanan untuk peran IAM.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda untuk mengambil kredenal keamanan untuk peran IAM.

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

IMDSv1

Linux

Jalankan perintah berikut dari instance Linux Anda untuk mengambil kredensi keamanan untuk peran IAM.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda untuk mengambil kredenal keamanan untuk peran IAM.

```
Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role-name
```

Berikut ini adalah output contoh. Jika Anda tidak dapat mengambil kredensi keamanan, lihat Saya tidak dapat mengakses kredensil keamanan sementara pada instans EC2 saya di Panduan Pengguna IAM.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

Untuk aplikasi, AWS CLI, dan Alat untuk PowerShell perintah Windows yang berjalan pada instance, Anda tidak perlu secara eksplisit mendapatkan kredensil keamanan sementara — AWS SDKs, AWS CLI, dan Alat untuk Windows PowerShell secara otomatis mendapatkan kredensil dari layanan metadata instans EC2 dan menggunakannya. Untuk membuat panggilan di luar instans menggunakan kredensial keamanan sementara (sebagai contoh, untuk menguji kebijakan IAM), Anda harus menyediakan kunci akses, kunci rahasia, dan token sesi. Untuk informasi selengkapnya, lihat Menggunakan Kredensil Keamanan Sementara untuk Meminta Akses ke AWS Sumber Daya di Panduan Pengguna IAM.

Berikan izin untuk melampirkan peran IAM ke instance

Identitas di Anda Akun AWS, seperti pengguna IAM, harus memiliki izin khusus untuk meluncurkan instans Amazon EC2 dengan peran IAM, melampirkan peran IAM ke instance, mengganti peran IAM untuk sebuah instance, atau melepaskan peran IAM dari sebuah instance. Anda harus memberikan izin untuk menggunakan tindakan API berikut seperti yang diperlukan:

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:DisassociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

> **Note**
>
> Jika Anda menentukan sumber daya untuk `iam:PassRole` as*, ini akan memberikan akses untuk meneruskan peran IAM Anda ke sebuah instance. Untuk mengikuti praktik terbaik dengan hak istimewa terkecil, tentukan peran IAM tertentu dengan`iam:PassRole`, seperti yang ditunjukkan dalam contoh kebijakan di bawah ini. ARNs

Contoh kebijakan untuk akses terprogram

Kebijakan IAM berikut memberikan izin untuk meluncurkan instans dengan peran IAM, melampirkan peran IAM ke instance, atau mengganti peran IAM untuk instans menggunakan atau Amazon EC2 API. AWS CLI

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:DisassociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

Persyaratan tambahan untuk akses konsol

Untuk memberikan izin untuk menyelesaikan tugas yang sama menggunakan konsol Amazon EC2, Anda juga harus menyertakan tindakan API`iam:ListInstanceProfiles`.

Melampirkan IAM role ke instans

Anda dapat membuat IAM role dan melampirkan peran itu ke instans selama atau setelah peluncuran dilakukan. Anda juga dapat mengganti atau melepaskan peran IAM.

Membuat dan melampirkan peran IAM selama peluncuran instance (Disarankan)

1. Selama peluncuran instans EC2, perluas Detail lanjutan.
2. Di bagian profil instans IAM, pilih Buat peran IAM baru.
3. Formulir pembuatan peran inline terbuka, memungkinkan Anda untuk:
   - Tentukan nama Peran (misalnya,`EC2-S3-Access-Role`)
   - Tentukan izin dengan memilih kebijakan AWS terkelola atau membuat kebijakan khusus untuk instans Anda

     Misalnya, untuk memberikan akses S3, pilih kebijakan `AmazonS3ReadOnlyAccess` terkelola
   - Tinjau kebijakan kepercayaan yang memungkinkan `ec2.amazonaws.com` untuk mengambil peran
   - Tambahkan tag opsional untuk metadata
4. Pilih Buat peran.

   Peran yang baru dibuat dipilih secara otomatis dan akan dilampirkan ke instance Anda melalui profil instance saat instance diluncurkan.

> **Note**
>
> Saat Anda membuat peran menggunakan konsol selama peluncuran instance, profil instance dengan nama yang sama dengan peran akan dibuat secara otomatis. Profil instance adalah wadah yang meneruskan informasi peran IAM ke instance saat diluncurkan.

Important

- Anda hanya dapat melampirkan satu IAM role saja ke instans, tapi Anda dapat melampirkan peran yang sama ke banyak instans.
- Mengaitkan kebijakan IAM dengan hak istimewa paling sedikit yang membatasi akses ke panggilan API tertentu yang dibutuhkan aplikasi.

Untuk informasi selengkapnya tentang cara membuat dan menggunakan IAM role, lihat Peran dalam Panduan Pengguna IAM.

Melampirkan peran IAM yang ada selama peluncuran instans

Untuk melampirkan peran IAM yang ada ke instans saat peluncuran menggunakan konsol Amazon EC2, perluas Detail lanjutan. Untuk profil instans IAM, pilih peran IAM dari daftar dropdown.

Note

Jika Anda membuat peran IAM menggunakan konsol IAM, profil instance dibuat untuk Anda dan diberi nama yang sama dengan peran tersebut. Jika Anda membuat peran IAM menggunakan API AWS CLI, atau AWS SDK, Anda mungkin telah memberikan nama yang berbeda pada profil instans Anda dari peran tersebut.

Anda dapat melampirkan peran IAM ke instance yang sedang berjalan atau dihentikan. Jika instance sudah memiliki peran IAM yang terpasang, Anda harus menggantinya dengan peran IAM yang baru.

Console

Untuk melampirkan IAM role ke instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pilih Tindakan, Keamanan, Ubah peran IAM.
5. Untuk peran IAM, pilih profil instans IAM.
6. Pilih Perbarui peran IAM.

AWS CLI

Untuk melampirkan IAM role ke instans

Gunakan associate-iam-instance-profileperintah untuk melampirkan peran IAM ke instance. Saat menentukan profil instans, Anda dapat menggunakan Amazon Resource Name (ARN) dari profil instans, atau Anda dapat menggunakan namanya.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

PowerShell

Untuk melampirkan IAM role ke instans

Gunakan Register-EC2IamInstanceProfilecmdlet.

```
Register-EC2IamInstanceProfile `
    -InstanceId i-1234567890abcdef0 `
    -IamInstanceProfile_Name TestRole-1
```

Untuk mengganti peran IAM pada instance yang sudah memiliki peran IAM terlampir, instance harus berjalan. Anda dapat melakukan hal ini jika Anda ingin mengubah IAM role untuk instans tanpa melepaskan peran terlampir yang ada terlebih dahulu. Sebagai contoh, Anda dapat melakukan hal ini untuk memastikan bahwa tindakan-tindakan API yang dilakukan oleh aplikasi yang berjalan pada instans tidak terganggu.

Console

Untuk mengganti sebuah peran IAM ke sebuah instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pilih Tindakan, Keamanan, Ubah peran IAM.
5. Untuk peran IAM, pilih profil instans IAM.
6. Pilih Perbarui peran IAM.

AWS CLI

Untuk mengganti IAM role untuk instans

1. Jika diperlukan, gunakan perintah describe-iam-instance-profile-associations untuk mendapatkan ID asosiasi.

```
aws ec2 describe-iam-instance-profile-associations \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --query IamInstanceProfileAssociations.AssociationId
```

2. Gunakan perintah replace-iam-instance-profile-association. Tentukan ID asosiasi untuk profil instance yang ada dan ARN atau nama profil instance baru.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

PowerShell

Untuk mengganti IAM role untuk instans

1. Jika diperlukan, gunakan Get-EC2IamInstanceProfileAssociationcmdlet untuk mendapatkan ID asosiasi.

```
(Get-EC2IamInstanceProfileAssociation -Filter @{Name="instance-id";
 Values="i-0636508011d8e966a"}).AssociationId
```

2. Gunakan Set-EC2IamInstanceProfileAssociationcmdlet. Tentukan ID asosiasi untuk profil instance yang ada dan ARN atau nama profil instance baru.

```
Set-EC2IamInstanceProfileAssociation `
    -AssociationId iip-assoc-0044d817db6c0a4ba `
    -IamInstanceProfile_Name TestRole-2
```

Anda dapat melepaskan peran IAM dari instance yang sedang berjalan atau dihentikan.

Console

Untuk melepaskan IAM role terlampir dari instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pilih Tindakan, Keamanan, Ubah peran IAM.
5. Untuk IAM role, pilih No IAM Role (Tanpa IAM Role).
6. Pilih Perbarui peran IAM.
7. Saat dipromosikan untuk konfirmasi, masukkan Lepaskan, lalu pilih Lepaskan.

AWS CLI

Untuk melepaskan IAM role terlampir dari instans

1. Jika diperlukan, gunakan describe-iam-instance-profile-associations untuk mendapatkan ID asosiasi untuk profil instans IAM untuk dilepaskan.

```
aws ec2 describe-iam-instance-profile-associations \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --query IamInstanceProfileAssociations.AssociationId
```

2. Gunakan perintah disassociate-iam-instance-profile.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

PowerShell

Untuk melepaskan IAM role terlampir dari instans

1. Jika diperlukan, gunakan Get-EC2IamInstanceProfileAssociationuntuk mendapatkan ID asosiasi untuk profil instans IAM untuk dilepaskan.

```
(Get-EC2IamInstanceProfileAssociation -Filter @{Name="instance-id";
 Values="i-0636508011d8e966a"}).AssociationId
```

2. Gunakan Unregister-EC2IamInstanceProfilecmdlet.

```
Unregister-EC2IamInstanceProfile -AssociationId iip-assoc-0044d817db6c0a4ba
```

Peran identitas instans untuk instans Amazon EC2

Setiap instans Amazon EC2 yang Anda luncurkan memiliki peran identitas instans yang mewakili identitasnya. Peran identitas instance adalah jenis peran IAM. AWS layanan dan fitur yang terintegrasi untuk menggunakan peran identitas instance dapat menggunakannya untuk mengidentifikasi instance ke layanan.

Kredensional peran identitas instans dapat diakses dari Layanan Metadata Instans (IMDS) di `/identity-credentials/ec2/security-credentials/ec2-instance`. Kredensialnya terdiri dari AWS temporary access key pair dan session token. Mereka digunakan untuk menandatangani permintaan AWS Sigv4 ke AWS layanan yang menggunakan peran identitas instance. Kredensial hadir dalam metadata instans terlepas dari apakah layanan atau fitur yang menggunakan peran identitas instans diaktifkan pada instans.

Peran identitas instans dibuat secara otomatis saat instance diluncurkan, tidak memiliki dokumen kebijakan role-trust, dan tidak tunduk pada identitas atau kebijakan sumber daya apa pun.

Layanan yang didukung

AWS Layanan berikut menggunakan peran identitas instance:

- Amazon EC2 — EC2 Instance Connect menggunakan peran identitas instans untuk memperbarui kunci host untuk instance Linux.
- Amazon GuardDuty — GuardDuty Runtime Monitoring menggunakan peran identitas instans untuk memungkinkan agen runtime mengirim telemetri keamanan ke titik akhir VPC. GuardDuty
- AWS Lambda— Instans Terkelola Lambda menggunakan peran identitas instans untuk kait siklus hidup, telemetri, dan distribusi artefak.
- AWS Security Token Service (AWS STS) - Kredensial peran identitas instance dapat digunakan dengan tindakan. AWS STS `GetCallerIdentity`
- AWS Systems Manager— Saat menggunakan Konfigurasi Manajemen Host Default, AWS Systems Manager gunakan identitas yang disediakan oleh peran identitas instans untuk mendaftarkan instans EC2. Setelah mengidentifikasi instans Anda, Systems Manager dapat

meneruskan peran IAM `AWSSystemsManagerDefaultEC2InstanceManagementRole` ke instans Anda.

Peran identitas instans tidak dapat digunakan dengan AWS layanan atau fitur lain karena tidak memiliki integrasi dengan peran identitas instance.

ARN peran identitas instans

ARN peran identitas instans ARN mengambil format berikut:

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Contoh:

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-1234567890abcdef0
```

Untuk informasi selengkapnya ARNs, lihat Amazon Resource Names (ARNs) di Panduan Pengguna IAM.

Manajemen pembaruan untuk instans Amazon EC2

Kami merekomendasikan agar Anda melakukan patch, memperbarui, dan mengamankan sistem operasi dan aplikasi pada instans EC2 Anda secara berkala. Anda dapat menggunakan AWS Systems Manager Patch Manager untuk mengotomatisasi proses penginstalan pembaruan terkait keamanan untuk sistem operasi maupun aplikasi.

Untuk instans EC2 dalam grup Auto Scaling, Anda dapat menggunakan runbook AWS-PatchAsgInstance untuk membantu menghindari penggantian instans yang sedang di-patch. Atau, Anda dapat menggunakan layanan pembaruan otomatis atau proses yang direkomendasikan untuk menginstal pembaruan yang disediakan oleh vendor aplikasi.

Sumber daya

- AL2023— Memperbarui AL2023 di Panduan Pengguna Amazon Linux 2023
- AL2— Kelola perangkat lunak pada instans Amazon Linux 2 Anda di Panduan Pengguna Amazon Linux 2
- Contoh Windows — the section called “Manajemen pembaruan”

Praktik terbaik keamanan untuk instans Windows

Kami menyarankan Anda mengikuti praktik terbaik keamanan ini untuk instans Windows Anda.

Daftar Isi

- Praktik terbaik keamanan tingkat tinggi
- Manajemen pembaruan
- Manajemen konfigurasi
- Manajemen perubahan
- Audit dan akuntabilitas untuk instans Windows Amazon EC2

Praktik terbaik keamanan tingkat tinggi

Anda harus mematuhi praktik terbaik keamanan tingkat tinggi berikut untuk instance Windows Anda:

- Akses paling sedikit — Berikan akses hanya ke sistem dan lokasi yang dipercaya dan diharapkan. Hal ini berlaku untuk semua produk Microsoft, seperti Active Directory, server produktivitas bisnis Microsoft, serta layanan infrastruktur, seperti Remote Desktop Services, server proksi terbalik, server web IIS, dan lainnya. Gunakan AWS kemampuan seperti grup keamanan instans Amazon EC2, daftar kontrol akses jaringan (ACLs), dan public/private subnet Amazon VPC untuk melapisi keamanan di beberapa lokasi dalam arsitektur. Dalam instance Windows, pelanggan dapat menggunakan Windows Firewall untuk lebih lanjut melapisi defense-in-depth strategi dalam penyebaran mereka. Cukup instal komponen dan aplikasi OS yang diperlukan agar sistem berfungsi sebagaimana peruntukannya. Konfigurasikan layanan infrastruktur, seperti IIS, untuk dijalankan di bawah akun layanan atau untuk menggunakan fitur, seperti identitas kolam aplikasi, agar dapat mengakses sumber daya secara lokal dan jarak jauh di seluruh infrastruktur Anda.
- Keistimewaan terkecil — Tentukan kumpulan hak istimewa minimum yang dibutuhkan instance dan akun untuk menjalankan fungsinya. Batasi server dan pengguna tersebut agar hanya memperbolehkan izin yang ditentukan ini. Gunakan teknik, seperti Kontrol Akses Berbasis Peran, untuk mengurangi luas permukaan akun administratif dan membuat peran paling terbatas untuk menyelesaikan tugas. Gunakan fitur OS, seperti Encrypting File System (EFS), di dalam NTFS untuk mengenkripsi data diam yang sensitif serta mengontrol akses aplikasi dan pengguna ke data diam tersebut.
- Manajemen konfigurasi — Buat konfigurasi server dasar yang menggabungkan patch up-to-date keamanan dan suite perlindungan berbasis host yang mencakup anti-virus, anti-malware, deteksi/

pencegahan intrusi, dan pemantauan integritas file. Nilai setiap server menurut data baseline yang tercatat saat ini untuk mengidentifikasi dan menandai setiap deviasi. Pastikan setiap server dikonfigurasi untuk menghasilkan serta menyimpan data log dan audit yang sesuai dengan aman.

- Manajemen perubahan — Buat proses untuk mengontrol perubahan pada garis dasar konfigurasi server dan bekerja menuju proses perubahan yang sepenuhnya otomatis. Manfaatkan juga Just Enough Administration (JEA) dengan Windows PowerShell DSC untun membatasi akses administratif ke fungsi minimum yang diperlukan.
- Manajemen Patch — Menerapkan proses yang secara teratur menambal, memperbarui, dan mengamankan sistem operasi dan aplikasi pada instans EC2 Anda.
- Log audit — Akses audit dan semua perubahan pada instans Amazon EC2 untuk memverifikasi integritas server dan memastikan hanya perubahan resmi yang dibuat. Manfaatkan fitur seperti Enhanced Logging for IIS untuk meningkatkan kemampuan logging default. AWS kemampuan seperti VPC Flow Logs dan juga AWS CloudTrail tersedia untuk mengaudit akses jaringan, termasuk allowed/denied permintaan dan panggilan API, masing-masing.

Manajemen pembaruan

Untuk memastikan hasil terbaik saat menjalankan Windows Server di Amazon EC2, sebaiknya Anda menerapkan praktik terbaik berikut:

- Configure Windows Update
- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Reboot instance Windows Anda setelah Anda menginstal pembaruan. Untuk informasi selengkapnya, lihat Nyalakan ulang EC2 instans Amazon Anda.

Untuk informasi selengkapnya, tentang cara meningkatkan atau migrasi instans Windows ke versi Windows Server yang lebih baru, lihat Tingkatkan instans EC2 Windows ke versi Windows Server yang lebih baru.

Konfigurasikan Pembaruan Windows

Secara default, instance yang diluncurkan dari AWS Windows Server AMIs tidak menerima pembaruan melalui Pembaruan Windows.

Perbarui driver Windows

Pertahankan driver terbaru di semua instans Windows EC2 untuk memastikan bahwa perbaikan masalah dan peningkatan performa terbaru telah diterapkan di seluruh armada Anda. Bergantung pada jenis instans Anda, Anda harus memperbarui AWS PV, Amazon ENA, dan AWS NVMe driver.

- Gunakan topik SNS untuk menerima pembaruan untuk rilis driver baru.
- Gunakan runbook AWS Systems Manager Otomasi AWSSupport-UpgradeWindowsAWSDriversuntuk menerapkan pembaruan dengan mudah di seluruh instans Anda.

Luncurkan instance menggunakan Windows terbaru AMIs

AWS merilis Windows baru AMIs setiap bulan, yang berisi patch OS terbaru, driver, dan agen peluncuran. Anda harus memanfaatkan AMI terkini saat meluncurkan instans baru atau saat membangun gambar kustom Anda sendiri.

- Untuk melihat pembaruan pada setiap rilis AWS Windows AMIs, lihat riwayat versi AWS Windows AMI.
- Untuk membangun dengan yang terbaru yang tersedia AMIs, lihat Kueri untuk AMI Windows Terbaru Menggunakan Parameter Store Systems Manager.
- Untuk informasi selengkapnya tentang Windows khusus AMIs yang dapat Anda gunakan untuk meluncurkan instans untuk database dan kasus penggunaan pengerasan kepatuhan, lihat Windows Khusus AMIs di Referensi AWS AMI Windows.

Uji system/application kinerja sebelum migrasi

Migrasi aplikasi perusahaan untuk AWS dapat melibatkan banyak variabel dan konfigurasi. Selalu uji performa solusi EC2 untuk memastikan bahwa:

- Tipe Instans dikonfigurasi dengan benar, termasuk ukuran instans, peningkatan jaringan, dan penghunian (bersama atau khusus).
- Topologi instans sesuai untuk beban kerja dan memanfaatkan fitur berperforma tinggi bila diperlukan, seperti penghunian khusus, grup penempatan, volume penyimpanan instans, dan bare metal.

Instal versi terbaru EC2 Launch v2

Instal agen EC2 Launch v2 terbaru untuk memastikan bahwa penyempurnaan terbaru diterapkan di seluruh armada Anda. Untuk informasi selengkapnya, lihat Instal EC2 Launch v2.

Jika Anda memiliki armada campuran, atau jika ingin terus menggunakan agen EC2Launch (Windows Server 2016 dan 2019) atau EC2 Config (khusus OS warisan), perbarui ke versi terbaru agen masing-masing.

Pembaruan otomatis didukung pada kombinasi versi Windows Server dan agen peluncuran berikut. Anda dapat memilih pembaruan otomatis di konsol Manajemen Host Pengaturan Cepat SSM di bawah Agen Peluncuran Amazon EC2.

Versi Windows	EC2Luncurkan v1	EC2Luncurkan v2
2016	✓	✓
2019	✓	✓
2022		✓

- Untuk informasi selengkapnya tentang memperbarui ke EC2 Launch v2, lihatthe section called “Instal EC2 Launch v2”.
- Untuk informasi tentang memperbarui EC2 Config secara manual, lihat. the section called “Instal EC2 Config”
- Untuk informasi tentang memperbarui EC2 Peluncuran secara manual, lihatthe section called “Instal EC2 Peluncuran”.

Manajemen konfigurasi

Amazon Machine Image (AMI) menyediakan konfigurasi awal untuk instans Amazon EC2 yang mencakup OS Windows dan kustomisasi spesifik pelanggan yang bersifat opsional, seperti kontrol aplikasi dan keamanan. Buat katalog AMI yang berisi garis dasar konfigurasi keamanan khusus untuk memastikan bahwa semua instance Windows diluncurkan dengan kontrol keamanan standar. Garis dasar keamanan dapat dimasukkan ke dalam AMI, di-bootstrap secara dinamis saat instans EC2 diluncurkan, atau dikemas sebagai produk untuk distribusi seragam melalui portofolio Service Catalog. AWS Untuk informasi selengkapnya tentang cara mengamankan AMI, lihat Praktik Terbaik untuk Membangun AMI.

Setiap instans Amazon EC2 harus mematuhi standar keamanan organisasi. Jangan menginstal peran dan fitur Windows apa pun yang tidak diperlukan, dan instal perangkat lunak sebagai perlindungan terhadap kode berbahaya (mitigasi antivirus, antimalware, eksploitasi), pantau integritas host, dan lakukan deteksi intrusi. Lakukan konfigurasi pada perangkat lunak keamanan untuk memantau dan mempertahankan pengaturan keamanan OS, melindungi integritas file OS penting, dan mewaspadai penyimpangan dari garis dasar keamanan. Pertimbangkan untuk melaksanakan rekomendasi tolok ukur konfigurasi keamanan yang diterbitkan oleh Microsoft, Center for Internet Security (CIS), atau National Institute of Standards and Technology (NIST). Pertimbangkan untuk menggunakan alat-alat Microsoft lainnya untuk server aplikasi tertentu, seperti Penganalisis Praktik Terbaik untuk SQL Server.

AWS pelanggan juga dapat menjalankan penilaian Amazon Inspector untuk meningkatkan keamanan dan kepatuhan aplikasi yang diterapkan pada instans Amazon EC2. Amazon Inspector secara otomatis menilai aplikasi dalam hal kelemahan atau penyimpangannya dari praktik terbaik dan menyertakan basis pengetahuan dari ratusan aturan yang dipetakan ke standar kepatuhan keamanan umum (misalnya PCI DSS) dan definisi kelemahan. Contoh-contoh aturan bawaan termasuk pemeriksaan apakah cara masuk dari root jarak jauh diaktifkan, atau apakah ada versi perangkat lunak yang lemah yang sudah diinstal. Aturan-aturan ini diperbarui secara berkala oleh peneliti AWS keamanan.

Saat mengamankan instans Windows, kami menyarankan Anda untuk menerapkan Layanan Domain Direktori Aktif agar dapat mengaktifkan infrastruktur yang dapat diskalakan, aman, dan dapat dikelola untuk lokasi yang didistribusikan. Selain itu, setelah meluncurkan instans dari konsol Amazon EC2 atau dengan menggunakan alat penyediaan Amazon EC2, AWS CloudFormation seperti, sebaiknya gunakan fitur OS asli, seperti Microsoft PowerShell Windows DSC untuk mempertahankan status konfigurasi jika terjadi penyimpangan konfigurasi.

Manajemen perubahan

Setelah garis dasar keamanan awal diterapkan ke instans Amazon EC2 pada saat peluncuran, kendalikan perubahan Amazon EC2 yang terjadi untuk mempertahankan keamanan mesin virtual Anda. Menetapkan proses manajemen perubahan untuk mengotorisasi dan menggabungkan perubahan pada AWS sumber daya (seperti grup keamanan, tabel rute, dan jaringan ACLs) serta konfigurasi OS dan aplikasi (seperti Windows atau patching aplikasi, upgrade perangkat lunak, atau pembaruan file konfigurasi).

AWS menyediakan beberapa alat untuk membantu mengelola perubahan pada AWS sumber daya, termasuk AWS CloudTrail,, AWS Config CloudFormation, dan AWS Elastic Beanstalk, dan

paket manajemen untuk Manajer Operasi Pusat Sistem dan Manajer Mesin Virtual Pusat Sistem. Perhatikan bahwa Microsoft merilis patch Windows pada hari Selasa kedua setiap bulan (atau sesuai kebutuhan) dan AWS memperbarui semua Windows yang AMIs dikelola oleh AWS dalam waktu lima hari setelah Microsoft merilis patch. Oleh karena itu, penting untuk terus menambal semua baseline AMIs, memperbarui CloudFormation template, dan konfigurasi grup Auto Scaling dengan IDs AMI terbaru, dan menerapkan alat untuk mengotomatiskan manajemen patch instance yang sedang berjalan.

Microsoft menyediakan beberapa opsi untuk mengelola perubahan OS Windows dan aplikasi. SCCM, contohnya, menyediakan cakupan siklus hidup penuh modifikasi lingkungan. Pilihlah alat-alat yang memenuhi persyaratan bisnis dan lakukan kontrol pada bagaimana perubahan akan memengaruhi prosedur SLA aplikasi, kapasitas, prosedur keamanan, dan pemulihan bencana. Hindari perubahan manual dan sebagai gantinya manfaatkan perangkat lunak manajemen konfigurasi otomatis atau alat baris perintah seperti EC2 Run Command atau Windows PowerShell untuk mengimplementasikan proses perubahan skrip dan berulang. Untuk membantu memenuhi persyaratan ini, gunakan host bastion dengan peningkatan pencatatan untuk semua interaksi dengan instans Windows Anda untuk memastikan bahwa semua peristiwa dan tugas direkam secara otomatis.

Audit dan akuntabilitas untuk instans Windows Amazon EC2

AWS CloudTrail, AWS Config, dan Aturan AWS Config menyediakan fitur audit dan pelacakan perubahan untuk mengaudit perubahan AWS sumber daya. Lakukan konfigurasi pada log peristiwa Windows untuk mengirimkan file log lokal ke sistem manajemen log terpusat untuk menyimpan data log untuk digunakan dalam analisis perilaku keamanan dan operasional. Microsoft System Center Operations Manager (SCOM) mengumpulkan informasi mengenai aplikasi Microsoft yang di-deploy ke instans Windows dan menerapkan serangkaian aturan yang telah dikonfigurasi sebelumnya dan serangkaian aturan kustom berdasarkan peran dan layanan aplikasi. System Center Management Packs yang dibangun di atas SCOM akan menyediakan pemantauan dan panduan konfigurasi spesifik aplikasi. Paket Manajemen ini mendukung Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014, dan banyak lagi server dan teknologi.

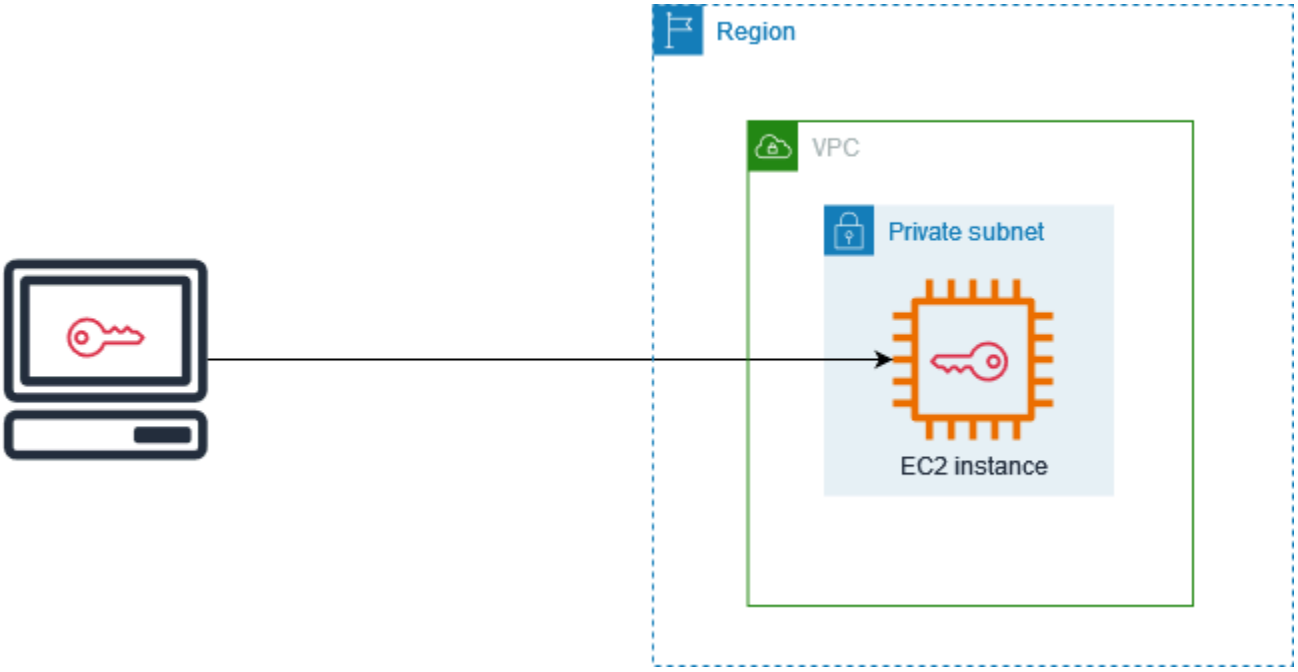
Selain alat manajemen sistem Microsoft, pelanggan dapat menggunakan Amazon CloudWatch untuk memantau pemanfaatan CPU instance, kinerja disk, I/O jaringan, dan melakukan pemeriksaan status host dan instance. Agen EC2 peluncuran EC2 Config, Launch, dan EC2 Launch v2 menyediakan akses ke fitur-fitur tambahan dan canggih untuk instance Windows. Misalnya, mereka dapat mengekspor log sistem Windows, keamanan, aplikasi, dan Layanan Informasi Internet (IIS) ke CloudWatch Log yang kemudian dapat diintegrasikan dengan CloudWatch metrik dan alarm Amazon.

Pelanggan juga dapat membuat skrip yang mengekspor penghitung kinerja Windows ke metrik CloudWatch khusus Amazon.

Pasangan kunci Amazon EC2 dan instans Amazon EC2

pasangan kunci, yang terdiri dari kunci publik dan kunci privat, adalah satu set kredensial keamanan yang Anda gunakan untuk membuktikan identitas Anda ketika terhubung ke instans Amazon EC2. Untuk instance Linux, kunci pribadi memungkinkan Anda untuk SSH dengan aman ke instans Anda. Untuk instance Windows, kunci pribadi diperlukan untuk mendekripsi kata sandi administrator, yang kemudian Anda gunakan untuk terhubung ke instans Anda.

Amazon EC2 menyimpan kunci publik pada instans Anda, dan Anda menyimpan kunci pribadi, seperti yang ditunjukkan pada diagram berikut. Penting bagi Anda untuk menyimpan kunci pribadi Anda di tempat yang aman karena siapa pun yang memiliki kunci pribadi Anda dapat terhubung ke instance Anda yang menggunakan key pair.



Ketika Anda meluncurkan sebuah instance, Anda dapat menentukan key pair, sehingga Anda dapat terhubung ke instance Anda menggunakan metode yang memerlukan key pair. Bergantung pada cara Anda mengelola keamanan, Anda dapat menentukan pasangan kunci yang sama untuk semua instans atau Anda dapat menentukan pasangan kunci yang berbeda.

Untuk instance Linux, ketika instance Anda melakukan booting untuk pertama kalinya, kunci publik yang Anda tentukan saat peluncuran ditempatkan pada instance Linux Anda dalam entri di

dalamnya`~/.ssh/authorized_keys`. Ketika Anda terhubung ke instans Linux Anda menggunakan SSH, untuk log in Anda harus menentukan kunci privat yang sesuai dengan kunci publik.

Untuk informasi selengkapnya tentang menghubungkan ke instans EC2 Anda, lihatConnect ke instans EC2.

> **Important**
>
> Karena Amazon EC2 tidak menyimpan salinan kunci privat Anda, tidak ada cara yang bisa dilakukan untuk memulihkan kunci privat tersebut jika Anda menghilangkannya. Akan tetapi, masih ada cara untuk terhubung ke instans yang kunci privatnya hilang. Untuk informasi selengkapnya, lihat Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance saya?

Sebagai alternatif dari pasangan kunci, Anda dapat menggunakan AWS Systems Manager Session Manageruntuk terhubung ke instance Anda dengan shell berbasis browser satu-klik interaktif atau (). AWS Command Line Interface AWS CLI

Daftar Isi

- Membuat pasangan kunci untuk instans Amazon EC2
- Jelaskan pasangan kunci Anda
- Menghapus pasangan kunci Anda
- Menambahkan atau mengganti kunci publik pada instance Linux Anda
- Lakukan verifikasi terhadap sidik jari pasangan kunci Anda

Membuat pasangan kunci untuk instans Amazon EC2

Anda dapat menggunakan Amazon EC2 untuk membuat pasangan kunci, atau Anda dapat menggunakan alat pihak ketiga untuk membuat pasangan kunci, lalu mengimpornya ke Amazon EC2.

Amazon EC2 mendukung kunci RSA SSH-2 2048-bit untuk instance Linux dan Windows. Amazon EC2 juga mendukung ED25519 kunci untuk instans Linux.

Untuk petunjuk tentang cara menyambung ke instans Anda setelah Anda membuat key pair, lihat the section called “Hubungkan ke instans Linux Anda, menggunakan SSH.” danthe section called “Hubungkan ke instans Windows Anda menggunakan RDP”.

Daftar Isi

- Membuat pasangan kunci menggunakan Amazon EC2
- Buat key pair menggunakan AWS CloudFormation
- Membuat pasangan kunci menggunakan alat pihak ketiga dan mengimpor kunci publik ke Amazon EC2

Membuat pasangan kunci menggunakan Amazon EC2

Saat Anda membuat pasangan kunci menggunakan Amazon EC2, kunci publik akan disimpan di Amazon EC2, dan Anda akan menyimpan kunci privat.

Anda dapat membuat hingga 5.000 pasangan kunci per Wilayah. Untuk meminta peningkatan, buat kasus dukungan. Untuk informasi selengkapnya, lihat Membuat kasus dukungan di Panduan Dukungan Pengguna.

Console

Untuk membuat pasangan kunci menggunakan Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, di Jaringan & Keamanan, pilih Pasangan Kunci.
3. Pilih Buat pasangan kunci.
4. Untuk Nama, masukkan nama deskriptif untuk pasangan kunci tersebut. Amazon EC2 akan mengaitkan kunci publik dengan nama yang Anda cantumkan sebagai nama kunci. Nama kunci dapat terdiri dari hingga 255 karakter ASCII. Tidak boleh mengandung spasi di depan maupun belakang.
5. Pilih jenis key pair yang sesuai untuk sistem operasi Anda:

   (Instance Linux) Untuk jenis pasangan Kunci, pilih RSA atau. ED25519

   (Instans Windows) Untuk jenis pasangan kunci, pilih RSA. ED25519kunci tidak didukung untuk instance Windows.
6. Untuk Format file kunci privat, pilih format untuk menyimpan kunci privat tersebut. Untuk menyimpan kunci privat dalam format yang dapat digunakan dengan OpenSSH, pilih pem. Untuk menyimpan kunci privat dalam format yang dapat digunakan dengan PuTTY, pilih ppk.
7. Untuk menambahkan tanda ke kunci publik, pilih Tambah tanda (Tambahkan tanda), lalu masukkan kunci dan nilai untuk tanda tersebut. Ulangi hal itu untuk setiap tanda.

8. Pilih Buat pasangan kunci.
9. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Nama file dasar adalah nama yang Anda tentukan sebagai nama pasangan kunci Anda, dan ekstensi dari nama file tersebut ditentukan oleh format file yang Anda pilih. Simpan file kunci privat di suatu tempat yang aman.

   > **Important**
   >
   > Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

10. Jika Anda berencana menggunakan klien SSH pada komputer macOS atau Linux untuk terhubung ke instans Linux, gunakan perintah berikut untuk mengatur izin file kunci privat Anda sehingga hanya Anda yang dapat membacanya.

    ```
    chmod 400 key-pair-name.pem
    ```

    Jika Anda tidak mengatur izin tersebut, Anda tidak akan dapat terhubung ke instans Anda menggunakan pasangan kunci ini. Untuk informasi selengkapnya, lihat Kesalahan: File kunci privat yang tidak dilindungi.

AWS CLI

Untuk membuat pasangan kunci menggunakan Amazon EC2

1. Gunakan perintah create-key-pair seperti berikut untuk membuat pasangan kunci dan untuk menyimpan kunci privat dalam file `.pem`. `--query`Opsi mencetak materi kunci pribadi ke output. `--output`Opsi ini menyimpan materi kunci pribadi dalam file yang ditentukan. Ekstensi harus salah satu `.pem` atau `.ppk`, tergantung pada format kunci. Nama kunci pribadi dapat berbeda dari nama kunci publik, tetapi untuk kemudahan penggunaan, gunakan nama yang sama.

   ```
   aws ec2 create-key-pair \
       --key-name my-key-pair \
       --key-type rsa \
       --key-format pem \
       --query "KeyMaterial" \
       --output text > my-key-pair.pem
   ```

2. Jika Anda berencana menggunakan klien SSH pada komputer macOS atau Linux untuk terhubung ke instans Linux, gunakan perintah berikut untuk mengatur izin file kunci privat Anda sehingga hanya Anda yang dapat membacanya.

   ```
   chmod 400 key-pair-name.pem
   ```

   Jika Anda tidak mengatur izin tersebut, Anda tidak akan dapat terhubung ke instans Anda menggunakan pasangan kunci ini. Untuk informasi selengkapnya, lihat Kesalahan: File kunci privat yang tidak dilindungi.

PowerShell

Untuk membuat pasangan kunci menggunakan Amazon EC2

Gunakan New-EC2KeyPaircmdlet sebagai berikut untuk menghasilkan kunci dan menyimpannya ke file `.pem` atau `.ppk`. Out-FileCmdlet menyimpan materi kunci pribadi dalam file dengan ekstensi yang ditentukan. Ekstensi harus salah satu `.pem` atau `.ppk`, tergantung pada format kunci. Nama kunci pribadi dapat berbeda dari nama kunci publik, tetapi untuk kemudahan penggunaan, gunakan nama yang sama.

```
(New-EC2KeyPair `
    -KeyName "my-key-pair" `
    -KeyType "rsa" `
    -KeyFormat "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Buat key pair menggunakan AWS CloudFormation

Saat Anda membuat key pair baru menggunakan CloudFormation, kunci pribadi disimpan ke AWS Systems Manager Parameter Store. Nama parameter memiliki format berikut:

```
/ec2/keypair/key_pair_id
```

Untuk informasi selengkapnya, lihat Penyimpanan Parameter AWS Systems Manager dalam Panduan Pengguna AWS Systems Manager .

Untuk membuat key pair menggunakan CloudFormation

1. Tentukan AWS::EC2::KeyPairsumber daya di template Anda.

```
Resources:
  NewKeyPair:
    Type: 'AWS::EC2::KeyPair'
    Properties:
      KeyName: new-key-pair
```

2. Gunakan perintah describe-key-pairs sebagai berikut untuk mendapatkan ID dari pasangan kunci.

```
aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
 KeyPairs[*].KeyPairId --output text
```

Berikut ini adalah output contoh.

```
key-05abb699beEXAMPLE
```

3. Gunakan perintah get-parameter sebagai berikut untuk mendapatkan parameter kunci Anda dan menyimpan materi kunci dalam file `.pem`.

```
aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
 --query Parameter.Value --output text > new-key-pair.pem
```

Izin IAM yang diperlukan

CloudFormation Untuk mengaktifkan mengelola parameter Parameter Store atas nama Anda, peran IAM yang diambil oleh CloudFormation atau pengguna Anda harus memiliki izin berikut:

- `ssm:PutParameter` – Memberikan izin guna membuat parameter untuk materi kunci privat.
- `ssm:DeleteParameter` – Memberikan izin guna menghapus parameter yang menyimpan materi kunci privat. Izin ini diperlukan apakah pasangan kunci diimpor atau dibuat oleh CloudFormation.

Ketika CloudFormation menghapus key pair yang dibuat atau diimpor oleh stack, ia melakukan pemeriksaan izin untuk menentukan apakah Anda memiliki izin untuk menghapus parameter, meskipun CloudFormation membuat parameter hanya ketika membuat key pair, bukan ketika

mengimpor key pair. CloudFormation tes untuk izin yang diperlukan menggunakan nama parameter fabrikasi yang tidak cocok dengan parameter apa pun di akun Anda. Oleh karena itu, Anda mungkin melihat nama parameter fabrikasi dalam pesan kesalahan `AccessDeniedException`.

Membuat pasangan kunci menggunakan alat pihak ketiga dan mengimpor kunci publik ke Amazon EC2

Alih-alih menggunakan Amazon EC2 untuk membuat key pair, Anda dapat membuat key pair RSA atau ED25519 dengan menggunakan alat pihak ketiga dan kemudian mengimpor kunci publik ke Amazon EC2.

Ketentuan untuk pasangan kunci

- Jenis yang didukung:
  - (Linux dan Windows) RSA
  - (Hanya Linux) ED25519

    > **Note**
    >
    > ED25519 kunci tidak didukung untuk instance Windows.

  - Amazon EC2 tidak menerima kunci DSA.
- Format yang didukung:
  - Format kunci publik OpenSSH (untuk Linux, format dalam) `~/.ssh/authorized_keys`
  - (Hanya Linux) Jika Anda terhubung menggunakan SSH saat menggunakan EC2 Instance Connect API, SSH2 formatnya juga didukung.
  - Format file kunci privat SSH harus dalam format PEM atau PPK
  - (Khusus RSA) Format DER dengan enkode Base64
  - (Khusus RSA) Format file kunci publik SSH sebagaimana yang ditentukan dalam RFC 4716
- Panjang yang didukung:
  - 1024, 2048, dan 4096.
  - (Hanya Linux) Jika Anda terhubung menggunakan SSH saat menggunakan EC2 Instance Connect API, panjang yang didukung adalah 2048 dan 4096.

Cara membuat pasangan kunci menggunakan alat pihak ketiga

1. Buat pasangan kunci dengan alat pihak ketiga yang Anda kehendaki. Sebagai contoh, Anda dapat menggunakan ssh-keygen (alat yang disediakan bersamaan dengan instalasi OpenSSH standar). Atau, Java, Ruby, Python, dan banyak bahasa pemrograman lainnya menyediakan pustaka standar yang dapat Anda gunakan untuk membuat key pair.

   > **Important**
   >
   > Kunci privat harus berupa format PEM atau PPK. Sebagai contoh, gunakan `ssh-keygen -m PEM` untuk membuat kunci OpenSSH dalam format PEM.

2. Simpan kunci publik ke file lokal. Misalnya, `~/.ssh/my-key-pair.pub` (Linux, macOS) atau `C:\keys\my-key-pair.pub` (Windows). Ekstensi nama file untuk file ini bukan hal penting.
3. Simpan kunci privat ke file lokal yang memiliki ekstensi `.pem` atau `.ppk`. Misalnya, `~/.ssh/my-key-pair.pem` atau `~/.ssh/my-key-pair.ppk` (Linux, macOS) atau `C:\keys\my-key-pair.pem` atau `C:\keys\my-key-pair.ppk` (Windows). Ekstensi file penting karena, tergantung pada alat yang Anda gunakan untuk terhubung ke instance Anda, Anda memerlukan format file tertentu. OpenSSH membutuhkan `.pem` file, sedangkan Putty membutuhkan file. `.ppk`

   > **Important**
   >
   > Simpan file kunci privat di suatu tempat yang aman. Anda harus memberikan nama kunci publik Anda saat meluncurkan instans, dan nama kunci privat yang terkait setiap kali Anda terhubung dengan instans tersebut.

Setelah Anda membuat pasangan kunci, gunakan salah satu metode berikut ini untuk mengimpor kunci publik Anda ke Amazon EC2.

Console

Cara mengimpor kunci publik ke Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Pasangan Kunci.
3. Pilih Impor pasangan kunci.

4. Untuk Nama, masukkan nama deskriptif untuk kunci publik. Nama dapat terdiri dari hingga 255 karakter ASCII. Tidak termasuk spasi di bagian paling depan dan paling belakang.

   > **Note**
   >
   > Ketika Anda terhubung ke instans Anda dari konsol EC2, konsol akan menyarankan nama ini untuk nama file kunci privat Anda.

5. Pilih Browse (Jelajah) untuk melakukan navigasi ke dan memilih kunci publik Anda, atau tempelkan konten kunci publik Anda ke bidang Konten kunci publik.
6. Pilih Impor pasangan kunci.
7. Pastikan kunci publik yang Anda impor muncul dalam daftar pasangan kunci.

AWS CLI

Cara mengimpor kunci publik ke Amazon EC2

Gunakan perintah import-key-pair.

```
aws ec2 import-key-pair \
    --key-name my-key-pair \
    --public-key-material fileb://path/my-key-pair.pub
```

Cara melakukan verifikasi terhadap pasangan kunci yang berhasil diimpor

Gunakan perintah describe-key-pairs.

```
aws ec2 describe-key-pairs --key-names my-key-pair
```

PowerShell

Cara mengimpor kunci publik ke Amazon EC2

Gunakan Import-EC2KeyPaircmdlet.

```
$publickey=[Io.File]::ReadAllText("C:\Users\TestUser\.ssh\id_rsa.pub")
Import-EC2KeyPair `
    -KeyName my-key-pair `
    -PublicKey $publickey
```

Cara melakukan verifikasi terhadap pasangan kunci yang berhasil diimpor

Gunakan Get-EC2KeyPaircmdlet.

```
Get-EC2KeyPair -KeyName my-key-pair
```

Jelaskan pasangan kunci Anda

Anda dapat menjelaskan pasangan kunci yang Anda simpan di Amazon EC2. Anda juga dapat mengambil materi kunci publik dan melakukan identifikasi terhadap kunci publik yang ditentukan saat peluncuran.

Tugas

- Jelaskan pasangan kunci Anda
- Mengambil materi kunci publik
- Mengidentifikasi kunci publik yang ditentukan saat peluncuran

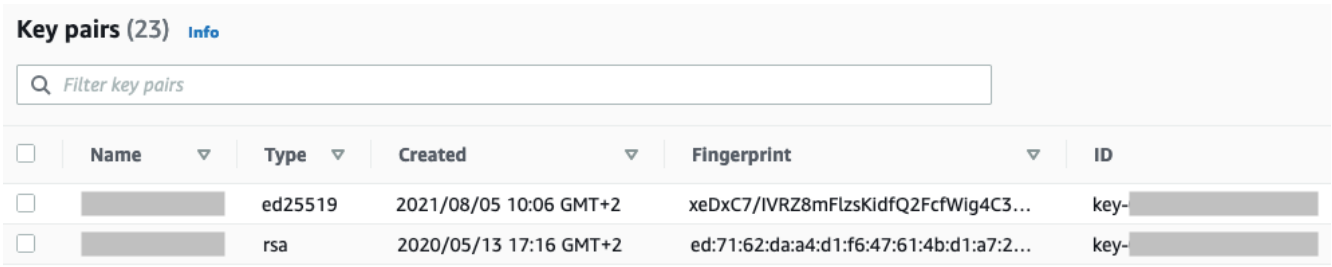
Jelaskan pasangan kunci Anda

Anda dapat melihat informasi berikut ini tentang kunci publik Anda yang disimpan di Amazon EC2: nama kunci publik, ID, jenis kunci, sidik jari, materi kunci publik, tanggal dan waktu (di zona waktu UTC) tempat kunci dibuat oleh Amazon EC2 (jika kunci dibuat oleh alat pihak ketiga, maka tanggal dan waktu tersebut adalah tanggal dan waktu dari kunci yang diimpor ke Amazon EC2), dan setiap tanda yang dikaitkan dengan kunci publik tersebut.

Console

Untuk melihat informasi tentang pasangan kunci Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi yang ada di sebelah kiri, pilih Pasangan Kunci.
3. Anda dapat melihat informasi tentang setiap kunci publik dalam tabel Key Pairs (Pasangan kunci).



4. Untuk melihat tag kunci publik, pilih kotak centang di sebelah kunci, lalu pilih Tindakan, Kelola tag.

AWS CLI

Untuk melihat informasi tentang key pair

Gunakan perintah describe-key-pairs.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

PowerShell

Untuk melihat informasi tentang key pair

Gunakan Get-EC2KeyPaircmdlet.

```
Get-EC2KeyPair -KeyName key-pair-name
```

Mengambil materi kunci publik

Anda bisa mendapatkan materi kunci publik untuk pasangan kunci Anda. Berikut ini adalah contoh kunci publik. Perhatikan bahwa ada jeda baris yang ditambahkan untuk keterbacaan.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Private key

Untuk mengambil materi kunci publik menggunakan ssh-keygen (Linux)

Di komputer Linux atau macOS lokal Anda, gunakan perintah. ssh-keygen Tentukan jalur tempat Anda mengunduh kunci privat Anda (file `.pem`).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

Jika ssh-keygen perintah ini gagal, jalankan chmod perintah berikut untuk memastikan bahwa file kunci pribadi memiliki izin yang diperlukan.

```
chmod 400 key-pair-name.pem
```

Untuk mengambil materi kunci publik menggunakan Pu TTYgen (Windows)

Di komputer Windows lokal Anda, mulai PuTTYgen. Pilih Muat. Pilih file kunci privat `.ppk` atau `.pem`. Pu TTYgen menampilkan kunci publik di bawah kunci Publik untuk menempel ke file authorized_keys OpenSSH. Anda juga dapat melihat kunci publik dengan memilih Simpan kunci publik, dengan menentukan nama untuk file, menyimpan file, lalu membuka file tersebut.

AWS CLI

Untuk mengambil materi kunci publik

Gunakan describe-key-pairsperintah berikut dan tentukan `--include-public-key` opsi.

```
aws ec2 describe-key-pairs \
    --key-names key-pair-name \
    --include-public-key \
    --query "KeyPairs[].PublicKey"
```

PowerShell

Untuk mengambil materi kunci publik

Gunakan Get-EC2KeyPaircmdlet.

```
(Get-EC2KeyPair -KeyName key-pair-name -IncludePublicKey $true).PublicKey
```

IMDSv2

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

Linux

Jalankan perintah berikut dari instance Linux Anda.

```
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda.

```
Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

Mengidentifikasi kunci publik yang ditentukan saat peluncuran

Jika Anda menentukan kunci publik saat meluncurkan instans, maka nama kunci publik tersebut akan direkam oleh instans. Nama kunci publik yang dilaporkan untuk sebuah instans tidak berubah, bahkan jika Anda mengubah kunci publik pada instance atau menambahkan kunci publik.

Console

Untuk mengidentifikasi kunci publik yang ditentukan pada peluncuran instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pada tab Detail, di bawah Detail instans, temukan Pasangan kunci yang ditetapkan saat peluncuran.

AWS CLI

Untuk mengidentifikasi kunci publik yang ditentukan pada peluncuran instance

Gunakan perintah describe-instance berikut.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query "Reservations[].Instances[].KeyName" \
    --output text
```

Berikut ini adalah output contoh.

```
key-pair-name
```

PowerShell

Untuk mengidentifikasi kunci publik yang ditentukan pada peluncuran instance

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Select KeyName
```

Berikut ini adalah output contoh.

```
KeyName
-------
key-pair-name
```

Menghapus pasangan kunci Anda

Anda dapat menghapus key pair, yang menghapus kunci publik yang disimpan di Amazon EC2. Menghapus key pair tidak menghapus kunci pribadi yang cocok.

Saat Anda menghapus kunci publik menggunakan metode berikut, Anda hanya akan menghapus kunci publik yang Anda simpan di Amazon EC2 saat Anda membuat atau mengimpor pasangan kunci. Menghapus kunci publik tidak akan menghapus kunci publik tersebut dari instans mana pun yang padanya kunci publik tersebut telah Anda tambahkan, baik ketika Anda meluncurkan instans atau setelahnya. Hal ini juga tidak akan menghapus kunci privat di komputer lokal Anda. Anda dapat terus terhubung ke instans yang Anda luncurkan menggunakan kunci publik yang Anda hapus dari Amazon EC2 selama Anda masih memiliki file kunci privat (`.pem`).

> **Important**
>
> Jika Anda menggunakan grup Auto Scaling (misalnya, dalam lingkungan Elastic Beanstalk), pastikan bahwa kunci publik yang Anda hapus tidak ditentukan dalam templat peluncuran atau konfigurasi peluncuran yang dikaitkan. Jika Amazon EC2 Auto Scaling mendeteksi instans yang tidak sehat, ia akan meluncurkan instans pengganti. Namun demikian, peluncuran instans tersebut akan gagal jika kunci publik tidak dapat ditemukan. Untuk informasi selengkapnya, lihat Templat peluncuran di Panduan Pengguna Amazon EC2 Auto Scaling.

Console

Cara menghapus kunci publik Anda di Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Pasangan Kunci.
3. Pilih pasangan kunci yang akan dihapus lalu pilih Tindakan, Hapus.
4. Dalam bidang konfirmasi, masukkan `Delete` lalu pilih Delete (Hapus).

AWS CLI

Cara menghapus kunci publik Anda di Amazon EC2

Gunakan perintah delete-key-pair.

```
aws ec2 delete-key-pair --key-name my-key-pair
```

PowerShell

Cara menghapus kunci publik Anda di Amazon EC2

Gunakan Remove-EC2KeyPaircmdlet.

```
Remove-EC2KeyPair -KeyName my-key-pair
```

Menambahkan atau mengganti kunci publik pada instance Linux Anda

Jika Anda kehilangan kunci pribadi, Anda kehilangan akses ke setiap instance yang menggunakan key pair. Untuk informasi lebih lanjut tentang menghubungkan ke instance menggunakan key pair yang berbeda dari yang Anda tentukan saat peluncuran, lihat Saya kehilangan kunci pribadi saya.

Saat meluncurkan instans, Anda dapat menentukan pasangan kunci. Jika Anda menentukan pasangan kunci, saat instans Anda melakukan booting untuk pertama kalinya, materi kunci publik akan ditempatkan pada instans Linux Anda di entri dalam `~/.ssh/authorized_keys`. Ketika Anda pertama kali terhubung ke instance Linux Anda menggunakan SSH, Anda menentukan pengguna default dan kunci pribadi yang sesuai dengan kunci publik yang disimpan pada instance Linux Anda.

Setelah terhubung ke instans, Anda dapat mengubah key pair yang digunakan untuk mengakses akun sistem default instance Anda dengan menambahkan kunci publik baru pada instance, atau dengan mengganti kunci publik (menghapus kunci publik yang ada dan menambahkan yang baru) pada instance. Anda juga dapat menghapus semua kunci publik dari instans.

Anda dapat menambahkan atau mengganti key pair karena alasan berikut:

- Jika seorang pengguna dalam organisasi Anda memerlukan akses ke akun pengguna sistem yang menggunakan pasangan kunci terpisah, maka Anda dapat menambahkan kunci publik tersebut ke instans Anda.
- Jika seseorang memiliki salinan kunci privat (file `.pem`) dan Anda ingin mencegahnya agar tidak terhubung ke instans Anda (misalnya, ketika orang tersebut sudah meninggalkan organisasi Anda), maka Anda dapat mengganti kunci publik dengan yang baru.

- Jika Anda membuat AMI Linux dari instans, materi kunci publik akan disalin dari instans ke AMI. Jika Anda meluncurkan instans dari AMI, maka instans baru tersebut akan menyertakan kunci publik dari instans asli. Untuk mencegah seseorang yang memiliki kunci privat terhubung ke instans yang baru, Anda dapat menghapus kunci publik dari instans asli sebelum membuat AMI.

Gunakan prosedur berikut untuk memodifikasi key pair untuk pengguna default, sepertiec2-user. Untuk informasi tentang menambahkan pengguna ke instans Anda, lihat dokumentasi untuk sistem operasi pada instans Anda.

Cara menambah atau mengganti pasangan kunci

1. Buatlah pasangan kunci baru menggunakan konsol Amazon EC2 atau alat pihak ketiga.
2. Ambil kunci publik dari pasangan kunci baru Anda. Untuk informasi selengkapnya, lihat Mengambil materi kunci publik.
3. Terhubung ke instans Anda.
4. Pada contoh, menggunakan editor teks pilihan Anda, buka `.ssh/authorized_keys` file. Tempelkan informasi kunci publik dari key pair baru Anda di bawah informasi kunci publik yang ada, lalu simpan file tersebut.
5. Putuskan sambungan dari instans Anda. Uji apakah Anda dapat terhubung ke instance Anda menggunakan file kunci pribadi dari key pair baru.
6. Jika Anda menggunakan Auto Scaling, armada EC2, atau template peluncuran untuk meluncurkan instans, periksa apakah key pair yang Anda ganti ditentukan dalam template peluncuran atau konfigurasi peluncuran. Jika tidak, peluncuran instance akan gagal.
7. (Opsional) Jika Anda mengganti pasangan kunci yang sudah ada, hubungkan ke instans Anda dan hapus informasi kunci publik untuk pasangan kunci asli dari file `.ssh/authorized_keys`.

Untuk menghapus kunci publik dari instans

1. Terhubung ke instans Anda.
2. Dengan menggunakan editor teks yang Anda kehendaki, buka file `.ssh/authorized_keys` pada instans. Hapus informasi kunci publik, dan kemudian simpan file.

> **Warning**
>
> Jika Anda menghapus semua kunci publik dari sebuah instance dan memutuskan sambungan dari instance, Anda tidak dapat menyambung ke instance lagi kecuali Anda telah mengonfigurasi cara alternatif untuk masuk.

Lakukan verifikasi terhadap sidik jari pasangan kunci Anda

Untuk memverifikasi sidik jari key pair Anda, bandingkan sidik jari yang ditampilkan pada halaman Pasangan kunci di konsol Amazon EC2, atau dikembalikan oleh describe-key-pairsperintah, dengan sidik jari yang Anda hasilkan menggunakan kunci pribadi di komputer lokal Anda. Sidik jari ini harus cocok.

Saat Amazon EC2 menghitung sidik jari, Amazon EC2 mungkin menambahkan padding ke sidik jari dengan karakter =. Alat lain, seperti ssh-keygen, mungkin menghilangkan padding ini.

Jika Anda mencoba memverifikasi sidik jari instans EC2 Linux Anda, bukan sidik jari key pair Anda, lihat Dapatkan sidik jari instance.

Cara sidik jari dikalkulasi

Amazon EC2 menggunakan berbagai fungsi hash untuk menghitung sidik jari untuk pasangan kunci RSA dan ED25519. Selain itu, untuk pasangan kunci RSA, Amazon EC2 menghitung sidik jari secara berbeda menggunakan fungsi hash yang berbeda tergantung pada apakah pasangan kunci tersebut dibuat oleh Amazon EC2 atau diimpor ke Amazon EC2.

Tabel berikut ini mencantumkan fungsi hash yang digunakan untuk menghitung sidik jari untuk pasangan kunci RSA dan ED25519 yang dibuat oleh Amazon EC2 dan diimpor ke Amazon EC2.

(Instance Linux) Fungsi hash yang digunakan untuk menghitung sidik jari

Sumber pasangan kunci	Pasangan kunci RSA (Windows dan Linux)	ED25519 pasangan kunci (Linux)
Dibuat oleh Amazon EC2	SHA-1	SHA-256
Diimpor ke Amazon EC2	MD5[1]	SHA-256

[1] Jika Anda mengimpor kunci RSA publik ke Amazon EC2, sidik jari akan dihitung menggunakan fungsi hash MD5. Hal ini berlaku terlepas dari cara yang Anda gunakan untuk membuat pasangan kunci, misalnya, menggunakan alat pihak ketiga atau dengan membuat kunci publik baru dari kunci privat yang sudah ada yang dibuat menggunakan Amazon EC2.

Saat menggunakan pasangan kunci yang sama di Wilayah yang berbeda

Jika Anda berencana untuk menggunakan key pair yang sama untuk terhubung ke instance yang berbeda Wilayah AWS, Anda harus mengimpor kunci publik ke semua Wilayah tempat Anda akan menggunakannya. Jika Anda menggunakan Amazon EC2 untuk membuat pasangan kunci, Anda dapat Mengambil materi kunci publik mengimpor kunci publik ke Wilayah lain.

> **Note**
>
> - Jika Anda membuat pasangan kunci RSA menggunakan Amazon EC2, dan kemudian Anda membuat kunci publik dari kunci privat Amazon EC2, kunci publik yang diimpor akan memiliki sidik jari yang berbeda dari kunci publik yang asli. Ini karena sidik jari kunci RSA asli yang dibuat menggunakan Amazon EC2 dihitung menggunakan fungsi hash SHA-1, sedangkan sidik jari kunci RSA yang diimpor dihitung menggunakan fungsi hash. MD5
> - Untuk pasangan kunci ED25519, sidik jari akan tetap sama terlepas dari apakah pasangan kunci tersebut dibuat oleh Amazon EC2 atau diimpor ke Amazon EC2, karena fungsi hash SHA-256 yang sama digunakan untuk melakukan kalkulasi terhadap sidik jari.

Membuat sidik jari dari kunci privat

Gunakan salah satu perintah berikut untuk membuat sidik jari dari kunci privat di mesin lokal Anda.

Jika Anda menggunakan mesin lokal Windows, maka Anda dapat menjalankan perintah berikut menggunakan Windows Subsystem for Linux (WSL). Instal WSL dan distribusi Linux menggunakan instruksi di Cara menginstal Linux di Windows dengan WSL. Contoh dalam instruksi tersebut menginstal distribusi Ubuntu Linux, tetapi Anda dapat menginstal distribusi apa pun. Anda akan diminta untuk memulai ulang komputer Anda agar perubahan dapat diterapkan.

- Jika Anda membuat pasangan kunci menggunakan Amazon EC2

  Gunakan alat OpenSSL untuk membuat sidik jari seperti yang ditunjukkan dalam contoh-contoh berikut.

Untuk pasangan kunci RSA:

```
openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
 openssl sha1 -c
```

(Instance Linux) Untuk pasangan ED25519 kunci:

```
ssh-keygen -l -f path_to_private_key
```

- (Hanya pasangan kunci RSA) Jika Anda mengimpor kunci publik ke Amazon EC2

  Anda dapat mengikuti prosedur ini terlepas dari cara Anda membuat pasangan kunci, misalnya menggunakan alat pihak ketiga atau dengan membuat kunci publik baru dari kunci privat yang sudah ada yang dibuat menggunakan Amazon EC2

  Gunakan alat OpenSSL untuk membuat sidik jari seperti yang ditunjukkan dalam contoh berikut.

  ```
  openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
  ```

- Jika Anda membuat pasangan kunci OpenSSH menggunakan OpenSSH 7.8 atau yang lebih baru dan mengimpor kunci publik ke Amazon EC2

  Gunakan ssh-keygen untuk membuat sidik jari seperti yang ditunjukkan dalam contoh-contoh berikut.

  Untuk pasangan kunci RSA:

  ```
  ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
   | openssl md5 -c
  ```

  (Instance Linux) Untuk pasangan ED25519 kunci:

  ```
  ssh-keygen -l -f path_to_private_key
  ```

Grup keamanan Amazon EC2 untuk instans EC2 Anda

grup keamanan bertindak sebagai firewall virtual untuk instans EC2 Anda untuk mengontrol lalu lintas masuk dan ke luar. Aturan-aturan ke dalam mengontrol lalu lintas yang masuk ke instans Anda, dan

aturan-aturan ke luar mengontrol lalu lintas yang ke luar dari instans Anda. Saat Anda meluncurkan instans, artinya Anda menentukan satu atau beberapa grup keamanan pada instans tersebut. Jika Anda tidak menentukan grup keamanan, maka Amazon EC2 akan menggunakan grup keamanan default untuk VPC. Setelah Anda meluncurkan instans, Anda dapat mengubah grup keamanannya.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Untuk informasi lebih lanjut, lihatKeamanan dalam Amazon EC2. AWS menyediakan grup keamanan sebagai salah satu alat untuk mengamankan instans Anda, dan Anda perlu mengonfigurasinya untuk memenuhi kebutuhan keamanan Anda. Jika Anda memiliki persyaratan yang tidak sepenuhnya dipenuhi oleh grup keamanan, maka Anda dapat mempertahankan firewall Anda sendiri pada instans Anda selain menggunakan grup keamanan.

Harga

Tidak ada biaya tambahan untuk menggunakan grup keamanan.

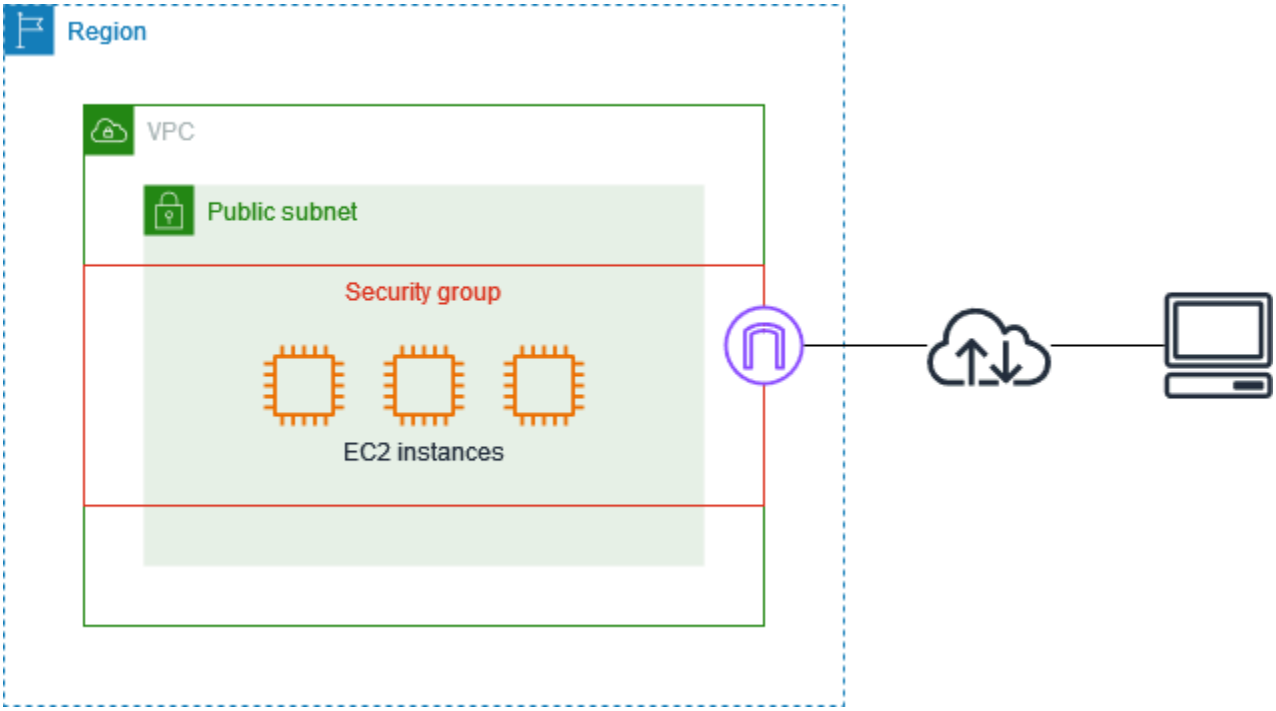
Daftar Isi

- Ikhtisar
- Membuat grup keamanan untuk instans Amazon EC2 Anda
- Mengubah grup keamanan untuk instans Amazon EC2 Anda
- Hapus grup keamanan Amazon EC2
- Pelacakan koneksi grup keamanan Amazon EC2
- Aturan-aturan grup keamanan untuk kasus penggunaan yang berbeda

Ikhtisar

Anda dapat mengaitkan setiap instance dengan beberapa grup keamanan, dan Anda dapat mengaitkan setiap grup keamanan dengan beberapa instance. Anda menambahkan aturan ke setiap grup keamanan yang mengizinkan lalu lintas ke atau dari instans terkait. Anda dapat melakukan modifikasi terhadap aturan-aturan untuk grup keamanan kapan saja. Aturan-aturan baru dan aturan-aturan yang dimodifikasi akan secara otomatis diterapkan ke semua instans yang dikaitkan dengan grup keamanan. Ketika Amazon EC2 memutuskan apakah akan mengizinkan lalu lintas untuk mencapai instans, Amazon EC2 mengevaluasi semua aturan dari semua grup keamanan yang terkait dengan instans. Untuk informasi selengkapnya, lihat Aturan grup keamanan di Panduan Pengguna Amazon VPC.

Diagram berikut menunjukkan VPC dengan subnet, gateway internet, dan grup keamanan. Subnet berisi instans EC2. Grup keamanan dikaitkan dengan instance. Satu-satunya lalu lintas yang mencapai instance adalah lalu lintas yang diizinkan oleh aturan grup keamanan. Misalnya, jika grup keamanan berisi aturan yang memungkinkan lalu lintas SSH dari jaringan Anda, maka Anda dapat terhubung ke instance Anda dari komputer menggunakan SSH. Jika grup keamanan berisi aturan yang memungkinkan semua lalu lintas dari sumber daya yang terkait dengannya, maka setiap instance dapat menerima lalu lintas apa pun yang dikirim dari instance lain.



Grup keamanan bersifat stateful—jika Anda mengirimkan permintaan dari instans Anda, maka lalu lintas tanggapan untuk permintaan tersebut diperbolehkan untuk mengalir tanpa memedulikan aturan-aturan ke dalam grup keamanan. Juga, tanggapan terhadap lalu lintas masuk yang diizinkan diizinkan mengalir keluar, terlepas dari aturan keluar. Untuk informasi selengkapnya, lihat Pelacakan koneksi.

Membuat grup keamanan untuk instans Amazon EC2 Anda

Grup keamanan bertindak sebagai firewall untuk instans-instans yang dikaitkan, mengontrol lalu lintas ke dalam dan ke luar pada tingkat instans. Anda dapat menambahkan aturan ke grup keamanan yang memungkinkan Anda terhubung ke instans menggunakan SSH (instance Linux) atau RDP (instance Windows). Anda juga dapat menambahkan aturan yang memungkinkan lalu lintas klien, misalnya, lalu lintas HTTP dan HTTPS yang ditujukan ke server web.

Anda dapat mengaitkan grup keamanan dengan instance saat meluncurkan instance. Saat Anda menambahkan atau menghapus aturan dari grup keamanan terkait, perubahan tersebut secara otomatis diterapkan ke semua instance yang Anda kaitkan dengan grup keamanan.

Setelah meluncurkan instance, Anda dapat mengaitkan grup keamanan tambahan. Untuk informasi selengkapnya, lihat Mengubah grup keamanan untuk instans Amazon EC2 Anda.

Anda dapat menambahkan aturan grup keamanan masuk dan keluar saat membuat grup keamanan atau menambahkannya nanti. Untuk informasi selengkapnya, lihat Mengonfigurasi aturan grup keamanan. Untuk contoh aturan yang dapat Anda tambahkan ke grup keamanan, lihatAturan-aturan grup keamanan untuk kasus penggunaan yang berbeda.

Pertimbangan-pertimbangan

- Grup keamanan baru dimulai dengan hanya aturan keluar yang memungkinkan semua lalu lintas meninggalkan sumber daya. Anda harus menambahkan aturan-aturan lain untuk mengizinkan lalu lintas ke dalam atau membatasi lalu lintas ke luar.
- Saat mengonfigurasi sumber untuk aturan yang memungkinkan akses SSH atau RDP ke instance Anda, jangan izinkan akses dari mana saja, karena itu akan memungkinkan akses ini ke instance Anda dari semua alamat IP di internet. Hal ini dapat diterima untuk waktu yang singkat di lingkungan pengujian, tetapi tidak aman untuk lingkungan produksi.
- Jika ada lebih dari satu aturan untuk port tertentu, maka Amazon EC2 akan menerapkan aturan yang paling permisif. Misalnya, jika Anda memiliki aturan yang memungkinkan akses ke port TCP 22 (SSH) dari alamat IP 203.0.113.1, dan aturan lain yang memungkinkan akses ke port TCP 22 dari mana saja, maka setiap orang memiliki akses ke port TCP 22.
- Anda dapat mengaitkan beberapa grup keamanan dengan sebuah instance. Oleh karena itu, instans dapat memiliki ratusan aturan yang berlaku. Hal ini dapat menyebabkan masalah saat Anda mengakses instans tersebut. Kami menyarankan agar Anda sedapat mungkin membuat aturan-aturan yang padat.
- Saat Anda menentukan grup keamanan sebagai sumber atau tujuan dari aturan, aturan tersebut akan memengaruhi semua instans yang dikaitkan dengan grup keamanan tersebut. Lalu lintas masuk diizinkan berdasarkan alamat IP privat dari instans yang dikaitkan dengan grup keamanan sumber (dan bukan alamat IP publik atau alamat IP Elastis). Untuk informasi selengkapnya tentang alamat IP, lihat Pengalamatan IP instans Amazon EC2.
- Amazon EC2 memblokir lalu lintas pada port 25 secara default. Untuk informasi selengkapnya, lihat Pembatasan pada email yang dikirim menggunakan port 25.

Console

Cara membuat grup keamanan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Security Groups (Grup Keamanan).
3. Pilih Buat grup keamanan.
4. Masukkan nama deskriptif dan deskripsi singkat untuk grup keamanan. Anda tidak dapat mengubah nama dan deskripsi grup keamanan setelah dibuat.
5. Untuk VPC, pilih VPC tempat Anda akan menjalankan instans Amazon EC2.
6. (Opsional) Untuk menambahkan aturan masuk, pilih Aturan masuk. Untuk setiap aturan, pilih Tambahkan aturan dan tentukan protokol, port, dan sumber. Misalnya, untuk mengizinkan lalu lintas SSH, pilih SSH untuk Jenis dan tentukan IPv4 alamat publik komputer atau jaringan Anda untuk Sumber.
7. (Opsional) Untuk menambahkan aturan keluar, pilih Aturan keluar. Untuk setiap aturan, pilih Tambahkan aturan dan tentukan protokol, port, dan tujuan. Jika tidak, Anda dapat mempertahankan aturan default, yang memungkinkan semua lalu lintas keluar.
8. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai.
9. Pilih Create security group (Buat grup keamanan).

AWS CLI

Cara membuat grup keamanan

Gunakan perintah berikut create-security-group.

```
aws ec2 create-security-group \
    --group-name my-security-group \
    --description "my security group" \
    --vpc-id vpc-1234567890abcdef0
```

Untuk contoh yang menambahkan aturan, lihatthe section called “Mengonfigurasi aturan grup keamanan”.

PowerShell

Cara membuat grup keamanan

Gunakan New-EC2SecurityGroupcmdlet.

```
New-EC2SecurityGroup `
    -GroupName my-security-group `
    -Description "my security group" `
    -VpcId vpc-1234567890abcdef0
```

Untuk contoh yang menambahkan aturan, lihatthe section called “Mengonfigurasi aturan grup keamanan”.

Mengubah grup keamanan untuk instans Amazon EC2 Anda

Anda dapat menentukan grup keamanan untuk instans Amazon EC2 saat meluncurkannya. Setelah meluncurkan instance, Anda dapat menambah atau menghapus grup keamanan. Anda juga dapat menambahkan, menghapus, atau mengedit aturan grup keamanan untuk grup keamanan terkait kapan saja.

Grup keamanan dikaitkan dengan antarmuka jaringan. Menambahkan atau menghapus grup keamanan mengubah grup keamanan yang terkait dengan antarmuka jaringan utama. Anda juga dapat mengubah grup keamanan yang terkait dengan antarmuka jaringan sekunder apa pun. Untuk informasi selengkapnya, lihat Memodifikasi atribut antarmuka jaringan.

Tugas

- Menambah atau menghapus grup keamanan
- Mengonfigurasi aturan grup keamanan

Menambah atau menghapus grup keamanan

Setelah meluncurkan instans, Anda dapat menambahkan atau menghapus grup keamanan dari daftar grup keamanan terkait. Saat Anda mengaitkan beberapa grup keamanan dengan instans, aturan-aturan dari masing-masing grup keamanan akan digabungkan secara efektif untuk membuat satu set aturan. Amazon EC2 menggunakan seperangkat aturan ini untuk menentukan apakah akan mengizinkan lalu lintas.

Persyaratan

- Instans harus berada dalam status `running` atau `stopped`.

Console

Untuk mengubah grup keamanan instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans Anda, dan kemudian pilih Actions (Tindakan), Security (Keamanan), Change security groups (Ubah grup keamanan).
4. Untuk Grup keamanan terkait, pilih grup keamanan dari daftar dan pilih Add security group (Tambahkan grup keamanan).

   Untuk menghapus grup keamanan yang sudah dikaitkan, pilih Remove (Hapus) untuk grup keamanan itu.
5. Pilih Save (Simpan).

AWS CLI

Untuk mengubah grup keamanan instans

Gunakan perintah berikut modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --groups sg-1234567890abcdef0
```

PowerShell

Untuk mengubah grup keamanan instans

Gunakan Edit-EC2InstanceAttributecmdlet.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -Group sg-1234567890abcdef0
```

Mengonfigurasi aturan grup keamanan

Setelah membuat grup keamanan, Anda dapat menambahkan, memperbarui, dan menghapus aturan grup keamanannya. Saat Anda menambahkan, memperbarui, atau menghapus aturan, perubahan secara otomatis diterapkan ke sumber daya yang terkait dengan grup keamanan.

Untuk contoh aturan yang dapat Anda tambahkan ke grup keamanan, lihatAturan-aturan grup keamanan untuk kasus penggunaan yang berbeda.

Izin yang diperlukan

Sebelum memulai, pastikan Anda memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat Contoh: Cara menggunakan grup keamanan.

Protokol dan port

- Dengan konsol, ketika Anda memilih jenis yang telah ditentukan, Protokol dan rentang Port ditentukan untuk Anda. Untuk memasukkan rentang port, Anda harus memilih salah satu dari jenis kustom berikut: TCP Kustom atau UDP Kustom.
- Dengan itu AWS CLI, Anda dapat menambahkan satu aturan dengan satu port menggunakan `--port` opsi `--protocol` dan. Untuk menambahkan beberapa aturan, atau aturan dengan rentang port, gunakan `--ip-permissions` opsi sebagai gantinya.

Sumber dan tujuan

- Dengan konsol, Anda dapat menentukan yang berikut ini sebagai sumber untuk aturan masuk atau tujuan untuk aturan keluar:
  - Kustom — Blok IPv4 CIDR, blok IPv6 CIDR, grup keamanan, atau daftar awalan.
  - Di mana saja- IPv4 - Blok CIDR 0.0.0.0/0 IPv4 .
  - Di mana saja- IPv6 - Blok IPv6 CIDR: :/0.
  - IP saya — IPv4 Alamat publik komputer lokal Anda.
- Dengan AWS CLI, Anda dapat menentukan blok IPv4 CIDR menggunakan `--cidr` opsi atau grup keamanan menggunakan `--source-group` opsi. Untuk menentukan daftar awalan atau blok IPv6 CIDR, gunakan opsi. `--ip-permissions`

> **Warning**
>
> Jika Anda menambahkan aturan masuk untuk port 22 (SSH) atau 3389 (RDP), kami sangat menyarankan agar Anda hanya mengotorisasi alamat IP tertentu atau rentang alamat yang memerlukan akses ke instans Anda. Jika Anda memilih Anywhere- IPv4, Anda mengizinkan lalu lintas dari semua IPv4 alamat untuk mengakses instans Anda menggunakan protokol yang ditentukan. Jika Anda memilih Anywhere- IPv6, Anda mengizinkan lalu lintas dari semua IPv6 alamat untuk mengakses instans Anda menggunakan protokol yang ditentukan.

Console

Mengonfigurasi aturan grup keamanan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Security Groups (Grup Keamanan).
3. Pilih grup keamanan.
4. Untuk mengedit aturan masuk, pilih Edit aturan masuk dari Tindakan atau tab Aturan masuk.
   a. Untuk menambahkan aturan, pilih Tambahkan aturan dan masukkan jenis, protokol, port, dan sumber untuk aturan tersebut.

      Jika jenisnya adalah TCP atau UDP, Anda harus memasukkan rentang port untuk mengizinkan. Untuk ICMP kustom, Anda harus memilih jenis ICMP dari Protokol, dan, jika memungkinkan, nama kode dari Rentang port. Untuk jenis lainnya, protokol dan rentang port akan dikonfigurasikan untuk Anda.
   b. Untuk memperbarui aturan, ubah protokol, deskripsi, dan sumbernya sesuai kebutuhan. Namun, Anda tidak dapat mengubah jenis sumber. Misalnya, jika sumbernya adalah blok IPv4 CIDR, Anda tidak dapat menentukan blok IPv6 CIDR, daftar awalan, atau grup keamanan.
   c. Untuk menghapus aturan, pilih tombol Hapus.
5. Untuk mengedit aturan keluar, pilih Edit aturan keluar dari Tindakan atau tab Aturan keluar.
   a. Untuk menambahkan aturan, pilih Tambahkan aturan dan masukkan jenis, protokol, port, dan tujuan untuk aturan tersebut. Anda juga dapat memasukkan deskripsi opsional.

Jika jenisnya adalah TCP atau UDP, Anda harus memasukkan rentang port untuk mengizinkan. Untuk ICMP kustom, Anda harus memilih jenis ICMP dari Protokol, dan, jika memungkinkan, nama kode dari Rentang port. Untuk jenis lainnya, protokol dan rentang port akan dikonfigurasikan untuk Anda.

b. Untuk memperbarui aturan, ubah protokol, deskripsi, dan sumbernya sesuai kebutuhan. Namun, Anda tidak dapat mengubah jenis sumber. Misalnya, jika sumbernya adalah blok IPv4 CIDR, Anda tidak dapat menentukan blok IPv6 CIDR, daftar awalan, atau grup keamanan.

c. Untuk menghapus aturan, pilih tombol Hapus.

6. Pilih Simpan aturan.

AWS CLI

Untuk menambahkan aturan grup keamanan

Gunakan authorize-security-group-ingressperintah untuk menambahkan aturan masuk. Contoh berikut memungkinkan lalu lintas SSH masuk dari blok CIDR dalam daftar awalan yang ditentukan.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=22,ToPort=22,PrefixListIds=[{PrefixListId=pl-
f8a6439156EXAMPLE}]'
```

Gunakan authorize-security-group-egressperintah untuk menambahkan aturan keluar. Contoh berikut memungkinkan lalu lintas TCP keluar pada port 80 ke instance dengan grup keamanan yang ditentukan.

```
aws ec2 authorize-security-group-egress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=80,ToPort=80,UserIdGroupPairs=[{GroupId=sg-0aad1c26bb6EXAMPLE}]'
```

Untuk menghapus aturan grup keamanan

Gunakan revoke-security-group-ingressperintah berikut untuk menghapus aturan masuk.

```
aws ec2 revoke-security-group-egress \
    --group id sg-1234567890abcdef0 \
    --security-group-rule-ids sgr-09ed298024EXAMPLE
```

Gunakan revoke-security-group-egressperintah berikut untuk menghapus aturan keluar.

```
aws ec2 revoke-security-group-ingress \
    --group id sg-1234567890abcdef0 \
    --security-group-rule-ids sgr-0352250c1aEXAMPLE
```

Untuk mengubah aturan grup keamanan

Gunakan perintah modify-security-group-rules. Contoh berikut mengubah blok IPv4 CIDR dari aturan grup keamanan yang ditentukan.

```
aws ec2 modify-security-group-rules \
    --group id sg-1234567890abcdef0 \
    --security-group-rules
 'SecurityGroupRuleId=sgr-09ed298024EXAMPLE,SecurityGroupRule={IpProtocol=tcp,FromPort=80,To
```

PowerShell

Untuk menambahkan aturan grup keamanan

Gunakan Grant-EC2SecurityGroupIngresscmdlet untuk menambahkan aturan masuk. Contoh berikut memungkinkan lalu lintas SSH masuk dari blok CIDR dalam daftar awalan yang ditentukan.

```
$plid = New-Object -TypeName Amazon.EC2.Model.PrefixListId
$plid.Id = "pl-f8a6439156EXAMPLE"
Grant-EC2SecurityGroupIngress `
    -GroupId sg-1234567890abcdef0 `
    -IpPermission @{IpProtocol="tcp"; FromPort=22; ToPort=22; PrefixListIds=$plid}
```

Gunakan Grant-EC2SecurityGroupEgresscmdlet untuk menambahkan aturan keluar. Contoh berikut memungkinkan lalu lintas TCP keluar pada port 80 ke instance dengan grup keamanan yang ditentukan.

```
$uigp = New-Object -TypeName Amazon.EC2.Model.UserIdGroupPair
$uigp.GroupId = "sg-0aad1c26bb6EXAMPLE"
```

```
Grant-EC2SecurityGroupEgress `
    -GroupId sg-1234567890abcdef0 `
    -IpPermission @{IpProtocol="tcp"; FromPort=80; ToPort=80; UserIdGroupPairs=
$uigp}
```

Untuk menghapus aturan grup keamanan

Gunakan Revoke-EC2SecurityGroupIngresscmdlet untuk menghapus aturan masuk.

```
Revoke-EC2SecurityGroupIngress `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRuleId sgr-09ed298024EXAMPLE
```

Gunakan Revoke-EC2SecurityGroupEgresscmdlet untuk menghapus aturan keluar.

```
Revoke-EC2SecurityGroupEgress `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRuleId sgr-0352250c1aEXAMPLE
```

Untuk mengubah aturan grup keamanan

Gunakan Edit-EC2SecurityGroupRulecmdlet. Contoh berikut mengubah blok IPv4 CIDR dari aturan grup keamanan yang ditentukan.

```
$sgrr = New-Object -TypeName Amazon.EC2.Model.SecurityGroupRuleRequest
$sgrr.IpProtocol = "tcp"
$sgrr.FromPort = 80
$sgrr.ToPort = 80
$sgrr.CidrIpv4 = "0.0.0.0/0"
$sgr = New-Object -TypeName Amazon.EC2.Model.SecurityGroupRuleUpdate
$sgr.SecurityGroupRuleId = "sgr-09ed298024EXAMPLE"
$sgr.SecurityGroupRule = $sgrr
Edit-EC2SecurityGroupRule  `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRule $sgr
```

Hapus grup keamanan Amazon EC2

Setelah selesai dengan grup keamanan yang Anda buat untuk digunakan dengan instans Amazon EC2, Anda dapat menghapusnya.

Persyaratan

- Grup keamanan tidak dapat dikaitkan dengan instance atau antarmuka jaringan.
- Grup keamanan tidak dapat direferensikan oleh aturan di grup keamanan lain.

Console

Cara menghapus grup keamanan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. (Opsional) Untuk memverifikasi bahwa grup keamanan Anda tidak terkait dengan instans, lakukan hal berikut:
   a. Pada panel navigasi, pilih Grup Keamanan.
   b. Salin ID grup keamanan untuk dihapus.
   c. Di panel navigasi, pilih Instans.
   d. Di bilah pencarian, tambahkan Grup keamanan IDs sama dengan filter dan tempel ID grup keamanan. Jika tidak ada hasil, maka grup keamanan tidak terkait dengan instance. Jika tidak, Anda harus memisahkan grup keamanan sebelum Anda dapat menghapusnya.
3. Pada panel navigasi, pilih Grup Keamanan.
4. Pilih grup keamanan lalu pilih Tindakan, Hapus Grup Keamanan.
5. Jika Anda memilih lebih dari satu grup keamanan, Anda akan diminta untuk konfirmasi. Jika beberapa grup keamanan tidak dapat dihapus, kami menampilkan status setiap grup keamanan, yang menunjukkan apakah itu akan dihapus. Untuk mengonfirmasi penghapusan, masukkan Hapus.
6. Pilih Hapus.

AWS CLI

Cara menghapus grup keamanan

Gunakan perintah berikut delete-security-group.

```
aws ec2 delete-security-group --group-id sg-1234567890abcdef0
```

PowerShell

Cara menghapus grup keamanan

Gunakan Remove-EC2SecurityGroupcmdlet.

```
Remove-EC2SecurityGroup -GroupId sg-1234567890abcdef0
```

Pelacakan koneksi grup keamanan Amazon EC2

Grup keamanan Anda menggunakan pelacakan koneksi untuk melacak informasi tentang lalu lintas ke dan dari instans. Aturan-aturan diterapkan berdasarkan status koneksi lalu lintas untuk menentukan apakah lalu lintas diizinkan atau ditolak. Dengan pendekatan ini, grup keamanan berada dalam status stateful. Artinya tanggapan-tanggapan terhadap lalu lintas ke dalam diizinkan mengalir ke luar dari instans tanpa memedulikan aturan grup keamanan ke luar, dan sebaliknya.

Sebagai contoh, anggaplah bahwa Anda memulai perintah seperti netcat atau yang mirip dengan instans Anda dari komputer rumah Anda, dan aturan grup keamanan ke dalam Anda mengizinkan lalu lintas ICMP. Informasi tentang koneksi (termasuk informasi port) akan dilacak. Lalu lintas tanggapan dari instans untuk perintah tidak dilacak sebagai permintaan baru, tetapi sebagai koneksi yang telah terbentuk dan diizinkan untuk mengalir ke luar dari instans, meskipun aturan grup keamanan ke luar Anda membatasi lalu lintas ICMP ke luar.

Untuk protokol selain TCP, UDP, atau ICMP, hanya alamat IP dan nomor protokol saja yang dilacak. Jika instans Anda mengirimkan lalu lintas ke host lain, dan host tersebut mengirimkan jenis lalu lintas yang sama ke instans Anda dalam 600 detik, maka grup keamanan untuk instans Anda akan menerimanya terlepas dari aturan-aturan ke dalam grup keamanan tersebut. Grup keamanan tersebut menerimanya karena dianggap sebagai lalu lintas tanggapan untuk lalu lintas asli.

Ketika Anda mengubah aturan grup keamanan, koneksi-koneksi yang dilacak tidak akan langsung terputus. Grup keamanan akan tetap mengizinkan paket sampai koneksi yang ada waktunya habis. Untuk memastikan lalu lintas langsung terputus, atau bahwa semua lalu lintas tunduk pada aturan-aturan firewall tanpa memedulikan status pelacakan, Anda dapat menggunakan ACL jaringan untuk subnet Anda. Jaringan ACLs tidak memiliki kewarganegaraan dan oleh karena itu tidak secara otomatis mengizinkan lalu lintas respons. Menambahkan ACL jaringan yang memblokir lalu lintas di salah satu arah akan memutuskan koneksi yang ada. Untuk informasi selengkapnya, lihat ACLs Jaringan dalam Panduan Pengguna Amazon VPC.

> **Note**
>
> Grup keamanan tidak berpengaruh pada lalu lintas DNS ke atau dari Route 53 Resolver, kadang-kadang disebut sebagai 'alamat IP VPC+2 '(lihat Apa itu Amazon Route 53 Resolver? di Panduan Pengembang Amazon Route 53), atau 'AmazonProvidedDNS' (lihat set opsi Bekerja dengan DHCP di Panduan Pengguna Amazon Virtual Private Cloud). Jika Anda ingin memfilter permintaan DNS melalui Route 53 Resolver, Anda dapat mengaktifkan Firewall DNS Route 53 Resolver (lihat Firewall DNS Route 53 Resolver di Panduan Developer Amazon Route 53).

Koneksi-koneksi yang tidak dilacak

Tidak semua aliran lalu lintas dilacak. Jika aturan grup keamanan mengizinkan aliran TCP atau UDP untuk semua lalu lintas (0.0.0.0/0 atau: :/0) dan ada aturan yang sesuai di arah lain yang mengizinkan semua lalu lintas respons (0.0.0.0/0 atau: :/0) untuk port apa pun (0-65535), maka arus lalu lintas itu tidak dilacak, kecuali itu adalah bagian dari koneksi yang dilacak secara otomatis. Lalu lintas tanggapan untuk aliran yang tidak dilacak akan diizinkan berdasarkan aturan-aturan ke dalam atau ke luar yang mengizinkan lalu lintas tanggapan, bukan berdasarkan informasi pelacakan.

Aliran lalu lintas yang tidak dilacak akan langsung diputus jika aturan yang memungkinkan aliran dihapus atau dimodifikasi. Sebagai contoh, jika Anda memiliki aturan ke luar (0.0.0.0/0) yang terbuka dan Anda menghapus aturan yang mengizinkan semua lalu lintas SSH ke dalam (0.0.0.0/0) (port TCP 22) ke instans (atau memodifikasinya sehingga koneksi tidak diizinkan lagi), maka koneksi SSH yang sudah ada pada instans tersebut akan langsung dibuang. Koneksi tersebut sebelumnya tidak dilacak, sehingga perubahan yang diterapkan akan memutus koneksi itu. Di sisi lain, jika Anda memiliki aturan ke dalam yang lebih sempit yang dari awal mengizinkan koneksi SSH (artinya koneksi dilacak), tetapi kemudian Anda mengubah aturan tersebut sehingga tidak lagi mengizinkan koneksi baru dari alamat klien SSH saat ini, maka koneksi SSH yang sudah ada tidak akan terputus karena koneksi itu sudah dilacak.

Koneksi-koneksi yang dilacak secara otomatis

Koneksi yang dilakukan melalui berikut ini secara otomatis dilacak, bahkan jika konfigurasi grup keamanan tidak memerlukan pelacakan:

- Gateway internet khusus egress
- Akselerator Global Accelerator

- Gateway NAT
- Titik akhir firewall Network Firewall
- Penyeimbang Beban Jaringan
- AWS PrivateLink (antarmuka titik akhir VPC)
- AWS Lambda (Antarmuka jaringan elastis hyperplane)
- Titik akhir gateway DynamoDB - Setiap koneksi ke DynamoDB mengkonsumsi 2 entri conntrack.

Tunjangan pelacakan koneksi

Amazon EC2 menetapkan jumlah maksimum koneksi yang dapat dilacak untuk setiap instans. Setelah jumlah maksimum tercapai, setiap paket yang dikirim atau diterima akan dihapus karena koneksi baru tidak dapat dibuat. Ketika ini terjadi, aplikasi-aplikasi yang mengirim dan menerima paket tidak akan dapat berkomunikasi dengan semestinya. Gunakan metrik performa jaringan `conntrack_allowance_available` untuk menentukan jumlah koneksi yang dilacak yang masih tersedia untuk tipe instans tersebut.

Untuk menentukan apakah paket sudah dihapus karena lalu lintas jaringan untuk instans Anda melebihi jumlah maksimum koneksi yang dapat dilacak, gunakan metrik performa jaringan `conntrack_allowance_exceeded`. Untuk informasi selengkapnya, lihat Pantau kinerja jaringan untuk pengaturan ENA pada instans EC2 Anda.

Dengan Penyeimbangan Beban Elastis, jika Anda melebihi jumlah maksimum koneksi yang dapat dilacak untuk setiap instans, kami merekomendasikan agar Anda menskalakan jumlah instans yang terdaftar dengan penyeimbang beban atau ukuran instans yang terdaftar dengan penyeimbang beban.

Praktik terbaik pelacakan koneksi

Perutean asimetris, di mana lalu lintas masuk ke sebuah instance melalui satu antarmuka jaringan dan pergi melalui antarmuka jaringan yang berbeda, dapat mengurangi kinerja puncak yang dapat dicapai oleh instans jika arus dilacak.

Untuk mempertahankan kinerja puncak dan mengoptimalkan manajemen koneksi saat pelacakan koneksi diaktifkan untuk grup keamanan Anda, kami merekomendasikan konfigurasi berikut:

- Hindari topologi routing asimetris, jika memungkinkan.
- Alih-alih menggunakan grup keamanan untuk pemfilteran, gunakan jaringan ACLs.

- Jika Anda harus menggunakan grup keamanan dengan pelacakan koneksi, konfigurasikan batas waktu pelacakan koneksi idle sesingkat mungkin. Untuk detail selengkapnya tentang batas waktu pelacakan koneksi idle, lihat bagian berikut.
- Dengan batas waktu default yang lebih pendek pada instans Nitrov6, aplikasi dengan koneksi berumur panjang (seperti kumpulan koneksi database, koneksi HTTP persisten, atau beban kerja streaming) harus mengonfigurasi nilai yang sesuai saat peluncuran instance. `TcpEstablishedTimeout`
- Untuk koneksi yang berumur panjang, konfigurasikan TCP keep alives untuk dikirim pada interval kurang dari 5 menit untuk memastikan koneksi tetap terbuka dan mempertahankan status terlacaknya. Ini membantu mencegah koneksi terputus karena batas waktu idle dan mengurangi overhead pembentukan kembali koneksi.

Untuk informasi lebih lanjut tentang penyetelan kinerja pada sistem Nitro, lihat. Pertimbangan sistem nitro untuk penyetelan kinerja

Waktu habis pelacakan koneksi idle

Grup keamanan melacak setiap koneksi yang dibuat untuk memastikan bahwa paket yang kembali dikirim seperti yang diharapkan. Ada jumlah maksimum koneksi yang dapat dilacak per instans. Koneksi yang tetap dalam keadaan idle dapat menyebabkan terbebaninya pelacakan koneksi dan menyebabkan koneksi tidak dilacak dan paket terputus. Anda sekarang dapat mengatur batas waktu untuk pelacakan koneksi pada antarmuka jaringan Elastis.

> **Note**
>
> Fitur ini hanya tersedia dengan instance berbasis Nitro. Anda harus menguji aplikasi Anda pada instance pembuatan Nitrov6 dengan batas waktu pelacakan koneksi default `350` kedua yang dikurangi sebelum menerapkan ke produksi.

Ada tiga batas waktu yang dapat dikonfigurasi:

- TCP menetapkan batas waktu: Batas waktu (dalam detik) untuk koneksi TCP idle dalam keadaan mapan.
  - Min: `60` detik
  - Maks: `432000` detik

  - Default: 350 detik untuk jenis instans Nitrov6, tidak termasuk P6e-. GB200 Dan 432000 detik untuk jenis contoh lainnya, termasuk P6e-. GB200
  - Direkomendasikan: Kurang dari 432000 detik
- Batas waktu UDP: Batas waktu (dalam detik) untuk alur UDP idle yang telah melihat lalu lintas hanya dalam satu arah atau transaksi permintaan-respons tunggal.
  - Min: 30 detik
  - Maks: 60 detik
  - Default: 30 detik
- Batas waktu aliran UDP: Batas waktu (dalam detik) untuk alur UDP idle yang diklasifikasikan sebagai alur yang telah melihat lebih dari satu transaksi permintaan-respons.
  - Min: 60 detik
  - Maks: 180 detik
  - Default: 180 detik

Anda mungkin ingin memodifikasi batas waktu default untuk salah satu kasus berikut:

- Jika Anda memantau koneksi yang dilacak menggunakan metrik performa jaringan Amazon EC2, metrik conntrack_allowance_exceeded dan conntrack_allowance_available memungkinkan Anda memantau paket yang terputus dan pemanfaatan koneksi yang dilacak untuk secara proaktif mengelola kapasitas instans EC2 dengan tindakan peningkatatan atau penurunan skala untuk membantu memenuhi permintaan koneksi jaringan sebelum memutuskan paket. Jika Anda mengamati penurunan conntrack_allowance_exceeded pada instans EC2 Anda, Anda dapat memperoleh manfaat dari menyetel batas waktu yang ditetapkan TCP yang lebih rendah untuk memperhitungkan sesi basi yang dihasilkan dari klien yang tidak tepat atau kotak tengah jaringan. TCP/UDP
- Biasanya, penyeimbang beban atau firewall memiliki batas waktu idle yang Ditetapkan TCP dalam kisaran 60 hingga 90 menit. Jika Anda menjalankan beban kerja yang diharapkan akan menangani jumlah koneksi yang sangat banyak (lebih dari 100k) dari peralatan seperti firewall jaringan, Anda disarankan untuk mengonfigurasi batas waktu yang sama pada antarmuka jaringan EC2.
- Jika Anda menjalankan beban kerja yang menggunakan topologi perutean asimetris, kami sarankan Anda mengonfigurasi batas waktu idle yang ditetapkan TCP selama 60 detik.
- Jika Anda menjalankan beban kerja dengan jumlah koneksi yang tinggi seperti DNS, SIP, SNMP, Syslog, Radius, dan layanan lain yang terutama menggunakan UDP untuk melayani permintaan,

pengaturan batas waktu 'UDP-stream' ke 60-an memberikan lebih tinggi scale/performance untuk kapasitas yang ada dan untuk mencegah kegagalan abu-abu.

- Untuk TCP/UDP koneksi melalui Network Load Balancers, semua koneksi dilacak. Nilai batas waktu idle untuk aliran TCP adalah 350 detik dan aliran UDP adalah 120 detik, serta bervariasi dari nilai batas waktu tingkat antarmuka. Anda mungkin ingin mengonfigurasi batas waktu di tingkat antarmuka jaringan untuk memungkinkan lebih banyak fleksibilitas untuk batas waktu daripada default untuk penyeimbang beban.

Anda memiliki opsi untuk mengonfigurasi batas waktu pelacakan koneksi saat Anda melakukan hal berikut:

- Membuat antarmuka jaringan
- Memodifikasi atribut antarmuka jaringan
- Meluncurkan instans EC2
- Buat templat peluncuran instans EC2

Contoh

Dalam contoh berikut, grup keamanan memiliki aturan ke dalam yang mengizinkan lalu lintas TCP dan ICMP, dan aturan ke luar yang mengizinkan semua lalu lintas ke luar.

Ke dalam

Tipe protokol	Nomor port	Sumber
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	Semua	0.0.0.0/0

Ke luar

Tipe protokol	Nomor port	Destinasi
Semua	Semua	0.0.0.0/0
Semua	Semua	::/0

Dengan koneksi jaringan langsung ke instans atau antarmuka jaringan, perilaku pelacakannya adalah sebagai berikut:

- Lalu lintas TCP ke dalam dan ke luar pada port 22 (SSH) akan dilacak, karena aturan ke dalam hanya mengizinkan lalu lintas dari 203.0.113.1/32 saja, dan bukan semua alamat IP (0.0.0.0/0).
- Lalu lintas TCP ke dalam dan ke luar pada port 80 (HTTP) tidak akan dilacak, karena aturan ke dalam dan ke luar mengizinkan lalu lintas dari semua alamat IP.
- Lalu lintas ICMP selalu dilacak.

Jika Anda menghapus aturan keluar untuk IPv4 lalu lintas, semua lalu lintas masuk dan keluar dilacak, termasuk IPv4 lalu lintas pada port 80 (HTTP). Hal yang sama berlaku untuk IPv6 lalu lintas jika Anda menghapus aturan keluar untuk IPv6 lalu lintas.

Aturan-aturan grup keamanan untuk kasus penggunaan yang berbeda

Anda dapat membuat grup keamanan dan menambahkan aturan-aturan yang mencerminkan peran dari instans yang dikaitkan dengan grup keamanan tersebut. Sebagai contoh, instans yang dikonfigurasi sebagai server web akan membutuhkan aturan-aturan grup keamanan yang mengizinkan akses HTTP dan HTTPS ke dalam. Demikian juga, instans basis data akan membutuhkan aturan-aturan yang mengizinkan akses untuk jenis basis data, seperti akses melalui port 3306 untuk MySQL.

Berikut ini adalah contoh jenis aturan yang dapat Anda tambahkan ke grup keamanan untuk jenis akses tertentu.

Contoh

- Aturan-aturan server web
- Aturan-aturan server basis data
- Aturan-aturan untuk terhubung ke instans dari komputer Anda

- Aturan-aturan untuk terhubung ke instans-instans dari instans dengan grup keamanan yang sama
- Aturan-aturan untuk melakukan ping/ICMP
- Aturan-aturan server DNS
- Aturan-aturan Amazon EFS
- Aturan-aturan Penyeimbangan Beban Elastis

Lihat petunjuknya di Membuat grup keamanan dan the section called “Mengonfigurasi aturan grup keamanan”.

Aturan-aturan server web

Aturan-aturan ke dalam berikut mengizinkan akses HTTP dan HTTPS dari alamat IP mana pun. Jika VPC diaktifkan IPv6, Anda dapat menambahkan aturan untuk mengontrol lalu lintas HTTP dan HTTPS masuk dari alamat. IPv6

Tipe protokol	Nomor protokol	Port	IP sumber	Catatan
TCP	6	80 (HTTP)	0.0.0.0/0	Memungkinkan akses HTTP masuk dari alamat apa pun IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Memungkinkan akses HTTPS masuk dari alamat apa pun IPv4
TCP	6	80 (HTTP)	::/0	Memungkinkan akses HTTP ke dalam dari alamat IPv6 apa pun
TCP	6	443 (HTTPS)	::/0	Memungkinkan akses HTTPS ke dalam dari alamat IPv6 apa pun

Aturan-aturan server basis data

Aturan-aturan ke dalam berikut adalah contoh aturan yang dapat Anda tambahkan untuk akses basis data, tergantung dari jenis basis data apa yang Anda jalankan pada instans Anda. Untuk informasi selengkapnya tentang instans Amazon RDS, lihat Panduan Pengguna Amazon RDS.

Untuk IP sumber, pilih salah satu hal berikut:

- alamat IP atau rentang alamat IP tertentu (dalam notasi blok CIDR) dalam jaringan lokal Anda
- ID grup keamanan untuk sekelompok instans yang mengakses basis data

Tipe protokol	Nomor protokol	Port	Catatan
TCP	6	1433 (MS SQL)	Port default untuk mengakses basis data Microsoft SQL Server, contohnya, pada instans Amazon RDS
TCP	6	3306 (MYSQL/Aurora)	Port default untuk mengakses basis data MySQL atau Aurora, contohnya, pada instans Amazon RDS
TCP	6	5439 (Redshift)	Port default untuk mengakses basis data klaster Amazon Redshift.
TCP	6	5432 (PostgreSQL)	Port default untuk mengakses basis data PostgreSQL, contohnya, pada instans Amazon RDS
TCP	6	1521 (Oracle)	Port default untuk mengakses basis data Oracle, contohnya, pada instans Amazon RDS

Opsional, Anda dapat membatasi lalu lintas ke luar dari server basis data Anda. Sebagai contoh, mungkin Anda ingin mengizinkan akses ke internet untuk pembaruan perangkat lunak, tetapi membatasi semua jenis lalu lintas lainnya. Anda harus terlebih dahulu menghapus aturan ke luar default yang mengizinkan semua lalu lintas ke luar.

Tipe protokol	Nomor protokol	Port	IP Tujuan	Catatan
TCP	6	80 (HTTP)	0.0.0.0/0	Memungkinkan akses HTTP keluar ke alamat apa pun IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Memungkinkan akses HTTPS keluar ke alamat apa pun IPv4
TCP	6	80 (HTTP)	::/0	(Hanya VPC yang IPv6 diaktifkan) Memungkinkan akses HTTP keluar ke alamat apa pun IPv6
TCP	6	443 (HTTPS)	::/0	(Hanya VPC yang IPv6 diaktifkan) Memungkinkan akses HTTPS keluar ke alamat apa pun IPv6

Aturan-aturan untuk terhubung ke instans dari komputer Anda

Untuk terhubung ke instans Anda, grup keamanan Anda harus memiliki aturan-aturan ke dalam yang mengizinkan akses SSH (untuk instans Linux) atau akses RDP (untuk instans Windows).

Tipe protokol	Nomor protokol	Port	IP sumber
TCP	6	22 (SSH)	IPv4 Alamat publik komputer Anda, atau berbagai alamat IP di jaringan lokal Anda. Jika VPC Anda diaktifkan IPv6 dan instans Anda memiliki IPv6 alamat, Anda dapat memasukkan IPv6 alamat atau rentang.
TCP	6	3389 (RDP)	IPv4 Alamat publik komputer Anda, atau berbagai alamat IP di jaringan lokal Anda. Jika VPC Anda diaktifkan IPv6 dan instans Anda memiliki IPv6

Tipe protokol	Nomor protokol	Port	IP sumber
			alamat, Anda dapat memasukkan IPv6 alamat atau rentang.

Aturan-aturan untuk terhubung ke instans-instans dari instans dengan grup keamanan yang sama

Untuk mengizinkan instans yang dikaitkan dengan grup keamanan yang sama untuk saling berkomunikasi satu sama lain, Anda harus secara eksplisit menambahkan aturan untuk hal ini.

> **Note**
>
> Jika Anda mengonfigurasi rute untuk meneruskan lalu lintas antara dua instans di subnet yang berbeda melalui perangkat middlebox, Anda harus memastikan bahwa grup keamanan untuk kedua instans tersebut mengizinkan lalu lintas mengalir di antara instans. Grup keamanan untuk setiap instans harus mereferensikan alamat IP privat instans lain, atau rentang CIDR dari subnet yang berisi instans yang lain, sebagai sumbernya. Jika Anda mereferensikan grup keamanan instans lain sebagai sumbernya, hal ini tidak akan mengizinkan lalu lintas mengalir di antara instans.

Tabel berikut ini menjelaskan aturan ke dalam untuk grup keamanan yang memungkinkan instans yang dikaitkan untuk saling berkomunikasi satu sama lain. Aturan ini mengizinkan semua jenis lalu lintas.

Tipe protokol	Nomor protokol	Port	IP sumber
-1 (Semua)	-1 (Semua)	-1 (Semua)	ID grup keamanan, atau rentang CIDR dari subnet yang berisi instans lainnya (lihat catatan).

Aturan-aturan untuk melakukan ping/ICMP

Perintah ping merupakan jenis lalu lintas ICMP. Untuk melakukan ping pada instans Anda, Anda harus menambahkan aturan ICMP ke dalam berikut ini.

Tipe	Protokol	Sumber		
Kustom ICMP - IPv4	Permintaan Echo	IPv4 Alamat publik komputer Anda, IPv4 alamat tertentu, IPv4 atau IPv6 alamat dari mana saja.		
Semua ICMP - IPv4	IPv4 ICMP (1)	IPv4 Alamat publik komputer Anda, IPv4 alamat tertentu, IPv4 atau IPv6 alamat dari mana saja.		

Untuk menggunakan ping6 perintah untuk melakukan ping ke IPv6 alamat untuk instance Anda, Anda harus menambahkan ICMPv6 aturan masuk berikut.

Tipe	Protokol	Sumber		
Semua ICMP - IPv6	IPv6 ICMP (58)	IPv6 Alamat komputer Anda, IPv4 alamat tertentu, IPv4 atau IPv6 alamat dari mana saja.		

Aturan-aturan server DNS

Jika Anda telah mengatur instans EC2 Anda sebagai server DNS, maka Anda harus memastikan bahwa lalu lintas TCP dan UDP dapat menjangkau server DNS Anda melalui port 53.

Untuk IP sumber, pilih salah satu hal berikut:

- alamat IP atau rentang alamat IP (dalam notasi blok CIDR) di jaringan
- ID dari grup keamanan untuk serangkaian instans dalam jaringan Anda yang membutuhkan akses ke server DNS

Tipe protokol	Nomor protokol	Port
TCP	6	53
UDP	17	53

Aturan-aturan Amazon EFS

Jika Anda menggunakan sistem file Amazon EFS dengan instans Amazon EC2 Anda, maka grup keamanan yang Anda kaitkan dengan target pengaitan Amazon EFS Anda harus mengizinkan lalu lintas melalui protokol NFS.

Tipe protokol	Nomor protokol	Port	IP sumber	Catatan
TCP	6	2049 (NFS)	ID dari grup keamanan	Mengizinkan akses NFS ke dalam dari sumber daya (termasuk target pengaitan) yang dikaitkan dengan grup keamanan ini

Untuk mengaitkan sistem file Amazon EFS pada instans Amazon EC2 Anda, Anda harus terhubung ke instans Anda. Oleh karena itu, grup keamanan yang dikaitkan dengan instans Anda harus memiliki aturan-aturan yang mengizinkan SSH ke dalam dari komputer lokal atau jaringan lokal Anda.

Tipe protokol	Nomor protokol	Port	IP sumber	Catatan
TCP	6	22 (SSH)	Rentang alamat IP dari komputer lokal Anda, atau rentang alamat IP (dalam notasi blok CIDR) untuk jaringan Anda.	Mengizinkan akses SSH ke dalam dari komputer lokal Anda.

Aturan-aturan Penyeimbangan Beban Elastis

Jika Anda mendaftarkan instans EC2 Anda dengan penyeimbang beban, grup keamanan yang terkait dengan penyeimbang beban Anda harus mengizinkan komunikasi dengan instans. Untuk informasi selengkapnya, lihat berikut ini dalam dokumentasi Elastic Load Balancing.

- Grup keamanan untuk Application Load Balancer Anda
- Grup keamanan untuk Network Load Balancer Anda
- Konfigurasikan grup keamanan untuk Classic Load Balancer Anda

NitroTPM untuk instans Amazon EC2

Nitro Trusted Platform Module (NitroTPM) adalah perangkat virtual yang disediakan oleh Sistem Nitro AWS dan sesuai dengan Spesifikasi TPM 2.0. Perangkat virtual ini akan menyimpan artefak dengan aman (seperti kata sandi, sertifikat, atau kunci enkripsi) yang digunakan untuk melakukan autentikasi terhadap instans. NitroTPM dapat membuat kunci dan menggunakan kunci tersebut untuk fungsi kriptografi (seperti melakukan hashing, penandatanganan, enkripsi, dan dekripsi).

NitroTPM menyediakan boot terukur, sebuah proses di mana bootloader dan sistem operasi membuat hash kriptografi dari setiap biner boot dan menggabungkannya dengan nilai sebelumnya di NitroTPM internal Platform Configuration Registers (). PCRs Dengan boot terukur, Anda dapat memperoleh nilai PCR yang ditandatangani dari NitroTPM dan menggunakannya untuk membuktikan kepada entitas jarak jauh integritas dari perangkat lunak boot milik instans. Hal ini dikenal sebagai pengesahan jarak jauh.

Dengan NitroTPM, kunci dan rahasia dapat ditandai dengan nilai PCR tertentu sehingga kunci dan rahasia tersebut tidak akan pernah dapat diakses jika nilai PCR, dan dengan demikian integritas

instansnya, berubah. Bentuk akses bersyarat khusus ini disebut sebagai sealing and unsealing. Teknologi sistem operasi, seperti BitLocker, dapat menggunakan NitroTPM untuk menyegel kunci dekripsi drive sehingga drive hanya dapat didekripsi ketika sistem operasi telah boot dengan benar dan dalam keadaan baik yang diketahui.

Untuk menggunakan NitroTPM, Anda harus memilih Amazon Machine Image (AMI) yang telah dikonfigurasi untuk dukungan NitroTPM, dan kemudian menggunakan AMI untuk meluncurkan instans berbasis Nitro. Anda dapat memilih salah satu prebuilt Amazon AMIs atau membuatnya sendiri.

Harga

Tidak ada biaya tambahan yang dikenakan untuk menggunakan NitroTPM. Anda hanya harus membayar untuk sumber daya dasar yang Anda gunakan.

Daftar Isi

- Persyaratan untuk menggunakan NitroTPM dengan instans Amazon EC2
- Aktifkan AMI Linux untuk NitroTPM
- Verifikasi bahwa AMI diaktifkan untuk NitroTPM
- Mengaktifkan atau berhenti menggunakan NitroTPM pada instans Amazon EC2
- Verifikasi bahwa instans Amazon EC2 diaktifkan untuk NitroTPM
- Ambil kunci dukungan publik untuk instans EC2

Persyaratan untuk menggunakan NitroTPM dengan instans Amazon EC2

Untuk meluncurkan instance dengan NitroTPM diaktifkan, Anda harus memenuhi persyaratan berikut.

Topik

- AMIs
- Tipe instans
- Pertimbangan-pertimbangan

AMIs

AMI harus mengaktifkan NitroTPM.

Linux AMIs

Tidak ada yang telah dikonfigurasi sebelumnya AMIs. Anda harus mengkonfigurasi AMI Anda sendiri. Untuk informasi selengkapnya, lihat Aktifkan AMI Linux untuk NitroTPM.

Jendela AMIs

Untuk menemukan AMI AWS Windows yang telah dikonfigurasi sebelumnya untuk NitRotPM dan UEFI Secure Boot dengan kunci Microsoft, lihat Temukan Windows Server yang AMIs dikonfigurasi dengan NitRotPM dan UEFI Secure Boot di Referensi Windows.AWS AMIs

> **Note**
>
> Sistem operasi — AMI harus menyertakan sistem operasi dengan driver TPM 2.0 Command Response Buffer (CRB). Sebagian besar sistem operasi saat ini termasuk driver TPM 2.0 CRB.
> Mode boot UEFI — AMI harus dikonfigurasi untuk mode boot UEFI. Untuk informasi selengkapnya, lihat Boot Aman UEFI untuk instans Amazon EC2.

Tipe instans

Anda harus menggunakan salah satu jenis instance virtual berikut:

- Tujuan umum: M5, M5a, M5ad, M5d, M5dn, M5n, M5Zn, M6a, M6g, M6gd, M6i, M6iD, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex, M8a, M8AZN, m8g, m8gb, m8gd, m8gn, m8i, m8id, m8i-flex, t3, t3a, t4g
- Komputasi dioptimalkan: C5, C5a, C5ad, C5d, C5n, C6a, C6g, C6gd, C6Gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gN, C7i, C7i-flex, C8a, C8g, C8gB, C8gB d, C8GN, C8i, C8id, C8i-flex
- Memori dioptimalkan: R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6g, R6gd, R6i, R6iD, R6idn, R6in, R7a, R7g, R7gd, R7i, R7iZ, R8a, R8a, R8g, R8GB, R8GD, R8GN, R8i, R8id, R8i-Flex, U7i-6TB, U7i-8tb, U7i-12TB, U7in-16TB, U7in-24TB, U7in-32tb, X2iEDN, X2iEZN, X8g, X8AEDZ, X8i, z1d
- Penyimpanan dioptimalkan: D3, D3en, i3en, i4i, i7i, i7ie, i8g, i8ge, iM4gn
- Komputasi yang dipercepat: F2, G4dn, G5, G6, G6e, G6f, Gr6, Gr6f, G7e, Inf1, Inf2, P5, P5e, P5en, P6-B200, P6-B300, Trn2, Trn2u
- Komputasi kinerja tinggi: HPC6a, HPC6id, HPC8a

Pertimbangan-pertimbangan

Pertimbangan-pertimbangan berikut ini berlaku saat Anda menggunakan NitroTPM:

- Setelah Anda meluncurkan instance menggunakan AMI dengan nitRotPM diaktifkan, jika Anda ingin mengubah jenis instance, jenis instans baru yang Anda pilih juga harus mendukung NitRotPM.
- BitLocker volume yang dienkripsi dengan kunci berbasis NitroTPM hanya dapat digunakan pada instance asli.
- Status NitroTPM tidak ditampilkan di konsol Amazon EC2.
- Status NitroTPM tidak disertakan dalam Snapshot Amazon EBS.
- Status NitroTPM tidak disertakan dalam citra VM Import/Export.
- NitroTPM tidak didukung pada AWS Outposts., Local Zones, atau Wavelength Zones.

Aktifkan AMI Linux untuk NitroTPM

Untuk mengaktifkan NitRotPM untuk sebuah instance, Anda harus meluncurkan instance menggunakan AMI dengan NitroTPM diaktifkan. Anda harus mengkonfigurasi AMI Linux Anda dengan dukungan NitroTPM ketika Anda mendaftarkannya. Anda tidak dapat mengonfigurasi dukungan NitroTPM nanti.

Untuk daftar Windows AMIs yang telah dikonfigurasi sebelumnya untuk dukungan NitroTPM, lihat. Persyaratan untuk menggunakan NitroTPM dengan instans Amazon EC2

Anda harus membuat AMI dengan nitRotPM yang dikonfigurasi dengan menggunakan API. RegisterImage Anda tidak dapat menggunakan konsol Amazon EC2 atau Impor/Ekspor VM.

Untuk mengaktifkan AMI Linux untuk NitroTPM

1. Luncurkan instance sementara dengan AMI Linux yang Anda butuhkan. Perhatikan ID volume root, yang dapat Anda temukan di konsol pada tab Storage untuk instance.
2. Setelah instance mencapai `running` status, buat snapshot dari volume root instance. Untuk informasi selengkapnya, lihat Membuat snapshot volume EBS.
3. Daftarkan snapshot yang Anda buat sebagai AMI. Dalam pemetaan perangkat blok, tentukan snapshot yang Anda buat untuk volume root.

Berikut ini adalah contoh perintah register-image. Untuk `--tpm-support`, tentukan `v2.0`. Untuk `--boot-mode`, tentukan `uefi`.

```
aws ec2 register-image \
    --name my-image \
    --boot-mode uefi \
    --architecture x86_64 \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0abcdef1234567890} \
    --tpm-support v2.0
```

Berikut ini adalah contoh untuk Register-EC2Imagecmdlet.

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
    -Name my-image `
    -Architecture "x86_64" `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
    -BootMode Uefi `
    -TpmSupport V20
```

4. Hentikan instance sementara yang Anda luncurkan di langkah 1.

Verifikasi bahwa AMI diaktifkan untuk NitroTPM

Untuk mengaktifkan NitRotPM untuk sebuah instance, Anda harus meluncurkan instance menggunakan AMI dengan NitroTPM diaktifkan. Anda dapat menjelaskan gambar untuk memverifikasi bahwa itu diaktifkan untuk NitroTPM. Jika Anda adalah pemilik AMI, Anda dapat menggambarkan atribut `tpmSupport` gambar.

Konsol Amazon EC2 tidak ditampilkan. `TpmSupport`

AWS CLI

Untuk memverifikasi bahwa NitroTPM diaktifkan

Gunakan perintah describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].TpmSupport
```

Jika NitroTPM diaktifkan untuk AMI, outputnya adalah sebagai berikut. Jika TPM tidak diaktifkan, output kosong.

```
[
    "v2.0"
]
```

Atau, jika Anda adalah pemilik AMI, Anda dapat menggunakan describe-image-attributeperintah dengan `tpmSupport` atribut.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute tpmSupport
```

Berikut ini adalah output contoh.

```
{
    "ImageId": "ami-0abcdef1234567890",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Untuk menemukan AMIs dengan NitroTPM diaktifkan

Contoh berikut mencantumkan AMIs yang IDs Anda miliki dengan NitroTPM diaktifkan.

```
aws ec2 describe-images \
    --owners self \
    --filters Name=tpm-support,Values=v2.0 \
    --query Images[].ImageId
```

PowerShell

Untuk memverifikasi bahwa NitroTPM diaktifkan

Gunakan Get-EC2Imagecmdlet.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | Select TpmSupport
```

Jika NitroTPM diaktifkan untuk AMI, outputnya adalah sebagai berikut. Jika TPM tidak diaktifkan, output kosong.

```
TpmSupport
----------
v2.0
```

Atau, jika Anda adalah pemilik AMI, Anda dapat menggunakan Get-EC2ImageAttributecmdlet dengan atribut. `tpmSupport`

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute tpmSupport
```

Untuk menemukan AMIs dengan NitroTPM diaktifkan

Contoh berikut mencantumkan AMIs yang IDs Anda miliki dengan NitroTPM diaktifkan.

```
Get-EC2Image `
    -Owner self `
    -Filter @{Name="tpm-support; Values="v2.0"} | Select ImageId
```

Mengaktifkan atau berhenti menggunakan NitroTPM pada instans Amazon EC2

Anda dapat mengaktifkan instans Amazon EC2 untuk NitroTPM hanya saat peluncuran. Setelah instance diaktifkan untuk NitRotPM, Anda tidak dapat menonaktifkannya. Jika Anda tidak perlu lagi menggunakan NitroTPM, Anda harus mengkonfigurasi sistem operasi untuk berhenti menggunakannya.

Topik

- Meluncurkan instans dengan NitroTPM
- Menghentikan menggunakan NitroTPM pada instans

Meluncurkan instans dengan NitroTPM

Ketika Anda meluncurkan instans dengan prasyarat, NitroTPM secara otomatis akan diaktifkan pada instans. Anda dapat mengaktifkan NitroTPM pada instance hanya saat peluncuran. Untuk informasi tentang cara meluncurkan instans, lihat Luncurkan instans Amazon EC2.

Menghentikan menggunakan NitroTPM pada instans

Setelah meluncurkan instance dengan NitRotPM diaktifkan, Anda tidak dapat menonaktifkan NitRotPM untuk instance tersebut. Namun demikian, Anda dapat mengonfigurasi sistem operasi untuk berhenti menggunakan NitroTPM dengan menonaktifkan driver perangkat TPM 2.0 pada instans menggunakan alat-alat berikut:

- Untuk instance Linux, gunakan tpm-tools.
- Untuk instance Windows, gunakan konsol manajemen TPM (tpm.msc).

Untuk informasi selengkapnya tentang bagaimana menonaktifkan driver perangkat, lihat dokumentasi untuk sistem operasi Anda.

Verifikasi bahwa instans Amazon EC2 diaktifkan untuk NitroTPM

Anda dapat memverifikasi apakah instans Amazon EC2 diaktifkan untuk NitroTPM. Jika dukungan NitroTPM diaktifkan pada instance, perintah kembali. `"v2.0"` Jika tidak, `TpmSupport` bidang tidak ada dalam output.

Konsol Amazon EC2 tidak menampilkan bidang. `TpmSupport`

AWS CLI

Untuk memverifikasi apakah sebuah instance diaktifkan untuk NitRotPM

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].TpmSupport
```

PowerShell

Untuk memverifikasi apakah sebuah instance diaktifkan untuk NitRotPM

Gunakan Get-EC2Instancecmdlet.

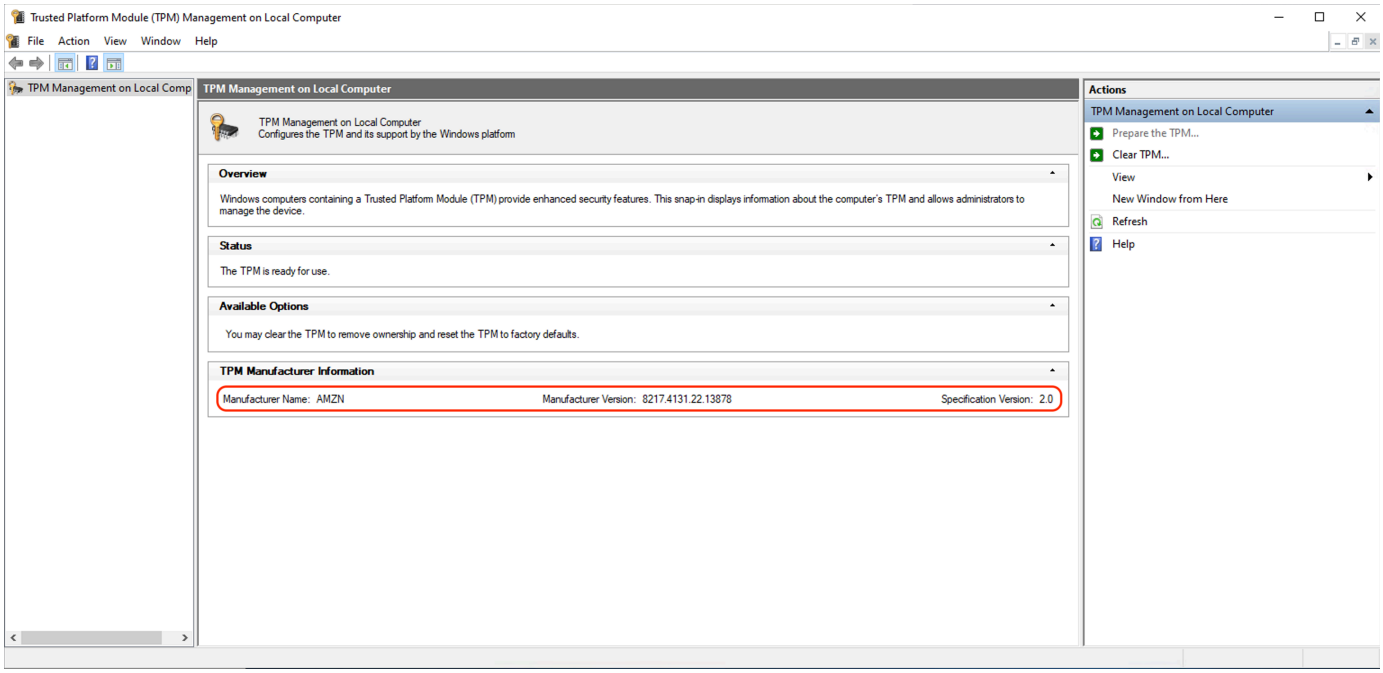
```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.TpmSupport
```

Verifikasi akses NitroTPM pada instance Windows Anda

(Hanya instance Windows) Untuk memverifikasi apakah NitrotPM dapat diakses oleh Windows

1. Hubungkan ke instans Windows EC2 Anda.
2. Pada instans tersebut, jalankan program tpm.msc.

   Jendela Manajemen TPM pada Komputer Lokal akan terbuka.
3. Periksa bidang Informasi Produsen TPM. Bidang tersebut berisi nama produsen dan versi NitroTPM yang ada pada instans.



Ambil kunci dukungan publik untuk instans EC2

Anda dapat dengan aman mengambil kunci dukungan publik untuk sebuah instance kapan saja.

AWS CLI

Untuk mengambil kunci dukungan publik untuk sebuah contoh

Gunakan perintah get-instance-tpm-ek-pub.

Contoh 1

Contoh berikut mendapatkan kunci dukungan `rsa-2048` publik dalam `tpmt` format untuk instance tertentu.

```
aws ec2 get-instance-tpm-ek-pub \
    --instance-id i-1234567890abcdef0 \
    --key-format tpmt \
    --key-type rsa-2048
```

Berikut ini adalah contoh output.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Contoh 2

Contoh berikut mendapatkan kunci dukungan `rsa-2048` publik dalam `der` format untuk instance tertentu.

```
aws ec2 get-instance-tpm-ek-pub \
    --instance-id i-1234567890abcdef0 \
    --key-format der \
    --key-type rsa-2048
```

Berikut ini adalah contoh output.

```
{
    "InstanceId": "i-1234567890abcdef0",
```

```
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

PowerShell

Untuk mengambil kunci dukungan publik untuk sebuah contoh

Gunakan Get-EC2InstanceTpmEkPubcmdlet.

Contoh 1

Contoh berikut mendapatkan kunci dukungan `rsa-2048` publik dalam `tpmt` format untuk instance tertentu.

```
Get-EC2InstanceTpmEkPub `
    -InstanceId i-1234567890abcdef0 `
    -KeyFormat tpmt `
    -KeyType rsa-2048
```

Contoh 2

Contoh berikut mendapatkan kunci dukungan `rsa-2048` publik dalam `der` format untuk instance tertentu.

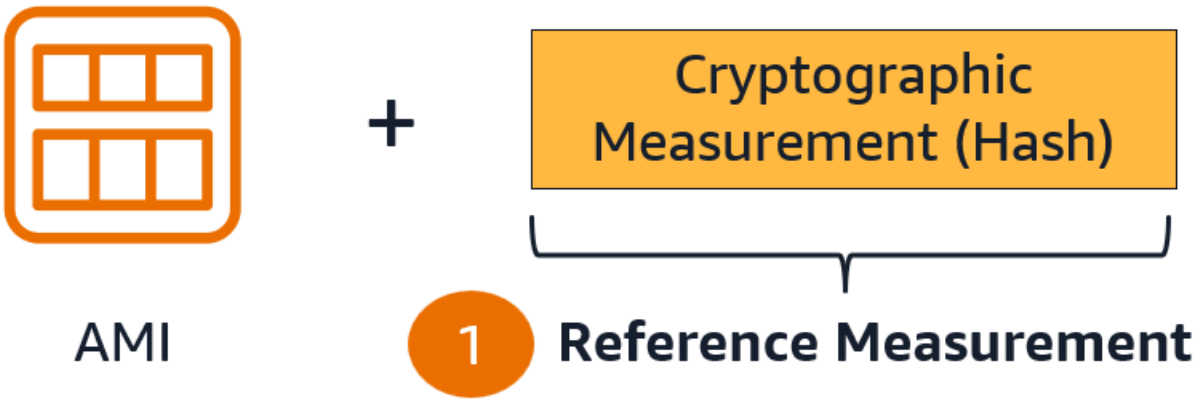
```
Get-EC2InstanceTpmEkPub `
    -InstanceId i-1234567890abcdef0 `
    -KeyFormat der `
    -KeyType rsa-2048
```

Pengesahan instans Amazon EC2

Pengesahan adalah proses yang memungkinkan Anda membuktikan secara kriptografi kepada pihak mana pun bahwa hanya perangkat lunak tepercaya, driver, dan proses boot yang berjalan

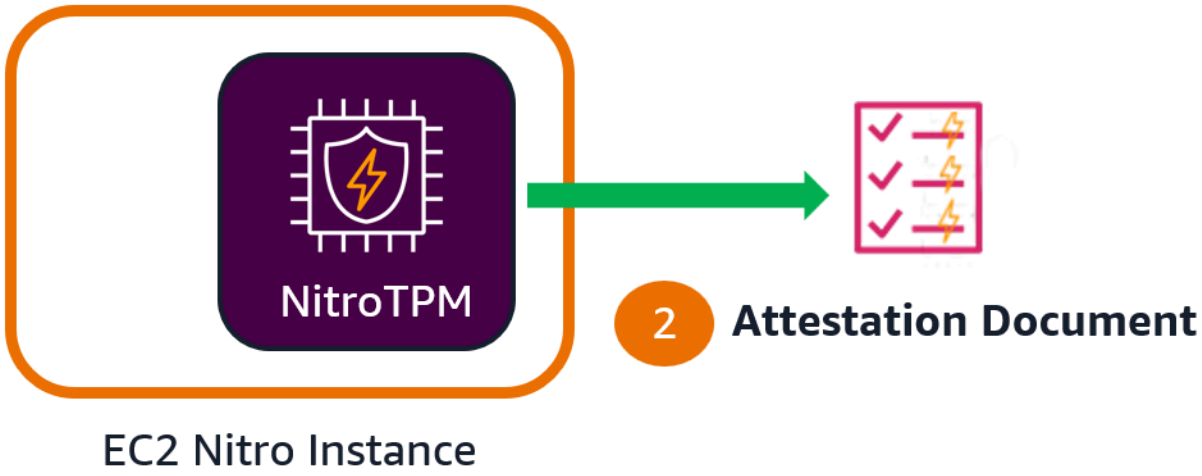
pada instans Amazon EC2. Pengesahan instans Amazon EC2 didukung oleh Nitro Trusted Platform Module (NitroTPM) dan Attestable. AMIs

Langkah pertama untuk pengesahan adalah membangun AMI yang Dapat Dibuktikan dan menentukan pengukuran referensi AMI tersebut. AMI yang Dapat Dibuktikan adalah AMI yang dibangun dari bawah ke atas untuk pengesahan. Pengukuran referensi adalah pengukuran semua perangkat lunak dan konfigurasi yang telah Anda sertakan dalam AMI Anda. Untuk informasi lebih lanjut tentang bagaimana Anda dapat memperoleh pengukuran referensi, lihatMembangun deskripsi gambar sampel.



Langkah selanjutnya adalah meluncurkan instans EC2 berkemampuan Nitro-TPM dengan AMI Attestable. Setelah Anda meluncurkan instance, Anda dapat menggunakan alat NitRotPM untuk menghasilkan Dokumen Pengesahan. Kemudian Anda dapat membandingkan pengukuran sebenarnya dari instans EC2 Anda dari Dokumen Pengesahan dengan pengukuran referensi untuk memeriksa apakah instance memiliki perangkat lunak dan konfigurasi yang Anda percayai.

Dengan membandingkan pengukuran referensi yang dihasilkan selama proses pembuatan AMI yang Dapat Dibuktikan dengan pengukuran yang disertakan dalam Dokumen Pengesahan instans, Anda dapat memvalidasi bahwa hanya perangkat lunak dan kode yang Anda percayai yang berjalan pada instance.



Integrasi dengan AWS KMS

Untuk mempermudah proses membandingkan pengukuran, Anda dapat menggunakan AWS Key Management Service (AWS KMS) sebagai verifier untuk Dokumen Pengesahan. Dengan AWS KMS, Anda dapat membuat kebijakan kunci KMS berbasis pengesahan yang memungkinkan operasi tertentu dengan kunci KMS hanya jika Anda memberikan Dokumen Pengesahan dengan pengukuran yang sesuai dengan pengukuran referensi. Untuk melakukannya, Anda menambahkan kunci kondisi tertentu ke kebijakan kunci KMS Anda yang menggunakan pengukuran referensi sebagai nilai kunci kondisi, lalu tentukan operasi KMS mana yang diizinkan jika kunci kondisi terpenuhi.

Saat Anda melakukan operasi KMS menggunakan kunci KMS, Anda harus melampirkan Dokumen Pengesahan ke permintaan KMS. AWS KMS kemudian memvalidasi pengukuran dari Dokumen Pengesahan terhadap pengukuran referensi dalam kebijakan kunci KMS, dan memungkinkan akses kunci hanya jika pengukuran cocok.

Selain itu, ketika Anda membuat Dokumen Pengesahan untuk sebuah instance, Anda harus menentukan kunci publik untuk key pair yang Anda miliki. Kunci publik yang ditentukan termasuk dalam Dokumen Pengesahan. Ketika AWS KMS memvalidasi Dokumen Pengesahan dan memungkinkan operasi dekripsi, secara otomatis mengenkripsi respons dengan kunci publik yang disertakan dalam Dokumen Pengesahan sebelum dikembalikan. Ini memastikan bahwa respons dapat didekripsi dan digunakan hanya dengan kunci pribadi yang cocok untuk kunci publik yang disertakan dalam Dokumen Pengesahan.

Ini memastikan bahwa hanya instance yang menjalankan perangkat lunak dan kode tepercaya yang dapat melakukan operasi kriptografi menggunakan kunci KMS.

Membuktikan lingkungan komputasi yang terisolasi

Secara umum, Anda dapat membuat dan mengonfigurasi instans EC2 menjadi lingkungan komputasi terisolasi, yang tidak menyediakan akses interaktif dan tidak ada mekanisme bagi administrator dan pengguna Anda untuk mengakses data yang sedang diproses dalam instans EC2. Dengan pengesahan instans EC2, Anda dapat membuktikan kepada pihak ketiga atau layanan bahwa instans Anda berjalan sebagai lingkungan komputasi yang terisolasi. Untuk informasi selengkapnya, lihat Mengisolasi data dari operator Anda sendiri.

Sebagai contoh, lihat contoh deskripsi gambar Amazon Linux 2023 yang membuat lingkungan komputasi terisolasi. Anda dapat menggunakan deskripsi gambar sampel ini sebagai titik awal dan menyesuaikannya untuk memenuhi kebutuhan Anda.

AWS model tanggung jawab bersama

NitroTPM dan AMI Attestable adalah blok bangunan yang dapat membantu Anda mengatur dan mengonfigurasi pengesahan pada instans EC2 Anda. Anda bertanggung jawab untuk mengonfigurasi AMI untuk memenuhi kasus penggunaan Anda masing-masing. Untuk informasi selengkapnya, lihat AWS Model Tanggung Jawab Bersama.

Topik

- Dapat dibuktikan AMIs
- Bersiaplah AWS KMS untuk pengesahan
- Dapatkan Dokumen Pengesahan NitroTPM
- Integrasi dengan AWS KMS
- Mengisolasi data dari operator Anda sendiri

Dapat dibuktikan AMIs

AMI yang Dapat Dibuktikan adalah Gambar Mesin Amazon (AMI) dengan hash kriptografi yang sesuai yang mewakili semua isinya. Hash dihasilkan selama proses pembuatan AMI, dan dihitung berdasarkan seluruh konten AMI itu, termasuk aplikasi, kode, dan proses boot.

Mempertahankan Negara yang Dapat Dibuktikan

Pengukuran instance didasarkan pada status boot awalnya. Setiap perubahan perangkat lunak atau kode yang dibuat pada instance setelah peluncuran dan yang bertahan setelah restart akan

mengubah pengukuran instance setelah restart. Jika pengukuran diubah, pengukuran tersebut menyimpang dari pengukuran referensi AMI yang Dapat Dibuktikan, dan instance tidak akan lagi dapat dibuktikan dengan sukses setelah instance dimulai ulang AWS KMS . Oleh karena itu, AMIs agar Attestable berguna, instance harus kembali ke status boot aslinya setelah restart.

Selalu kembali ke status boot asli memastikan bahwa sebuah instance dapat berhasil membuktikan setelah restart. Utilitas berikut dapat digunakan untuk memastikan bahwa instans Anda tetap dapat dibuktikan setelah restart:

- `erofs`— Sistem File Baca-Saja yang Ditingkatkan. Utilitas ini memastikan bahwa sistem file root Anda hanya-baca. Dengan utilitas ini, menulis ke sistem file, termasuk,`/etc`, dan `/run/var`, disimpan dalam memori dan hilang ketika instance dimulai ulang, meninggalkan sistem file root dalam status peluncuran aslinya. Untuk informasi selengkapnya, lihat dokumentasi erofs.
- `dm-verity`— Memberikan perlindungan integritas untuk sistem file root read-only. Utilitas menghitung hash dari blok sistem file dan menyimpannya di baris perintah kernel. Hal ini memungkinkan kernel untuk memverifikasi integritas sistem file selama boot. Untuk informasi selengkapnya, lihat dokumentasi dm-verity.

Persyaratan untuk membuat Attestable AMIs

Dapat dibuktikan AMIs memiliki persyaratan sebagai berikut:

- Sistem operasi dasar - Amazon Linux 2023 dan NixOS
- Arsitektur — `x86_64` atau `arm64` arsitektur
- Dukungan TPM - NitroTPM harus diaktifkan. Untuk informasi selengkapnya, lihat Persyaratan untuk menggunakan NitroTPM dengan instans Amazon EC2.
- Mode boot — Mode boot UEFI harus diaktifkan.

Topik

- Menciptakan Dapat Dibuktikan AMIs
- Buat contoh deskripsi gambar Amazon Linux 2023
- Contoh deskripsi gambar Amazon Linux 2023
- Sesuaikan contoh deskripsi gambar Amazon Linux 2023 untuk beban kerja Anda
- Hitung pengukuran PCR untuk AMI khusus

Menciptakan Dapat Dibuktikan AMIs

Untuk membuat AMI yang Dapat Dibuktikan, Anda harus menggunakan Amazon Linux 2023 dengan KIWI Next Generation (KIWI NG). Amazon Linux 2023 menyediakan semua perangkat lunak dan utilitas yang diperlukan untuk membangun AMI yang Dapat Dibuktikan menggunakan KIWI NG.

KIWI NG adalah alat sumber terbuka untuk membangun gambar berbasis Linux yang telah dikonfigurasi sebelumnya. KIWI NG menggunakan deskripsi gambar XMLyang menentukan isi dari sebuah gambar. Deskripsi gambar menentukan sistem operasi dasar, perangkat lunak, konfigurasi kernel, dan skrip yang akan dijalankan untuk membangun ready-to-use AMI untuk kasus penggunaan tertentu.

Selama waktu pembuatan AMI, Anda perlu menggunakan `nitro-tpm-pcr-compute` utilitas untuk menghasilkan pengukuran referensi berdasarkan Unified Kernel Image (UKI) yang dihasilkan oleh KIWI NG. Untuk informasi selengkapnya tentang penggunaan `nitro-tpm-pcr-compute` utilitas, lihatHitung pengukuran PCR untuk AMI khusus.

AWS menyediakan contoh deskripsi gambar Amazon Linux 2023 yang mencakup semua konfigurasi yang diperlukan untuk mengonfigurasi instans EC2 dalam lingkungan komputasi yang terisolasi. Untuk informasi selengkapnya, lihat Buat contoh deskripsi gambar Amazon Linux 2023.

Buat contoh deskripsi gambar Amazon Linux 2023

AWS memberikan contoh deskripsi gambar Amazon Linux 2023 yang dapat Anda gunakan sebagai titik awal untuk membuat Attestable kustom Anda sendiri AMIs untuk beban kerja Anda. Deskripsi gambar sampel mencakup Amazon Linux 2023 sebagai sistem operasi dasar, `dm-verity` dan `erofs` konfigurasi untuk kekekalan sistem file, dan menghapus semua akses interaktif (seperti SSH, koneksi instans EC2, dan konsol serial) untuk membuat lingkungan komputasi yang terisolasi. Untuk informasi selengkapnya tentang deskripsi gambar sampel, lihat repo Github.

Deskripsi gambar sampel secara otomatis menginstal alat nitRotPM (`nitro-tpm-pcr-compute`dan`nitro-tpm-attest`) pada gambar bawaan di direktori. `/usr/bin/` Ini memastikan bahwa alat sudah diinstal sebelumnya pada instance yang diluncurkan dari AMI.

Deskripsi gambar sampel mencakup skrip`edit_boot_install.sh`, yang mencakup perintah yang diperlukan untuk menghasilkan pengukuran referensi. Script memasang file image disk mentah (`.raw`) yang dibuat oleh KIWI NG ke perangkat loopback, menempatkan UKI, yang memiliki ekstensi `.efi` file, dan kemudian menjalankan `nitro-tpm-pcr-compute` utilitas untuk menghasilkan pengukuran referensi untuk AMI. Skrip secara otomatis dijalankan oleh KIWI NG selama waktu pembuatan.

Tutorial ini menunjukkan cara membuat deskripsi gambar sampel untuk membuat AMI yang Dapat Dibuktikan.

Untuk informasi selengkapnya tentang membuat deskripsi gambar Anda sendiri, lihat dokumentasi KIWI NG berikut:

- Mulai Cepat
- Deskripsi Gambar
- Contoh deskripsi gambar Amazon Linux 2023

Prasyarat

Identitas IAM Anda harus memiliki izin berikut untuk menyelesaikan tutorial ini:

- `ebs:CompleteSnapshot`,`ebs:StartSnapshot`, dan `ebs:PutSnapshotBlock` pada `arn:aws:ec2:*::snapshot/*`
- `ec2:RegisterImage` di semua sumber daya

Untuk membuat contoh deskripsi gambar Amazon Linux 2023 menggunakan KIWI NG

1. Luncurkan instans Amazon EC2 menggunakan AMI AL2023 terbaru. Untuk memastikan instans Anda memiliki ruang penyimpanan yang cukup untuk membangun AMI, pastikan Anda menyediakan setidaknya 12 GB penyimpanan.
2. Instal dependensi yang diperlukan. Perintah berikut menginstal utilitas berikut:
   - `kiwi-cli`
   - `veritysetup`
   - `erofs-utils`
   - `aws-nitro-tpm-tools`

   ```
   sudo dnf install -y kiwi-cli python3-kiwi kiwi-systemdeps-core python3-poetry-core
    qemu-img veritysetup erofs-utils git cargo aws-nitro-tpm-tools
   ```
3. Instal `coldsnap` utilitas. Utilitas ini memungkinkan Anda membuat snapshot Amazon EBS dari data gambar mentah. Anda akan menggunakan utilitas ini untuk membuat snapshot EBS dari file gambar disk mentah yang dibuat oleh KIWI NG.

```
git clone https://github.com/awslabs/coldsnap.git
cd coldsnap
cargo install --locked coldsnap
cd ..
```

4. Dapatkan contoh file deskripsi gambar.

```
sudo dnf install kiwi-image-descriptions-examples
```

File deskripsi gambar sampel diunduh ke direktori berikut: `/usr/share/kiwi-image-descriptions-examples/al2023/attestable-image-example`

5. Bangun deskripsi gambar sampel menggunakan `system build` perintah KIWI NG. Perintah berikut membuat file image disk mentah dalam `./image` direktori.

```
sudo kiwi-ng \
--color-output \
--loglevel 0 \
system build \
--description /usr/share/kiwi-image-descriptions-examples/al2023/attestable-image-example \
--target-dir ./image
```

Untuk informasi selengkapnya, lihat dokumentasi pembuatan sistem kiwi-ng.

6. Dapatkan pengukuran referensi untuk AMI. Pengukuran dihasilkan oleh `nitro-tpm-pcr-compute` utilitas selama waktu pembuatan gambar pada langkah sebelumnya. Anda dapat menemukan pengukuran referensi dalam file berikut: `./image/pcr_measurements.json`.

Pengukuran disediakan dalam format JSON berikut:

```
{
  "Measurements": {
    "HashAlgorithm": "SHA384 { ... }",
    "PCR4": "PCR4_measurement",
    "PCR7": "PCR7_measurement",
    "PCR12": "PCR12_measurement"
  }
}
```

7. Gunakan `coldsnap` utilitas untuk mengunggah gambar disk mentah yang dibuat oleh KIWI NG ke snapshot EBS. Perintah mengembalikan ID snapshot. Buat catatan ID, Anda akan membutuhkannya untuk langkah berikutnya.

```
SNAPSHOT=$(.cargo/bin/coldsnap upload ./image/al2023*.raw)
echo "Created snapshot: $SNAPSHOT"
```

   Untuk informasi lebih lanjut tentang `coldsnap` utilitas, lihat repo coldsnap GitHub .

8. Daftarkan AMI berkemampuan TPM 2.0 dengan mode boot UEFI menggunakan snapshot dari langkah sebelumnya. Untuk`--architecture`, tentukan `x86_64` untuk Intel, atau `arm64` untuk Graviton.

```
aws ec2 register-image \
--name "attestable_isolated_al2023_ami" \
--virtualization-type hvm \
--boot-mode uefi \
--architecture x86_64|arm64 \
--root-device-name /dev/xvda \
--block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=${SNAPSHOT}} \
--tpm-support v2.0 \
--ena-support
```

Contoh deskripsi gambar Amazon Linux 2023

Contoh deskripsi gambar Amazon Linux 2023 memiliki karakteristik sebagai berikut:

1. Boot Unified Kernel Image (UKI) — Boot menggunakan biner tunggal bertanda tangan yang menggabungkan kernel,`initrd`, dan parameter boot menjadi satu gambar yang tidak dapat diubah.
2. Sistem file root hanya-baca — Gunakan Sistem File Hanya Baca yang Ditingkatkan (`erofs`) dengan perlindungan dm-verity untuk memastikan bahwa sistem file root tidak dapat dimodifikasi dan mempertahankan verifikasi integritas kriptografi.
3. Sistem file overlay sementara — Buat sistem file overlay sementara yang memungkinkan penulisan sementara ke direktori seperti,, dan. `/etc` `/run` `/var` Karena sistem file overlay ini hanya ada di memori, semua perubahan secara otomatis hilang saat instance reboot, memastikan sistem kembali ke status tepercaya aslinya.

4. Metode akses jarak jauh yang dinonaktifkan - Hapus mekanisme akses jarak jauh berikut untuk mencegah akses jarak jauh:

Metode Akses	Deskripsi	Implementasi deskripsi gambar
SSH	Tidak termasuk server OpenSSH. Membuat instance secara inheren tidak mampu menangani lalu lintas SSH.	Abaikan `openssh-server` paket*
Data Pengguna	Menghapus Cloud-init. Menghilangkan kemampuan operator untuk menyediakan data pengguna ke instance dan menjalankan skrip boot-time.	Abaikan `cloud-init-cfg-ec2` paket `cloud-init` dan *
Kronis	Menonaktifkan port perintah chrony. Mencegah operator menjalankan perintah chrony pada instance yang sedang berjalan.	Abaikan `amazon-chrony-config` paket*
MOTD	Menghapus paket MOTD. Menghilangkan kemampuan operator untuk mengubah pesan atau fungsionalitas pada instance yang sedang berjalan.	Abaikan `update-motd` paket*
AWS SSM	Menghapus agen AWS SSM. Mencegah akses jarak jauh ke instance yang sedang berjalan menggunakan AWS SSM.	Abaikan `amazon-ssm-agent` paket*
EC2 Instance Connect	Menghapus paket EC2 Instance Connect. Menonaktifkan akses SSH menggunakan alat ini.	Abaikan `ec2-instance-connect` paket*

Metode Akses	Deskripsi	Implement asi deskripsi gambar
Konsol Serial	Menonaktifkan konsol serial. Memastikan bahwa akses konsol tidak tersedia untuk menjalankan instance dan menghapus kemampuan operator untuk masuk ke konsol serial.	Dinonakti fkan melalui parameter baris perintah kernel

* Untuk informasi lebih lanjut, lihat Elemen Deskripsi Gambar.

Sesuaikan contoh deskripsi gambar Amazon Linux 2023 untuk beban kerja Anda

Anda dapat menyesuaikan contoh deskripsi gambar Amazon Linux 2023 dan menyertakan paket perangkat lunak, skrip, dan file yang diperlukan untuk beban kerja spesifik Anda. Kustomisasi dicapai dengan menambahkan atau memodifikasi berbagai elemen dalam deskripsi gambar KIWI NG.

Topik

- Manajemen repositori
- Manajemen Package
- Menambahkan file dan direktori
- Menambahkan skrip kustom

Manajemen repositori

Secara default, deskripsi gambar sampel menyertakan satu `<repository>` elemen yang menunjuk ke titik akhir cermin untuk repositori inti Amazon Linux 2023. Jika perlu, Anda dapat menambahkan referensi ke repositori lain untuk menginstal perangkat lunak yang Anda butuhkan.

Deskripsi gambar sampel menggunakan manajer `dnf` paket, seperti yang didefinisikan dalam `<packagemanager>` elemen.

Untuk informasi selengkapnya tentang menambahkan repositori, lihat Menyiapkan Repositori.

Manajemen Package

Secara default, deskripsi gambar sampel mencakup semua paket yang diperlukan untuk membuat AMI Amazon Linux 2023 yang Dapat Dibuktikan untuk lingkungan komputasi terisolasi dengan `erofs` sistem file hanya-baca.

Anda dapat menyertakan paket perangkat lunak tambahan dalam deskripsi gambar dengan menambahkannya ke `<packages>` elemen dalam deskripsi gambar. `<packages>`Elemen mendefinisikan semua perangkat lunak yang harus diinstal ke dalam AMI.

Anda juga dapat menggunakan `<packages>` elemen untuk menghapus atau menghapus paket perangkat lunak tertentu.

Untuk informasi selengkapnya tentang menambahkan atau menghapus paket dalam deskripsi gambar, lihat Menambahkan dan Menghapus Paket.

Menambahkan file dan direktori

Deskripsi gambar sampel mencakup direktori pohon overlay (`/root/`). Direktori pohon overlay adalah direktori yang berisi file dan direktori yang akan disalin ke dalam gambar selama proses pembuatan gambar. File dan direktori apa pun yang Anda tempatkan ke direktori pohon overlay akan disalin langsung ke sistem file root gambar selama proses pembuatan gambar.

Direktori pohon overlay disalin ke dalam gambar setelah semua paket diinstal. File baru ditambahkan dan file yang ada ditimpa.

Menambahkan skrip kustom

Deskripsi gambar sampel mencakup skrip kustom tunggal,`edit_boot_install.sh`. Skrip ini mencakup perintah yang diperlukan untuk menjalankan `nitro-tpm-pcr-compute` utilitas, yang menghasilkan pengukuran referensi berdasarkan konten gambar. Skrip ini dipanggil segera setelah bootloader diinstal.

Jika diperlukan, Anda dapat menyertakan skrip kustom Anda sendiri dalam deskripsi gambar untuk melakukan tugas atau konfigurasi selama proses pembuatan gambar atau pada boot pertama gambar. Menggunakan skrip memungkinkan Anda untuk menyesuaikan gambar Anda dengan cara yang tidak dapat dicapai dengan menggunakan deskripsi gambar saja.

Untuk menyertakan skrip kustom dalam deskripsi gambar Anda, Anda perlu menamainya dengan benar berdasarkan jenis skrip, dan menambahkannya ke direktori yang sama dengan `appliance.kiwi` file. KIWI NG secara otomatis mendeteksi dan mengeksekusi skrip jika

diberi nama dengan benar dan ditempatkan di lokasi yang benar, tanpa perlu secara eksplisit mereferensikannya dalam file deskripsi gambar.

Untuk informasi selengkapnya tentang skrip yang didukung oleh KIWI NG, lihat Skrip yang Ditetapkan Pengguna.

Hitung pengukuran PCR untuk AMI khusus

`nitro-tpm-pcr-compute`Utilitas ini memungkinkan Anda menghasilkan pengukuran referensi untuk AMI yang Dapat Dibuktikan selama waktu pembuatan berdasarkan Unified Kernel Image (UKI).

Contoh deskripsi gambar Amazon Linux 2023 secara otomatis menginstal utilitas pada gambar bawaan di `/usr/bin/` direktori. Deskripsi gambar sampel juga menyertakan skrip dengan perintah yang diperlukan untuk menjalankan utilitas untuk menghasilkan pengukuran referensi selama waktu pembuatan gambar. Jika Anda menggunakan deskripsi gambar sampel, Anda tidak perlu menginstal utilitas atau menjalankannya secara manual. Untuk informasi selengkapnya, lihat Buat contoh deskripsi gambar Amazon Linux 2023.

Instal **`nitro-tpm-pcr-compute`** utilitas

Jika Anda menggunakan Amazon Linux 2023, Anda dapat menginstal `nitro-tpm-pcr-compute` utilitas dari repositori Amazon Linux sebagai berikut.

```
sudo yum install aws-nitro-tpm-tools
```

Alat-alat dipasang di `/usr/bin` direktori.

Gunakan **`nitro-tpm-pcr-compute`** utilitas

Utilitas menyediakan satu perintah,`nitro-tpm-pcr-compute`, untuk menghasilkan pengukuran referensi.

Ketika Anda menjalankan perintah, Anda harus menentukan yang berikut:

- Unified kernel image (`UKI.efi`) - Diperlukan untuk boot Standar dan UEFI.

Untuk menghasilkan pengukuran referensi untuk AMI yang Dapat Dibuktikan:

Gunakan perintah dan parameter berikut:

```
/usr/bin/nitro-tpm-pcr-compute \
```

```
--image UKI.efi
```

Utilitas mengembalikan pengukuran referensi dalam format JSON berikut:

```
{
  "Measurements": {
    "HashAlgorithm": "SHA384 { ... }",
    "PCR4": "PCR4_measurement",
    "PCR7": "PCR7_measurement",
    "PCR12": "PCR12_measurement"
  }
}
```

Untuk contoh praktis tentang cara menggunakan `nitro-tpm-pcr-compute` utilitas, lihat `edit_boot_install.sh` skrip yang disertakan dalam contoh deskripsi gambar Amazon Linux 2023.

Bersiaplah AWS KMS untuk pengesahan

> **Note**
>
> Jika Anda membuktikan layanan pihak ketiga, Anda harus membangun mekanisme kustom Anda sendiri untuk menerima, mengurai, dan memvalidasi Dokumen Pengesahan. Untuk informasi selengkapnya, lihat Validasi Dokumen Pengesahan NitroTPM.

Setelah membuat AMI Attestable, Anda harus memiliki pengukuran referensi yang dapat Anda gunakan untuk memvalidasi permintaan dari instans Amazon EC2. AWS KMS menyediakan dukungan bawaan untuk pengesahan dengan NitroTPM.

Untuk AWS KMS kunci yang Anda gunakan untuk mengenkripsi data rahasia, tambahkan kebijakan kunci yang mengizinkan akses kunci hanya jika permintaan API menyertakan Dokumen Pengesahan dengan pengukuran yang sesuai dengan pengukuran referensi yang Anda buat selama proses pembuatan AMI yang Dapat Dibuktikan. Penggunaan PCR4 dan PCR12 pengukuran untuk boot standar atau PCR7 pengukuran untuk Boot Aman. Ini memastikan bahwa hanya permintaan dari instance yang diluncurkan menggunakan AMI Attestable yang dapat melakukan operasi kriptografi menggunakan kunci. AWS KMS

AWS KMS menyediakan`kms:RecipientAttestation:NitroTPMPCR4`,`kms:RecipientAttestation:NitroTPM`

dan kunci `kms:RecipientAttestation:NitroTPMPCR12` kondisi yang memungkinkan Anda membuat kondisi berbasis pengesahan untuk kebijakan kunci NitroTPM KMS. Untuk informasi selengkapnya, lihat Kunci kondisi untuk NitroTPM.

Misalnya, kebijakan AWS KMS kunci berikut mengizinkan akses kunci hanya jika permintaan berasal dari instance dengan profil `MyEC2InstanceRole` instance terlampir, dan jika permintaan tersebut menyertakan Dokumen Pengesahan dengan nilai PCR 4 dan PCR 12 tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow requests from instances with attested AMI only",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyEC2InstanceRole"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateRandom"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {

 "kms:RecipientAttestation:NitroTPMPCR4":"EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde4

 "kms:RecipientAttestation:NitroTPMPCR12":"000000000000000000000000000000000000000000000000000000
        }
      }
    }
  ]
}
```

Dapatkan Dokumen Pengesahan NitroTPM

Dokumen Pengesahan adalah komponen kunci dari proses pengesahan NitroTPM. Ini berisi serangkaian pengukuran kriptografi yang dapat digunakan untuk memverifikasi identitas instance dan untuk membuktikan bahwa itu hanya menjalankan perangkat lunak tepercaya. Anda dapat menggunakan Dokumen Pengesahan dengan AWS KMS, yang menyediakan dukungan bawaan

untuk pengesahan NitroTPM, atau untuk membangun mekanisme pengesahan kriptografi Anda sendiri.

`nitro-tpm-attest`Utilitas ini memungkinkan Anda untuk mengambil Dokumen Pengesahan NitroTPM yang ditandatangani untuk instans Amazon EC2 selama runtime.

Contoh deskripsi gambar Amazon Linux 2023 secara otomatis menginstal utilitas pada gambar bawaan di `/usr/bin/` direktori. Ini memastikan bahwa utilitas sudah diinstal sebelumnya pada instance yang diluncurkan menggunakan AMI. Anda tidak perlu menginstal utilitas secara manual. Untuk informasi selengkapnya, lihat Buat contoh deskripsi gambar Amazon Linux 2023.

Topik

- Instal nitro-tpm-attest utilitas
- Gunakan nitro-tpm-attest utilitas
- Isi Dokumen Pengesahan NitroTPM
- Validasi Dokumen Pengesahan NitroTPM

Instal **`nitro-tpm-attest`** utilitas

Jika Anda menggunakan Amazon Linux 2023, Anda dapat menginstal `nitro-tpm-attest` utilitas dari repositori Amazon Linux sebagai berikut.

```
sudo yum install aws-nitro-tpm-tools
```

Gunakan **`nitro-tpm-attest`** utilitas

Utilitas menyediakan satu perintah,`nitro-tpm-attest`, untuk mengambil Dokumen Pengesahan. Perintah mengembalikan Dokumen Pengesahan yang dikodekan dalam Representasi Objek Biner Ringkas (CBOR) dan ditandatangani menggunakan CBOR Object Signing and Encryption (COSE).

Saat Anda menjalankan perintah, Anda dapat menentukan parameter opsional berikut:

- `public-key`Kunci publik yang dapat digunakan oleh AWS KMS atau layanan eksternal untuk mengenkripsi data respons sebelum dikembalikan. Ini memastikan bahwa hanya penerima yang dituju, yang memiliki kunci pribadi, yang dapat mendekripsi data. Misalnya, jika Anda membuktikan AWS KMS, layanan mengenkripsi data plaintext dengan kunci publik di Dokumen Pengesahan, dan mengembalikan ciphertext yang dihasilkan di bidang dalam respons. `CiphertextForRecipient` Hanya kunci RSA yang didukung.

- `user-data`Data pengguna dapat digunakan untuk mengirimkan data tambahan yang ditandatangani ke layanan eksternal. Data pengguna ini dapat digunakan untuk melengkapi protokol yang disepakati antara instance yang meminta dan layanan eksternal. Tidak digunakan untuk pengesahan dengan. AWS KMS
- `nonce`Nonce dapat digunakan untuk mengatur otentikasi tantangan-respons antara instance dan layanan eksternal untuk membantu mencegah serangan peniruan identitas. Menggunakan nonce memungkinkan layanan eksternal untuk memverifikasi bahwa itu berinteraksi dengan instance langsung dan bukan peniru yang menggunakan kembali Dokumen Pengesahan lama. Tidak digunakan untuk pengesahan dengan. AWS KMS

Untuk mengambil Dokumen Pengesahan

Gunakan perintah berikut dan parameter opsional:

```
/usr/bin/nitro-tpm-attest \
--public-key rsa_public_key \
--user-data user_data \
--nonce nonce
```

Untuk contoh lengkap yang menunjukkan cara membuat key pair RSA, dan cara meminta pengesahan dengan kunci publik, lihat repo. nitro-tpm-attest GitHub

Isi Dokumen Pengesahan NitroTPM

Dokumen Pengesahan dihasilkan oleh NitroTPM dan ditandatangani oleh Nitro Hypervisor. Ini mencakup serangkaian nilai register konfigurasi platform (PCR) yang terkait dengan instans Amazon EC2. PCRs Berikut ini termasuk dalam Dokumen Pengesahan:

> **Important**
>
> PCR0 dan PCR1 umumnya digunakan untuk mengukur kode boot awal, yang dikendalikan oleh AWS. Untuk memungkinkan pembaruan aman kode boot awal, ini PCRs akan selalu berisi nilai konstan.

- `PCR0`— Kode yang Dapat Dieksekusi Firmware Sistem Inti
- `PCR1`— Data Firmware Sistem Inti

- PCR2— Kode eksekusi yang diperluas atau dapat dicolokkan
- PCR3— Data Firmware yang Diperpanjang atau dapat dicolokkan
- PCR4— Kode Manajer Boot
- PCR5— Konfigurasi Kode Boot Manager dan Data dan Tabel Partisi GPT
- PCR6- Spesifikasi Produsen Platform Host
- PCR7— Kebijakan Boot Aman
- PCR8 - 15— Didefinisikan untuk digunakan oleh Sistem Operasi Statis
- PCR16— Debug
- PCR23— Support Aplikasi

PCR4, PCR7, dan PCR12secara khusus digunakan untuk memvalidasi bahwa sebuah instance diluncurkan menggunakan AMI Attestable. PCR4 dan PCR12 dapat digunakan untuk memvalidasi dengan boot standar, dan PCR7 dapat digunakan untuk memvalidasi dengan Boot Aman.

- PCR4 (Boot Manager Code) — Ketika sebuah instance dimulai, NitroTPM membuat hash kriptografi dari semua binari yang dieksekusi oleh lingkungan UEFI-nya. Dengan Attestable AMIs, binari boot ini menyematkan hash yang mencegah pemuatan binari di masa mendatang yang tidak memiliki hash yang cocok. Dengan cara ini, hash biner boot tunggal dapat menggambarkan dengan tepat kode apa yang akan dijalankan oleh sebuah instance.
- PCR7 (Secure Boot Policy) — Binari boot UEFI dapat ditandatangani dengan kunci penandatanganan UEFI Secure Boot. Ketika UEFI Secure Boot diaktifkan, UEFI akan mencegah eksekusi binari boot UEFI yang tidak sesuai dengan kebijakan yang dikonfigurasi. PCR7 berisi hash dari kebijakan UEFI Secure Boot instance.

  Jika Anda perlu mempertahankan satu kebijakan KMS yang tetap ada di seluruh pembaruan instans, Anda dapat membuat kebijakan yang memvalidasi PCR7 untuk memvalidasi sertifikat Boot Aman UEFI. Selama pembuatan AMI yang Dapat Dibuktikan, Anda kemudian dapat menandatangani biner boot dengan sertifikat Anda dan menginstalnya sebagai satu-satunya sertifikat yang diizinkan dalam data UEFI AMI. Perlu diingat bahwa model ini mengharuskan Anda untuk tetap membuat sertifikat baru, menginstalnya di kebijakan Anda dan memperbarui AMIs jika Anda ingin mencegah instance yang diluncurkan dari yang lama (tidak tepercaya) AMIs agar tidak meneruskan kebijakan KMS Anda.
- PCR12— Berisi hash dari baris perintah yang diteruskan ke biner boot UEFI. Diperlukan dalam hubungannya dengan PCR4 untuk boot standar untuk memvalidasi baris perintah tidak dimodifikasi.

Validasi Dokumen Pengesahan NitroTPM

> **Note**
>
> Topik ini ditujukan untuk pengguna yang menggunakan layanan manajemen kunci pihak ketiga, dan perlu membangun mekanisme validasi Dokumen Pengesahan mereka sendiri.

Topik ini memberikan gambaran rinci tentang seluruh alur pengesahan NitroTPM. Ini juga membahas apa yang dihasilkan oleh sistem AWS Nitro ketika Dokumen Pengesahan diminta, dan menjelaskan bagaimana layanan manajemen kunci harus memproses Dokumen Pengesahan.

Topik

- Dokumen Pengesahan
- Pengesahan Validasi dokumen

Tujuan pengesahan adalah untuk membuktikan bahwa sebuah instance adalah entitas yang dapat dipercaya, berdasarkan kode dan konfigurasi yang dijalankannya. Akar kepercayaan untuk instance berada dalam sistem AWS Nitro, yang menyediakan Dokumen Pengesahan.

Dokumen Pengesahan ditandatangani oleh AWS Nitro Attestation Public Key Infrastructure (PKI), yang mencakup otoritas sertifikat yang diterbitkan yang dapat dimasukkan ke dalam layanan apa pun.

Dokumen Pengesahan

Dokumen Pengesahan dikodekan dalam Representasi Objek Biner Ringkas (CBOR), dan ditandatangani menggunakan CBOR Object Signing and Encryption (COSE).

Untuk informasi lebih lanjut tentang CBOR, lihat RFC 8949: Representasi Objek Biner Ringkas (CBOR).

Spesifikasi Dokumen Pengesahan

Berikut ini menunjukkan struktur Dokumen Pengesahan.

```
AttestationDocument = {
    module_id: text,                    ; issuing Nitro hypervisor module ID
    timestamp: uint .size 8,            ; UTC time when document was created, in
                                        ; milliseconds since UNIX epoch
```

```
    digest: digest,                     ; the digest function used for calculating the
                                        ; register values
    nitrotpm_pcrs: { + index => pcr },  ; map of PCRs at the moment the Attestation
 Document was generated
    certificate: cert,                  ; the public key certificate for the public
 key
                                        ; that was used to sign the Attestation
 Document
    cabundle: [* cert],                 ; issuing CA bundle for infrastructure
 certificate
    ? public_key: user_data,            ; an optional DER-encoded key the attestation
                                        ; consumer can use to encrypt data with
    ? user_data: user_data,             ; additional signed user data, defined by
 protocol
    ? nonce: user_data,                 ; an optional cryptographic nonce provided by
 the
                                        ; attestation consumer as a proof of
 authenticity
}

cert = bytes .size (1..1024)       ; DER encoded certificate
user_data = bytes .size (0..1024)
pcr = bytes .size (32/48/64)       ; PCR content
index = 0..31
digest = "SHA384"
```

Parameter opsional dalam Dokumen Pengesahan (`public_key`,`user_data`, dan`nonce`) dapat digunakan untuk membuat protokol validasi kustom antara instance pembuktian dan layanan eksternal.

Pengesahan Validasi dokumen

Saat Anda meminta Dokumen Pengesahan dari Nitro Hypervisor, Anda menerima gumpalan biner yang berisi Dokumen Pengesahan yang ditandatangani. Dokumen Pengesahan yang ditandatangani adalah objek CBOR-encoded, Cose-signed (menggunakan struktur tanda tangan Cose_sign1). Proses validasi keseluruhan mencakup langkah-langkah berikut:

1. Dekode objek CBOR dan petakan ke struktur COSE_SIGN1.
2. Ekstrak Dokumen Pengesahan dari struktur Cose_sign1.
3. Verifikasi rantai sertifikat.
4. Pastikan bahwa Dokumen Pengesahan ditandatangani dengan benar.

Dokumen Pengesahan ditandatangani oleh AWS Nitro Attestation PKI, yang mencakup sertifikat root untuk partisi komersial. AWS Sertifikat root dapat diunduh https://aws-nitro-enclaves.amazonaws.comdari/ AWS_N itroEnclaves_Root-G1.zip, dan dapat diverifikasi menggunakan sidik jari berikut.

```
64:1A:03:21:A3:E2:44:EF:E4:56:46:31:95:D6:06:31:7E:D7:CD:CC:3C:17:56:E0:98:93:F3:C6:8F:79:BB:5B
```

Sertifikat root didasarkan pada AWS Certificate Manager Private Certificate Authority (AWS Private CA) kunci pribadi dan memiliki masa pakai 30 tahun. Subjek PCA memiliki format berikut.

```
CN=aws.nitro-enclaves, C=US, O=Amazon, OU=AWS
```

Topik

- COSE dan CBOR
- Validitas semantik
- Validitas sertifikat
- Validitas rantai sertifikat

COSE dan CBOR

Biasanya, struktur tanda tangan Cose_sign1 digunakan ketika hanya satu tanda tangan yang akan ditempatkan pada pesan. Parameter yang berhubungan dengan konten dan tanda tangan ditempatkan di header yang dilindungi daripada memiliki pemisahan Cose_sign. Struktur dapat dikodekan sebagai tag atau untagged, tergantung pada konteks yang akan digunakan. Struktur Cose_sign1 yang ditandai diidentifikasi oleh tag CBOR 18.

Objek CBOR yang membawa tubuh, tanda tangan, dan informasi tentang tubuh dan tanda tangan disebut struktur COSE_sign1. Struktur Cose_sign1 adalah array CBOR. Array mencakup bidang-bidang berikut.

```
[
  protected:   Header,
  unprotected: Header,
  payload:     This field contains the serialized content to be signed,
  signature:   This field contains the computed signature value.
]
```

Dalam konteks Dokumen Pengesahan, array mencakup yang berikut ini.

```
18(/* COSE_Sign1 CBOR tag is 18 */
    {1: -35}, /* This is equivalent with {algorithm: ECDS 384} */
    {}, /* We have nothing in unprotected */
    $ATTESTATION_DOCUMENT_CONTENT /* Attestation Document */,
    signature /* This is the signature */
)
```

Untuk informasi lebih lanjut tentang CBOR, lihat RFC 8949: Representasi Objek Biner Ringkas (CBOR).

Validitas semantik

Dokumen Pengesahan akan selalu memiliki bundel CA mereka dalam urutan berikut.

```
[ ROOT_CERT - INTERM_1 - INTERM_2 .... - INTERM_N]
      0          1          2             N - 1
```

Ingatlah urutan ini, karena beberapa alat yang ada, seperti Java CertPath dari Java PKI API Programmer's Guide, mungkin mengharuskan mereka untuk dipesan secara berbeda.

Untuk memvalidasi sertifikat, mulai dari bundel CA Dokumen Pengesahan dan buat rantai yang diperlukan, Di mana `TARGET_CERT` sertifikat dalam Dokumen Pengesahan.

```
[TARGET_CERT, INTERM_N, ..... , INTERM_2, INTERM_1, ROOT_CERT]
```

Validitas sertifikat

Untuk semua sertifikat dalam rantai, Anda harus memastikan bahwa tanggal saat ini termasuk dalam periode validitas yang ditentukan dalam sertifikat.

Validitas rantai sertifikat

Secara umum, rantai beberapa sertifikat mungkin diperlukan, yang terdiri dari sertifikat pemilik kunci publik yang ditandatangani oleh satu CA, dan nol atau lebih sertifikat tambahan yang CAs ditandatangani oleh yang lain CAs. Rantai semacam itu, yang disebut jalur sertifikasi, diperlukan karena pengguna kunci publik hanya diinisialisasi dengan sejumlah kunci publik CA yang terjamin. Prosedur validasi jalur sertifikasi untuk PKI internet didasarkan pada algoritma yang disediakan dalam X.509. Pemrosesan jalur sertifikasi memverifikasi pengikatan antara nama subjek yang dibedakan nama alternatif and/or subjek dan kunci publik subjek. Pengikatan dibatasi oleh kendala yang ditentukan dalam sertifikat yang terdiri dari jalur dan input yang ditentukan oleh pihak yang

mengandalkan. Kendala dasar dan ekstensi kendala kebijakan memungkinkan logika pemrosesan jalur sertifikasi untuk mengotomatiskan proses pengambilan keputusan.

> **Note**
>
> CRL harus dinonaktifkan saat melakukan validasi.

Menggunakan Java, mulai dari jalur root dan rantai sertifikat yang dihasilkan, validasi rantai adalah sebagai berikut.

```
validateCertsPath(certChain, rootCertficate) {
    /* The trust anchor is the root CA to trust */
    trustAnchors.add(rootCertificate);

    /* We need PKIX parameters to specify the trust anchors
     * and disable the CRL validation
     */
    validationParameters = new PKIXParameters(trustAnchors);
    certPathValidator = CertPathValidator.getInstance(PKIX);
    validationParameters.setRevocationEnabled(false);

    /* We are ensuring that certificates are chained correctly */
    certPathValidator.validate(certPath, validationParameters);
}
```

Integrasi dengan AWS KMS

Instance Anda harus memiliki aplikasi yang dapat membuat permintaan AWS KMS API dengan Dokumen Pengesahan yang diambil dari NitRotPM. Saat Anda membuat permintaan dengan Dokumen AWS KMS Pengesahan, validasi pengukuran dalam Dokumen Pengesahan yang disediakan terhadap pengukuran referensi dalam kebijakan kunci KMS. Permintaan hanya diperbolehkan jika pengukuran dalam Dokumen Pengesahan cocok dengan pengukuran referensi dalam kebijakan kunci KMS.

Saat Anda memanggil operasi Dekripsi,, DeriveSharedSecret, GenerateDataKey, GenerateDataKeyPair, atau GenerateRandomAPI dengan Dokumen Pengesahan, ini APIs mengenkripsi plaintext dalam respons di bawah kunci publik dari Dokumen Pengesahan, dan mengembalikan ciphertext alih-alih teks biasa. Ciphertext ini dapat didekripsi hanya dengan menggunakan kunci pribadi yang cocok yang dihasilkan dalam instance.

Untuk informasi lebih lanjut, lihat pengesahan Kriptografi untuk NitroTPM di Panduan Pengembang.AWS Key Management Service

> **Note**
>
> Jika Anda membuktikan layanan pihak ketiga, Anda harus membangun mekanisme kustom Anda sendiri untuk menerima, mengurai, dan memvalidasi Dokumen Pengesahan. Untuk informasi selengkapnya, lihat Validasi Dokumen Pengesahan NitroTPM.

Mengisolasi data dari operator Anda sendiri

Sistem AWS Nitro tidak memiliki akses operator. Tidak ada mekanisme bagi AWS sistem atau orang mana pun untuk masuk ke host Amazon EC2 Nitro, mengakses memori instans EC2, atau mengakses data pelanggan apa pun yang disimpan di penyimpanan instans terenkripsi lokal atau volume Amazon EBS terenkripsi jarak jauh.

Saat memproses data yang sangat sensitif, Anda dapat mempertimbangkan untuk membatasi akses ke data tersebut dengan mencegah operator Anda sendiri mengakses instans EC2.

Anda dapat membuat Attestable kustom AMIs yang dikonfigurasi untuk menyediakan lingkungan komputasi yang terisolasi. Konfigurasi AMI tergantung pada beban kerja dan persyaratan aplikasi Anda. Pertimbangkan praktik terbaik ini saat membangun AMI Anda untuk menciptakan lingkungan komputasi yang terisolasi.

- Hapus semua akses interaktif untuk mencegah operator atau pengguna mengakses instans.
- Pastikan bahwa hanya perangkat lunak dan kode tepercaya yang disertakan dalam AMI.
- Konfigurasikan firewall jaringan dalam instance untuk memblokir akses.
- Pastikan status hanya-baca dan tidak dapat diubah untuk semua penyimpanan dan sistem file.
- Batasi akses instans ke panggilan API yang diautentikasi, diotorisasi, dan dicatat.

Memperbarui Attestable AMIs yang tidak memiliki akses interaktif

Setelah Anda meluncurkan instance menggunakan lingkungan komputasi terisolasi AMI, tidak ada cara bagi pengguna atau operator mana pun untuk terhubung ke instance. Ini berarti bahwa tidak ada cara untuk menginstal atau memperbarui perangkat lunak apa pun pada instance setelah peluncuran.

Jika perangkat lunak baru atau pembaruan perangkat lunak diperlukan, Anda harus membuat AMI Attestable baru yang menyertakan pembaruan perangkat lunak atau perangkat lunak yang diperlukan. Kemudian, gunakan AMI itu untuk meluncurkan instance baru, atau untuk melakukan penggantian volume root pada instance asli. Setiap perubahan perangkat lunak yang dilakukan pada AMI akan menghasilkan hash baru yang dihasilkan.

Tindakan berikut akan menghasilkan perubahan pada pengukuran referensi dalam Dokumen Pengesahan NitroTPM:

- Menghentikan dan memulai instance yang diluncurkan dengan AMI yang Dapat Dibuktikan
- Melakukan penggantian volume root dengan AMI yang berbeda

Jika Anda melakukan salah satu tindakan ini, Anda kemudian harus memperbarui layanan pengesahan Anda dengan pengukuran referensi baru. Misalnya, Anda harus memperbarui kebijakan kunci KMS Anda ke pengukuran referensi baru jika Anda menggunakannya AWS KMS untuk pengesahan.

Instance mempertahankan materi kunci NitroTPM untuk seluruh siklus hidup instance, dan bertahan melalui stop/starts operasi penggantian volume root.

Credential Guard untuk instance Windows

Sistem AWS Nitro mendukung Credential Guard untuk instans Windows Amazon Elastic Compute Cloud (Amazon EC2). Credential Guard adalah fitur keamanan berbasis virtualisasi (VBS) Windows yang memungkinkan pembuatan lingkungan yang terisolasi untuk melindungi aset keamanan, seperti kredensial pengguna Windows dan pemberlakuan integritas kode, di luar perlindungan kernel Windows. Ketika Anda menjalankan instans EC2 Windows, Credential Guard menggunakan Sistem AWS Nitro untuk melindungi kredensi login Windows agar tidak diekstraksi dari memori sistem operasi.

Daftar Isi

- Prasyarat
- Luncurkan instance yang didukung
- Nonaktifkan integritas memori
- Aktifkan Credential Guard
- Verifikasi bahwa Credential Guard sedang berjalan

Prasyarat

Instans Windows Anda harus memenuhi persyaratan berikut untuk menggunakan Credential Guard.

Gambar Mesin Amazon (AMIs)

AMI harus dikonfigurasikan sebelumnya untuk mengaktifkan Secure Boot NitroTPM dan UEFI. Untuk informasi selengkapnya tentang dukungan AMIs, lihatthe section called “Persyaratan”.

Integritas memori

Integritas memori, juga dikenal sebagai integritas kode yang dilindungi hypervisor (HVCI) atau integritas kode yang diberlakukan hypervisor, tidak didukung. Sebelum Anda mengaktifkan Credential Guard, Anda harus memastikan fitur ini dinonaktifkan. Untuk informasi selengkapnya, lihat Nonaktifkan integritas memori.

Tipe instans

Jenis contoh berikut mendukung Credential Guard di semua ukuran kecuali disebutkan lain:`C5`,`C5d`,`C5n`,`C6i`,`C6id`,`C6in`,`C7i`,,`C7i-flex`,`M5`,`M5d`,`M5dn`,`M5n`,`M5zn`,`M6i`,`M6id`,`M6idn`,`M6in`,`M7i`,`M7i-flex`,`R5`,`R5b`,`R5d`,,`R5dn`,`R5n`,`R6i`,`R6id`,`R6idn`, `R6in` `R7iR7iz`,`T3`.

> **Note**
>
> - Meskipun NitRotPM memiliki beberapa jenis instance wajib yang sama, tipe instance harus menjadi salah satu tipe instance sebelumnya untuk mendukung Credential Guard.
> - Credential Guard tidak didukung untuk:
>   - Contoh logam telanjang.
>   - Jenis contoh berikut:`C7i.48xlarge`,`M7i.48xlarge`, dan`R7i.48xlarge`.

Untuk informasi selengkapnya tentang jenis instans, lihat Panduan Jenis Instans Amazon EC2.

Luncurkan instance yang didukung

Anda dapat menggunakan konsol Amazon EC2 atau AWS Command Line Interface (AWS CLI) untuk meluncurkan instance yang dapat mendukung Credential Guard. Anda akan memerlukan ID AMI yang kompatibel untuk meluncurkan instans Anda yang unik untuk setiap AWS Region.

> **Tip**
>
> Anda dapat menggunakan tautan berikut untuk menemukan dan meluncurkan instans dengan AMI yang disediakan Amazon yang kompatibel di konsol Amazon EC2: https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Console

Untuk meluncurkan sebuah instans

Ikuti langkah-langkah untuk meluncurkan instance, menentukan jenis instans yang didukung dan AMI Windows yang telah dikonfigurasi sebelumnya.

AWS CLI

Untuk meluncurkan sebuah instans

Gunakan perintah run-instances untuk meluncurkan instans menggunakan tipe instans yang didukung dan AMI Windows yang telah dikonfigurasi sebelumnya.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
    --subnet-id subnet-0abcdef1234567890
    --key-name key-name
```

PowerShell

Untuk meluncurkan sebuah instans

Gunakan perintah New-EC2Instance untuk meluncurkan instans menggunakan tipe instans yang didukung dan AMI Windows yang telah dikonfigurasi sebelumnya.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base `
    -InstanceType c6i.large `
```

```
    -Region us-east-1 `
    -SubnetId subnet-0abcdef1234567890 `
    -KeyName key-name
```

Nonaktifkan integritas memori

Anda dapat menggunakan Editor Kebijakan Grup Lokal untuk menonaktifkan integritas memori dalam skenario yang didukung. Panduan berikut dapat diterapkan untuk setiap pengaturan konfigurasi di bawah Virtualization Based Protection of Code Integrity:

- Diaktifkan tanpa kunci – Ubah pengaturan ke Dinonaktifkan untuk menonaktifkan integritas memori.
- Diaktifkan dengan kunci UEFI – Integritas memori telah diaktifkan dengan kunci UEFI. Integritas memori tidak dapat dinonaktifkan setelah diaktifkan dengan kunci UEFI. Sebaiknya buat instans baru dengan integritas memori dinonaktifkan dan menghentikan instans yang tidak didukung jika tidak digunakan.

Untuk menonaktifkan integritas memori dengan Editor Kebijakan Grup Lokal

1. Terhubung ke instans Anda sebagai akun pengguna dengan hak akses administrator menggunakan Protokol Desktop Jarak Jauh (RDP). Untuk informasi selengkapnya, lihat the section called “Connect menggunakan klien RDP”.
2. Buka menu Mulai dan cari **`cmd`** untuk memulai prompt perintah.
3. Jalankan perintah berikut untuk membuka Editor Kebijakan Grup Lokal: `gpedit.msc`
4. Di Editor Kebijakan Grup Lokal, pilih Konfigurasi Komputer, Templat Administratif, Sistem, Penjaga Perangkat.
5. Pilih Aktifkan Keamanan Berbasis Virtualisasi, lalu pilih Edit pengaturan kebijakan.
6. Buka drop-down pengaturan untuk Perlindungan Integritas Kode Berbasis Virtualisasi, pilih Nonaktifkan, lalu pilih Terapkan.
7. Boot ulang instans untuk menerapkan perubahan.

Aktifkan Credential Guard

Setelah meluncurkan instans Windows dengan tipe instans yang didukung dan AMI yang kompatibel dan mengonfirmasi bahwa integritas memori dinonaktifkan, Anda dapat mengaktifkan Credential Guard.

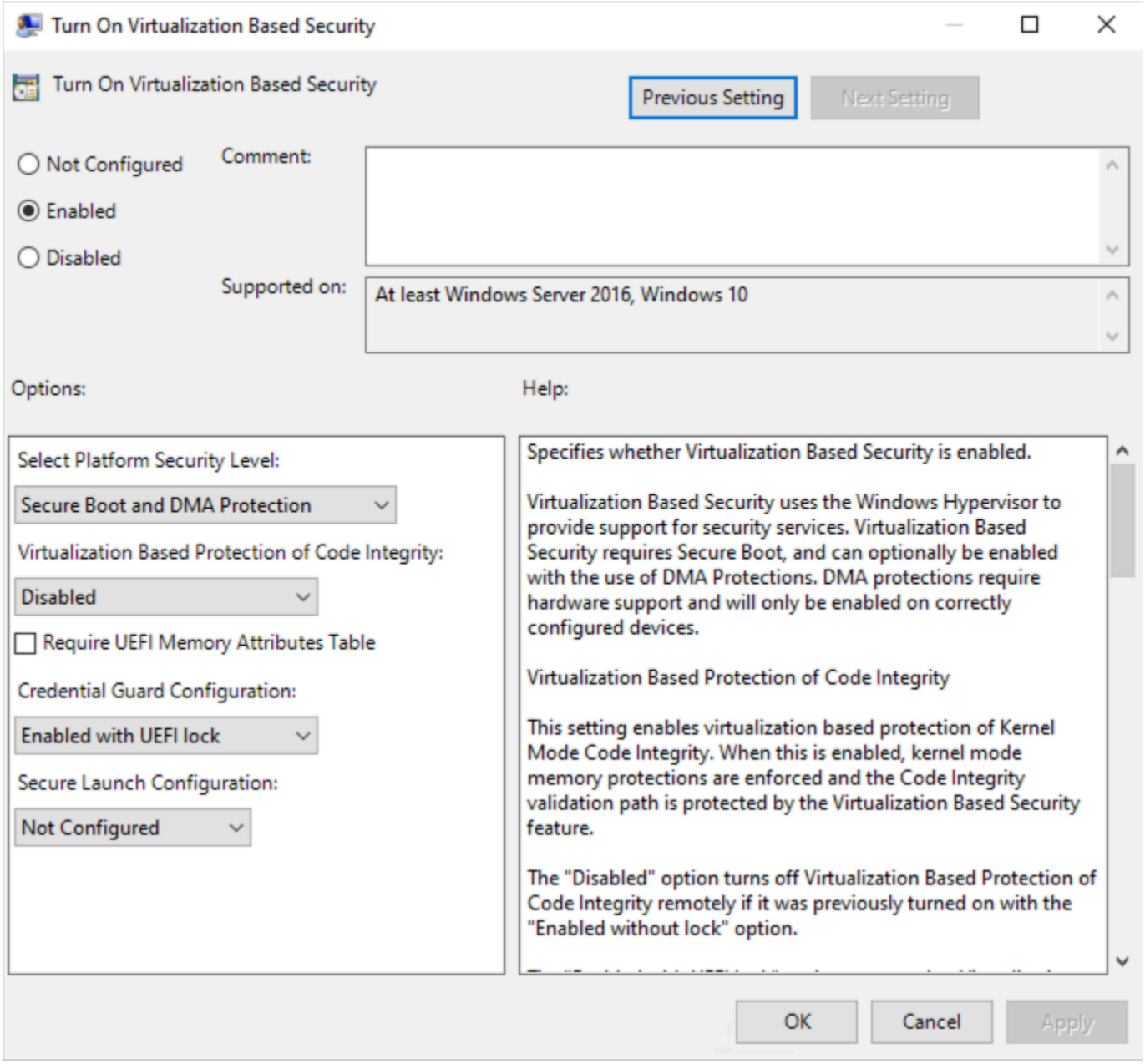
> **Important**
>
> Hak akses administrator diperlukan untuk melakukan langkah-langkah berikut guna mengaktifkan Credential Guard.

Mengaktifkan Credential Guard

1. Terhubung ke instans Anda sebagai akun pengguna dengan hak akses administrator menggunakan Protokol Desktop Jarak Jauh (RDP). Untuk informasi selengkapnya, lihat the section called “Connect menggunakan klien RDP”.
2. Buka menu Mulai dan cari **`cmd`** untuk memulai prompt perintah.
3. Jalankan perintah berikut untuk membuka Editor Kebijakan Grup Lokal: `gpedit.msc`
4. Di Editor Kebijakan Grup Lokal, pilih Konfigurasi Komputer, Templat Administratif, Sistem, Penjaga Perangkat.
5. Pilih Aktifkan Keamanan Berbasis Virtualisasi, lalu pilih Edit pengaturan kebijakan.
6. Pilih Diaktifkan dalam menu Aktifkan Keamanan Berbasis Virtualisasi.
7. Untuk Pilih Tingkat Keamanan Platform, pilih Secure Boot dan Perlindungan DMA.
8. Untuk Konfigurasi Credential Guard, pilih Diaktifkan dengan kunci UEFI.

   > **Note**
   >
   > Pengaturan kebijakan yang tersisa tidak diperlukan untuk mengaktifkan Credential Guard dan dapat dibiarkan sebagai Tidak Dikonfigurasikan.

   Gambar berikut menampilkan pengaturan VBS yang dikonfigurasikan seperti yang dijelaskan sebelumnya:



9. Boot ulang instans untuk menerapkan pengaturan.

Verifikasi bahwa Credential Guard sedang berjalan

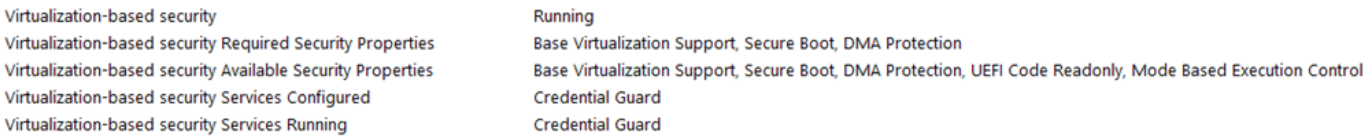
Anda dapat menggunakan alat Informasi Sistem Microsoft (`Msinfo32.exe`) untuk mengonfirmasi bahwa Credential Guard sedang berjalan.

> **Important**
>
> Anda harus melakukan boot ulang instans terlebih dahulu untuk menyelesaikan penerapan pengaturan kebijakan yang diperlukan untuk mengaktifkan Credential Guard.

Untuk memverifikasi bahwa Credential Guard sedang berjalan

1. Hubungkan ke instans Anda menggunakan Protokol Desktop Jarak Jauh (RDP). Untuk informasi selengkapnya, lihat the section called “Connect menggunakan klien RDP”.
2. Dalam sesi RDP ke instans Anda, buka menu Mulai dan cari **`cmd`** untuk memulai prompt perintah.
3. Buka Informasi Sistem dengan menjalankan perintah berikut: `msinfo32.exe`
4. Alat Informasi Sistem Microsoft mencantumkan detail untuk konfigurasi VBS. Di samping Layanan keamanan berbasis Virtualisasi, konfirmasi bahwa Credential Guard muncul sebagai Berjalan.

   Gambar berikut menampilkan VBS berjalan seperti yang dijelaskan sebelumnya:



Mengakses Amazon EC2 menggunakan titik akhir VPC antarmuka

Anda dapat meningkatkan postur keamanan VPC Anda dengan membuat koneksi pribadi antara sumber daya di VPC Anda dan Amazon EC2 API. Anda dapat mengakses Amazon EC2 API seolah-olah berada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. Direct Connect Instans EC2 di VPC Anda tidak memerlukan alamat IP publik untuk mengakses Amazon EC2 API.

Untuk informasi selengkapnya, lihat Akses Layanan AWS melalui AWS PrivateLink di AWS PrivateLink Panduan.

Daftar Isi

- Membuat titik akhir VPC antarmuka
- Membuat kebijakan titik akhir

Membuat titik akhir VPC antarmuka

Buatlah titik akhir antarmuka untuk Amazon EC2 menggunakan nama layanan berikut:

- com.amazonaws. ***region***.ec2 - Membuat titik akhir untuk tindakan Amazon EC2 API.

Untuk informasi selengkapnya, lihat Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan.AWS PrivateLink

Membuat kebijakan titik akhir

kebijakan titik akhir adalah sumber daya IAM yang dapat Anda lampirkan ke titik akhir antarmuka Anda. Kebijakan titik akhir default mengizinkan akses penuh ke Amazon EC2 API melalui titik akhir antarmuka. Untuk mengontrol akses yang diizinkan ke API Amazon EC2 dari VPC Anda, lampirkan kebijakan titik akhir kustom ke titik akhir antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- prinsipal utama yang dapat melakukan tindakan.
- Tindakan-tindakan yang dapat dilakukan.
- Sumber daya yang padanya tindakan dapat dilakukan.

> **Important**
>
> Jika kebijakan non-default diterapkan ke titik akhir VPC antarmuka untuk Amazon EC2, permintaan API tertentu yang gagal, seperti yang gagal`RequestLimitExceeded`, mungkin tidak dicatat atau Amazon. AWS CloudTrail CloudWatch

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan menggunakan kebijakan titik akhir di Panduan AWS PrivateLink .

Contoh berikut menunjukkan kebijakan titik akhir VPC yang menolak izin untuk membuat volume yang tidak terenkripsi atau untuk meluncurkan instans yang memiliki volume yang tidak terenkripsi. Contoh kebijakan tersebut juga memberikan izin untuk melakukan semua tindakan Amazon EC2 lainnya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Opsi penyimpanan untuk EC2 instans Amazon Anda

Amazon EC2 memberi Anda opsi penyimpanan easy-to-use data yang fleksibel, hemat biaya, dan untuk instans Anda. Setiap pilihan memiliki kombinasi performa dan daya tahan yang unik. Opsi penyimpanan ini dapat digunakan secara independen atau bersamaan untuk menyesuaikan kebutuhan Anda.

Blok penyimpanan

- Amazon EBS — Amazon EBS menyediakan volume penyimpanan tingkat blok yang tahan lama yang dapat Anda lampirkan dan lepaskan dari instans Anda. Anda dapat memasang beberapa volume EBS ke suatu instans. Volume EBS berlanjut secara terpisah dari masa aktif instans terkait. Anda dapat mengenkripsi volume EBS Anda. Untuk menyimpan salinan cadangan data, Anda dapat membuat snapshot dari volume EBS Anda. Snapshot disimpan di Amazon S3. Anda dapat membuat volume EBS dari snapshot.
- Instans menyimpan penyimpanan blok sementara untuk instans EC2— Toko instans menyediakan penyimpanan tingkat blok sementara untuk instance. Jumlah, ukuran, dan tipe volume penyimpanan instans ditentukan oleh tipe instans dan ukuran instans. Data pada suatu volume penyimpanan instans hanya akan berlanjut selama masa pakai instans yang terkait; jika Anda berhenti, melakukan hibernasi, atau mengakhiri suatu instans, data apa pun yang berupa volume penyimpanan instan akan hilang.

Penyimpanan objek

- Amazon S3- Amazon S3 menyediakan akses ke infrastruktur penyimpanan data yang andal dan murah. Ini dirancang untuk membuat komputasi skala web lebih mudah dengan memungkinkan Anda untuk menyimpan dan mengambil sejumlah data, kapan saja, dari dalam Amazon EC2 atau di mana saja di web. Misalnya, Anda dapat menggunakan Amazon S3 untuk menyimpan salinan cadangan data dan aplikasi Anda. Amazon EC2 menggunakan Amazon S3 untuk menyimpan snapshot EBS dan didukung Amazon S3. AMIs

Penyimpanan file

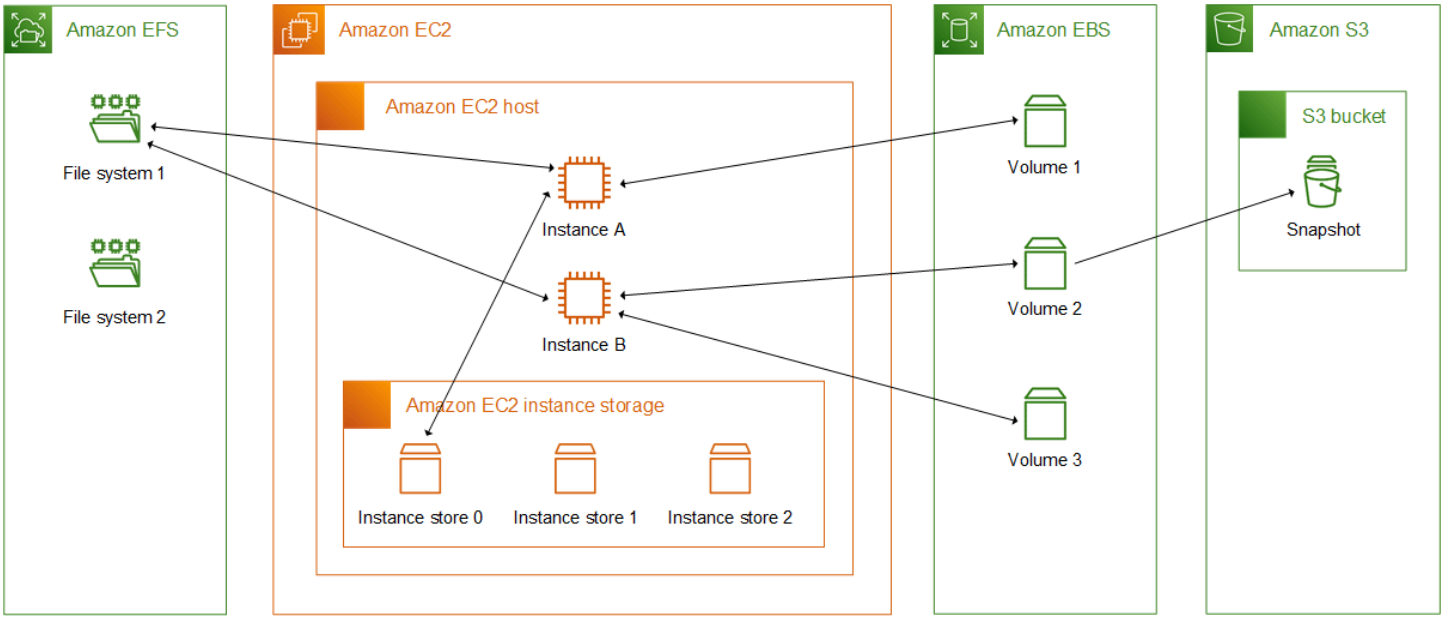
- Amazon EFS(Hanya instans Linux) - Amazon EFS menyediakan penyimpanan file yang dapat diskalakan untuk digunakan dengan Amazon. EC2 Anda dapat membuat sistem file EFS dan mengonfigurasikan instans Anda untuk memasang sistem file. Anda dapat menggunakan sistem file EFS sebagai sumber data umum untuk beban kerja dan aplikasi yang berjalan pada beberapa instans.
- Amazon FSx— Dengan Amazon FSx, Anda dapat meluncurkan, menjalankan, dan menskalakan sistem file berkinerja tinggi yang kaya fitur di cloud. Amazon FSx adalah layanan

yang dikelola sepenuhnya yang mendukung berbagai beban kerja. Anda dapat memilih antara sistem file yang banyak digunakan ini: Lustre, NetApp ONTAP, OpenZFS, dan Windows File Server.

Caching file

- Menggunakan Cache File Amazon dengan EC2 instans Amazon- Amazon File Cache menyediakan cache sementara berkinerja tinggi AWS untuk memproses data file. Cache menyediakan akses data baca dan tulis untuk menghitung beban kerja di Amazon EC2 dengan latensi sub-milidetik, hingga ratusan throughput, dan hingga jutaan GB/s IOPS.

Gambar berikut ini menunjukkan hubungan antara opsi penyimpanan ini dan instans Anda.



AWS Harga penyimpanan

Buka AWS Harga, gulir ke Harga untuk AWS produk dan pilih Penyimpanan. Pilih produk penyimpanan untuk membuka halaman harga.

Penyimpanan blok persisten Amazon EBS untuk instans Amazon EC2

Amazon Elastic Block Store (Amazon EBS) menyediakan sumber daya penyimpanan blok berkinerja tinggi yang dapat diskalakan yang dapat digunakan dengan instans Amazon EC2. Dengan Amazon EBS, Anda dapat membuat dan mengelola sumber daya penyimpanan blok berikut:

- Volume Amazon EBS — Ini adalah volume penyimpanan yang Anda lampirkan ke instans Amazon EC2. Setelah Anda melampirkan volume ke sebuah instance, Anda dapat menggunakannya dengan cara yang sama seperti Anda akan menggunakan penyimpanan blok. Instance dapat berinteraksi dengan volume seperti halnya dengan drive lokal.
- Snapshot Amazon EBS — Ini adalah point-in-time cadangan volume Amazon EBS yang bertahan secara independen dari volume itu sendiri. Anda dapat membuat snapshot untuk mencadangkan data pada volume Amazon EBS Anda. Anda kemudian dapat memulihkan volume baru dari snapshot tersebut kapan saja.

Anda dapat membuat dan melampirkan volume EBS ke instans selama peluncuran, dan Anda dapat membuat dan melampirkan volume EBS ke instance kapan saja setelah peluncuran. Anda juga dapat meningkatkan ukuran atau kinerja volume EBS Anda tanpa melepaskan volume atau memulai ulang instans Anda.

Anda dapat membuat snapshot EBS dari volume EBS kapan saja setelah pembuatan. Anda dapat menggunakan snapshot EBS untuk mencadangkan data yang tersimpan di volume Anda. Anda kemudian dapat menggunakan snapshot tersebut untuk memulihkan volume secara instan, atau untuk memigrasikan data di seluruh Akun AWS, AWS Wilayah, atau Availability Zone. Anda dapat menggunakan Amazon Data Lifecycle Manager atau AWS Backup untuk mengotomatiskan pembuatan, penyimpanan, dan penghapusan snapshot EBS Anda.

Volume EBS terkelola dikelola oleh penyedia layanan, seperti Amazon EKS Auto Mode. Anda tidak dapat langsung mengubah pengaturan volume EBS terkelola. Volume EBS terkelola diidentifikasi oleh nilai sebenarnya di bidang Dikelola. Untuk informasi selengkapnya, lihat Instans terkelola Amazon EC2.

Untuk informasi selengkapnya tentang bekerja dengan volume dan snapshot, lihat Panduan Pengguna Amazon EBS.

Batas volume Amazon EBS untuk instans Amazon EC2

Jumlah maksimum volume Amazon EBS yang dapat dilampirkan ke instans bergantung pada tipe instans dan ukuran instans. Jika Anda melebihi batas lampiran volume untuk sebuah instance, permintaan lampiran gagal dengan `AttachmentLimitExceeded` kesalahan tersebut.

Saat mempertimbangkan berapa banyak volume yang harus dilampirkan ke instans Anda, Anda harus mempertimbangkan apakah Anda memerlukan peningkatan I/O bandwidth atau peningkatan kapasitas penyimpanan.

Bandwidth versus kapasitas

Untuk kasus penggunaan bandwidth yang konsisten dan dapat diprediksi, gunakan instans Amazon EBS yang dioptimalkan dengan volume SSD Tujuan Umum atau volume SSD IOPS yang Disediakan. Untuk performa maksimum, cocokkan IOPS yang telah Anda sediakan untuk volume Anda dengan bandwidth yang tersedia untuk tipe instans Anda.

Untuk konfigurasi RAID, Anda mungkin menemukan bahwa array yang lebih besar dari 8 volume telah mengurangi pengembalian kinerja karena peningkatan overhead. I/O Uji performa aplikasi individual Anda dansesuai kebutuhan.

Daftar Isi

- Batas volume untuk instans yang dibangun di atas Sistem Nitro
  - Batas volume EBS khusus
  - Batas volume EBS bersama
- Batas volume untuk instans berbasis Xen
  - Instans Linux
  - Instans Windows

Batas volume untuk instans yang dibangun di atas Sistem Nitro

Batas volume untuk instance yang dibangun pada Sistem Nitro bergantung pada jenis instans. Beberapa jenis instans Nitro memiliki batas volume EBS khusus, sementara sebagian besar memiliki batas volume bersama. Untuk melihat batas lampiran volume untuk setiap jenis instans, lihat berikut ini:

- Spesifikasi Amazon EBS — Tujuan umum
- Spesifikasi Amazon EBS — Komputasi dioptimalkan
- Spesifikasi Amazon EBS - Memori yang dioptimalkan
- Spesifikasi Amazon EBS - Penyimpanan dioptimalkan
- Spesifikasi Amazon EBS - Komputasi yang dipercepat
- Spesifikasi Amazon EBS — Komputasi berkinerja tinggi
- Spesifikasi Amazon EBS — Generasi sebelumnya

Batas volume EBS khusus

Jenis instans Nitro berikut memiliki batas volume EBS khusus yang bervariasi tergantung pada ukuran instans. Batas tidak dibagikan dengan lampiran perangkat lain. Dengan kata lain, Anda dapat melampirkan sejumlah volume EBS hingga batas lampiran volume, terlepas dari jumlah perangkat yang terpasang, seperti volume penyimpanan NVMe instance dan antarmuka jaringan.

- Tujuan umum: M7a | M7i | M7i-Flex | M8a | M8AZN | M8g | M8gb | M8gD | M8gn | M8i | M8id | M8i-Flex
- Komputasi dioptimalkan: C7a | C7i | C7i-Flex | C8a | C8g | C8gb | C8gd | C8gn | C8i | C8id | C8i-Flex
- Memori dioptimalkan: R7a | R7i | R7iZ | R8a | R8g | R8gb | R8gd | R8gn | R8i | R8iD | R8i-flex | U7i-6tb | U7i-8tb | U7i-12tb | U7in-16TB | U7in-24TB | U7in-32tb | U7inh-32TB | Xinh-32tb | XxB 8g | x8AEDZ | x8i
- Penyimpanan dioptimalkan: i7i | i7ie | i8G | i8GE
- Komputasi dipercepat: F2 | G6 | G6e | G6f | Gr6 | GR6f | G7e | P4d | P4de | P5 | P5e | P5en | P6-B200 | P6-B300 | P6e- | Trn2 | Trn2u GB200
- Komputasi kinerja tinggi: HPC7a | HPC8a

Batas volume EBS bersama

Semua jenis instans Nitro lainnya (tidak tercantum dalamBatas volume EBS khusus) memiliki batas lampiran volume yang dibagi antara volume Amazon EBS, antarmuka jaringan, dan volume penyimpanan NVMe instans. Anda dapat melampirkan sejumlah volume Amazon EBS hingga batas tersebut, dikurangi jumlah antarmuka jaringan terlampir dan volume penyimpanan NVMe instans. Perlu diingat bahwa setiap instance harus memiliki setidaknya satu antarmuka jaringan, dan volume penyimpanan NVMe instance itu secara otomatis dilampirkan saat peluncuran.

Sebagian besar instans Nitro mendukung maksimal 28 lampiran. Contoh berikut menunjukkan cara menghitung berapa banyak volume EBS yang dapat Anda lampirkan.

Contoh

- Dengan `m5.xlarge` instance dengan hanya antarmuka jaringan utama, Anda dapat melampirkan 27 volume EBS.

  28 volume - 1 antarmuka jaringan = 27

- Dengan `m5.xlarge` instance dengan dua antarmuka jaringan tambahan, Anda dapat melampirkan 25 volume EBS.

  28 volume - 3 antarmuka jaringan = 25
- Dengan `m5d.xlarge` instance dengan dua antarmuka jaringan tambahan, Anda dapat melampirkan 24 volume EBS.

  28 volume - 3 antarmuka jaringan - 1 volume penyimpanan NVMe instance = 24

Batas volume untuk instans berbasis Xen

Batas volume untuk instance berbasis Xen, seperti T2, bergantung pada sistem operasi.

Untuk informasi selengkapnya, lihat contoh berbasis Xen.

Instans Linux

Melampirkan lebih dari 40 volume ke instans Linux berbasis Xen dapat menyebabkan kegagalan boot. Angka ini mencakup volume root, ditambah volume penyimpanan instans terlampir dan volume Amazon EBS.

Jika Anda mengalami masalah booting pada suatu instans dengan jumlah volume yang banyak, hentikan instans, lepaskan semua volume yang tidak penting dalam proses booting, mulai instans, lalu pasang kembali volume setelah instans berjalan.

> **Important**
>
> Memasang lebih dari 40 volume ke instans Linux berbasis Xen hanya didukung dengan upaya terbaik dan tidak dijamin.

Instans Windows

Tabel berikut menunjukkan batas volume untuk instans Windows berbasis Xen berdasarkan driver yang digunakan. Angka-angka ini termasuk volume root, ditambah volume penyimpanan instans dan volume Amazon EBS yang terlampir.

Driver	Batas Volume
AWS PV	26

Driver	Batas Volume
Citrix PV	26
Red Hat PV	17

Kami menyarankan Anda untuk tidak melampirkan lebih dari 26 volume ke instance Windows berbasis Xen dengan driver AWS PV atau Citrix PV, karena kemungkinan akan menyebabkan masalah kinerja. Untuk menentukan driver PV mana yang digunakan oleh instans Anda, atau untuk meningkatkan instans Windows Anda dari Red Hat ke driver Citrix PV, lihat the section called “Mutakhirkan driver PV”.

> **Important**
>
> Melampirkan lebih dari jumlah volume berikut ke instans Windows berbasis Xen hanya didukung berdasarkan upaya terbaik dan tidak dijamin.

Untuk informasi selengkapnya tentang cara nama perangkat terkait volume, lihat Cara volume dilampirkan dan dipetakan untuk instans Windows Amazon EC2.

Kartu EBS

Sebagian besar jenis instance mendukung satu kartu EBS. Jenis instans yang mendukung beberapa kartu EBS memberikan kinerja yang dioptimalkan EBS yang lebih tinggi, baik dalam throughput EBS maupun IOPS. Kinerja maksimum instans Amazon EC2 Anda tersebar merata di setiap kartu EBS. Misalnya, pada instans EC2 yang mendukung `1,000,000` total IOPS dengan 2 kartu EBS, setiap kartu EBS dapat mendukung hingga IOPS. `500,000` Untuk informasi tentang performa Amazon EBS yang didukung dari instans Amazon EC2 Anda, lihat. Jenis instans Amazon EBS yang dioptimalkan

Saat Anda melampirkan volume Amazon EBS ke instans yang mendukung beberapa kartu EBS, Anda dapat memilih kartu EBS untuk volume dengan menentukan indeks kartu EBS. Volume root harus dilampirkan ke indeks kartu EBS 0.

Jenis instans dengan beberapa kartu EBS

Jenis contoh berikut mendukung beberapa kartu EBS. Untuk informasi tentang jumlah volume Amazon EBS yang didukung oleh jenis instans, lihatBatas volume Amazon EBS untuk instans Amazon EC2.

Tipe Instans	Jumlah kartu EBS
Tujuan Umum	
m8gb.48xlarge	2
m8gb.logam-48xl	2
Komputasi Dioptimalkan	
c8gb.48xlarge	2
c8gb.metal-48xl	2
Memori Dioptimalkan	
r8gb.48xlarge	2
r8gb.metal-48xl	2

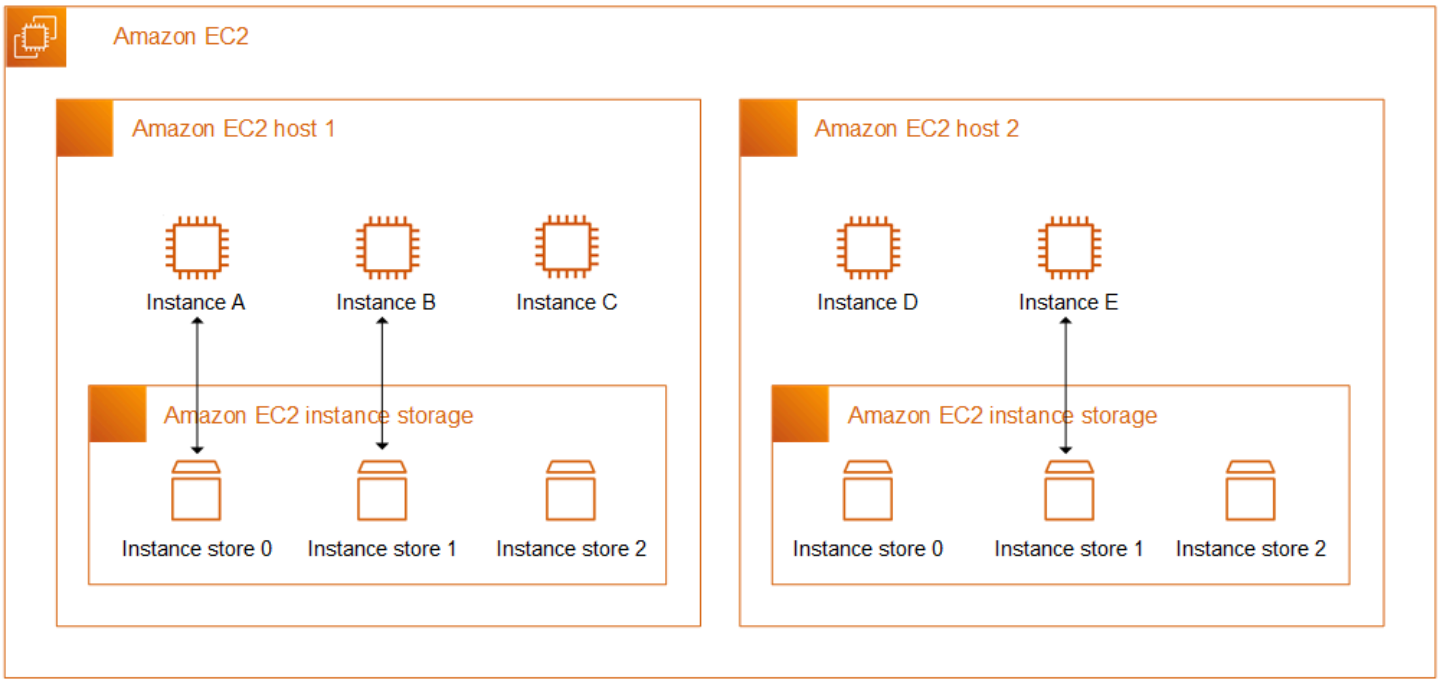
Instans menyimpan penyimpanan blok sementara untuk instans EC2

Toko instans menyediakan penyimpanan tingkat blok sementara untuk instans EC2 Anda. Penyimpanan ini disediakan oleh disk yang secara fisik terpasang ke komputer host. Penyimpanan instans ideal untuk penyimpanan sementara informasi yang sering berubah, seperti buffer, cache, data awal, dan konten sementara lainnya. Ini juga dapat digunakan untuk menyimpan data sementara yang Anda replikasi di seluruh armada instans, seperti kumpulan server web yang seimbang dengan beban.

Penyimpanan instans terdiri dari satu atau lebih volume penyimpanan instans yang terekspos sebagai perangkat blok. Ukuran penyimpanan instans serta jumlah perangkat yang tersedia bervariasi berdasarkan tipe instans dan ukuran instans. Misalnya, tidak setiap jenis instance

menyediakan volume penyimpanan instance. Untuk informasi selengkapnya, lihat Batas volume penyimpanan instans untuk instans EC2.

Perangkat virtual misalnya volume penyimpanan diberi nama perangkat virtual dalam urutan dari `ephemeral0` keephemeral23. Misalnya, dengan jenis instance yang mendukung satu volume penyimpanan instance, nama perangkat virtual dari satu volume adalah`ephemeral0`. Dengan tipe instans yang mendukung empat volume penyimpanan instans, nama perangkat virtual dari empat volume adalah sebagai berikut:`ephemeral0`,`ephemeral1`, `ephemeral2` dan`ephemeral3`.



Harga penyimpanan instans

Tidak ada biaya tambahan untuk menggunakan volume penyimpanan instans yang disediakan untuk instans Anda. Volume penyimpanan instans disertakan sebagai bagian dari biaya penggunaan instance.

Daftar Isi

- Persistensi data untuk volume penyimpanan instans Amazon EC2
- Batas volume penyimpanan instans untuk instans EC2
- Volume penyimpanan instans SSD untuk instans EC2
- Tambahkan volume penyimpanan instans ke instans EC2
- Aktifkan volume swap penyimpanan instans untuk instans M1 dan C1 EC2
- Inisialisasi volume penyimpanan instans pada instans EC2

- Statistik performa terperinci untuk volume penyimpanan instans Amazon EC2

Persistensi data untuk volume penyimpanan instans Amazon EC2

Volume penyimpanan instans dilampirkan hanya pada peluncuran instans. Anda tidak dapat memasang volume penyimpanan instans setelah peluncuran. Anda tidak dapat melepaskan volume penyimpanan instans dari satu instans dan memasangnya ke instans yang berbeda.

Volume penyimpanan instans hanya ada selama masa pakai instans yang dilampirkan. Anda tidak dapat mengonfigurasi volume penyimpanan instans agar bertahan melebihi masa pakai instans terkait.

Data pada volume penyimpanan instans tetap ada meskipun instans di-boot ulang. Namun, data tidak bertahan jika instans dihentikan, dihibernasi, atau dihentikan. Saat instans dihentikan, dihibernasi, atau diakhiri, setiap blok volume penyimpanan instans dihapus secara kriptografis.

Oleh karena itu, jangan bergantung pada volume penyimpanan instans untuk data jangka panjang yang berharga. Jika Anda perlu mempertahankan data yang disimpan pada volume penyimpanan instans di luar masa pakai instans, Anda perlu menyalin data tersebut secara manual ke penyimpanan yang lebih persisten, seperti volume Amazon EBS, bucket Amazon S3, atau sistem file Amazon EFS.

Ada beberapa peristiwa yang dapat mengakibatkan data Anda tidak bertahan sepanjang masa instans. Tabel berikut menunjukkan apakah data pada volume penyimpanan instans dipertahankan selama peristiwa tertentu, baik untuk instans virtualisasi maupun bare metal.

Peristiwa	Apa yang terjadi pada data Anda?
Peristiwa siklus hidup instans yang diinisiasi pengguna	
Instance di-boot ulang	Data tetap ada
Instance dihentikan	Data tidak bertahan
Contohnya hibernasi	Data tidak bertahan
Instance dihentikan	Data tidak bertahan
Jenis instance diubah	Data tidak bertahan *

Peristiwa	Apa yang terjadi pada data Anda?
AMI yang didukung EBS dibuat dari instance	Data tidak bertahan di AMI yang dibuat**
AMI yang didukung Amazon S3 dibuat dari instance (instance Linux)	Data tetap ada dalam bundel AMI yang diunggah ke Amazon S3 ***
Peristiwa OS yang diinisiasi pengguna	
Shutdown dimulai	Data tidak bertahan †
Restart dimulai	Data tetap ada
AWS acara terjadwal	
Contoh berhenti	Data tidak bertahan
Contoh reboot	Data tetap ada
Reboot sistem	Data tetap ada
Pensiun contoh	Data tidak bertahan
Peristiwa yang tidak direncanakan	
Pemulihan otomatis yang disederhanakan	Data tidak bertahan
CloudWatch pemulihan berbasis tindakan	Data tidak bertahan
Disk yang mendasarinya gagal	Data pada disk yang gagal tidak bertahan
Kegagalan daya	Data tetap ada saat reboot

* Jika tipe instans baru mendukung penyimpanan instans, instans mendapatkan jumlah volume penyimpanan instans yang didukung oleh tipe instans baru, tetapi data tidak ditransfer ke instans baru. Jika tipe instans baru tidak mendukung penyimpanan instans, instans tidak mendapatkan volume penyimpanan instans.

** Data tidak disertakan dalam AMI yang didukung EBS, dan tidak disertakan pada volume penyimpanan instans yang dilampirkan ke instans yang diluncurkan dari AMI tersebut.

*** Data disertakan dalam bundel AMI yang diunggah ke Amazon S3. Saat Anda meluncurkan instans dari AMI tersebut, instans mendapatkan volume penyimpanan instans yang dibundel dalam AMI dengan data yang dikandungnya pada saat AMI dibuat.

† Perlindungan penghentian dan perlindungan penghentian tidak melindungi instans terhadap penghentian atau penghentian instans sebagai akibat dari penghentian yang dimulai melalui sistem operasi pada instans. Data yang disimpan pada volume penyimpanan instans tidak bertahan dalam peristiwa penghentian dan penghentian instans.

Batas volume penyimpanan instans untuk instans EC2

Jumlah, ukuran, dan jenis volume penyimpanan instans ditentukan oleh jenis instance. Beberapa tipe instans, seperti C8i, M8i, dan R8i, tidak mendukung volume penyimpanan instans, sementara jenis instans lainnya, seperti C8id, M8id, dan R8id, mendukung volume penyimpanan instans. Anda tidak dapat melampirkan lebih banyak volume penyimpanan instans ke instans daripada yang didukung oleh tipe instans-nya. Untuk tipe instans yang mendukung volume penyimpanan instans, jumlah dan ukuran volume penyimpanan instans bervariasi menurut ukuran instans. Misalnya, `r8id.large` mendukung volume penyimpanan instans 1 x 118 GB, sementara `r8id.32xlarge` mendukung volume penyimpanan instans 2 x 3800 GB.

Untuk tipe NVMe instance dengan volume penyimpanan instance, semua volume penyimpanan instans yang didukung secara otomatis dilampirkan ke instance saat peluncuran. Misalnya jenis dengan volume penyimpanan NVMe non-instance, seperti C1, C3, M1, M2, M3, R3, D2, H1, I2, X1, dan X1e, Anda harus secara manual menentukan pemetaan perangkat blok untuk volume penyimpanan instance yang ingin Anda lampirkan saat peluncuran. Kemudian, setelah instans diluncurkan, Anda harus memformat dan memasang volume penyimpanan instans terlampir sebelum Anda dapat menggunakannya. Anda tidak dapat melampirkan volume penyimpanan instans setelah Anda meluncurkan instans tersebut.

Beberapa tipe contoh menggunakan NVMe solid state drive (SSD) berbasis SATA, sementara yang lain menggunakan hard disk drive (HDD) berbasis SATA. SSDs memberikan I/O kinerja acak tinggi dengan latensi yang sangat rendah, tetapi Anda tidak memerlukan data untuk bertahan saat instance dihentikan atau Anda dapat memanfaatkan arsitektur toleran kesalahan. Untuk informasi selengkapnya, lihat Volume penyimpanan instans SSD untuk instans EC2.

Data pada volume penyimpanan NVMe instance dan beberapa volume penyimpanan instans HDD dienkripsi saat istirahat. Untuk informasi selengkapnya, lihat Perlindungan data dalam Amazon EC2.

Volume penyimpanan instans yang tersedia

Panduan Jenis Instans Amazon EC2 menyediakan pengoptimalan kuantitas, ukuran, jenis, dan performa volume penyimpanan instans yang tersedia pada setiap jenis instans yang didukung. Untuk informasi selengkapnya, lihat berikut ini:

- Spesifikasi toko instans — Tujuan umum
- Spesifikasi toko instans — Komputasi dioptimalkan
- Spesifikasi toko instans - Memori dioptimalkan
- Spesifikasi toko instans — Penyimpanan dioptimalkan
- Spesifikasi toko instans — Komputasi yang dipercepat
- Spesifikasi toko instans — Komputasi berkinerja tinggi
- Spesifikasi toko instans — Generasi sebelumnya

Console

Untuk mengambil informasi volume penyimpanan instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Tipe Instans.
3. Tambahkan filter Penyimpanan instance lokal = true. Kolom Storage menunjukkan ukuran total penyimpanan instance untuk jenis instance.
4. (Opsional) Klik ikon Preferensi dan kemudian nyalakan jumlah disk penyimpanan. Kolom ini menunjukkan jumlah volume penyimpanan instance.
5. (Opsional) Tambahkan filter ke cakupan lebih lanjut ke jenis instans tertentu yang menarik.

AWS CLI

Untuk mengambil informasi volume penyimpanan instance

Gunakan perintah describe-instance-types. Contoh berikut menampilkan ukuran total penyimpanan instans untuk setiap jenis instance dalam keluarga instance R8i dengan volume penyimpanan instance.

```
aws ec2 describe-instance-types \
```

```
    --filters "Name=instance-type,Values=r8i*" "Name=instance-storage-
supported,Values=true" \
    --query 'sort_by(InstanceTypes, &InstanceStorageInfo.TotalSizeInGB)[].
{InstanceType:InstanceType,TotalSizeInGB:InstanceStorageInfo.TotalSizeInGB}' \
    --output table
```

Berikut ini adalah output contoh.

```
-------------------------------------
|        DescribeInstanceTypes       |
+------------------+-----------------+
|   InstanceType   |  TotalSizeInGB  |
+------------------+-----------------+
|  r8id.large      |  118            |
|  r8id.xlarge     |  237            |
|  r8id.2xlarge    |  474            |
|  r8id.4xlarge    |  950            |
|  r8id.8xlarge    |  1900           |
|  r8id.12xlarge   |  2850           |
|  r8id.16xlarge   |  3800           |
|  r8id.24xlarge   |  5700           |
|  r8id.32xlarge   |  7600           |
|  r8id.48xlarge   |  11400          |
|  r8id.metal-48xl |  11400          |
|  r8id.96xlarge   |  22800          |
|  r8id.metal-96xl |  22800          |
+------------------+-----------------+
```

Untuk mendapatkan detail penyimpanan instance lengkap untuk jenis instans

Gunakan perintah describe-instance-types.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r8id.32xlarge" \
    --query 'InstanceTypes[0].InstanceStorageInfo' \
    --output json
```

Contoh output menunjukkan bahwa jenis instance ini memiliki dua volume NVMe SSD 3800 GB, dengan total penyimpanan instans 7600 GB.

```
{
    "TotalSizeInGB": 7600,
```

```
    "Disks": [
        {
            "SizeInGB": 3800,
            "Count": 2,
            "Type": "ssd"
        }
    ],
    "NvmeSupport": "required",
    "EncryptionSupport": "required"
}
```

PowerShell

Untuk mengambil informasi volume penyimpanan instance

Gunakan Get-EC2InstanceTypecmdlet. Contoh berikut menampilkan ukuran total penyimpanan instans untuk setiap jenis instance dalam keluarga instance R8i dengan volume penyimpanan instance.

```
(Get-EC2InstanceType -Filter `
    @{Name="instance-type"; Values="r8i*"},
    @{Name="instance-storage-supported"; Values="true"}) |
    Sort-Object {$_.InstanceStorageInfo.TotalSizeInGB} |
    Format-Table InstanceType,

 @{Name="Disks.SizeInGB";Expression={$_.InstanceStorageInfo.Disks[0].SizeInGB}},
        @{Name="Disks.Count";Expression={$_.InstanceStorageInfo.Disks[0].Count}},
        @{Name="TotalSizeInGB";Expression={$_.InstanceStorageInfo.TotalSizeInGB}}
```

Berikut ini adalah output contoh.

```
InstanceType    Disks.SizeInGB Disks.Count TotalSizeInGB
------------    -------------- ----------- -------------
r8id.large                 118           1           118
r8id.xlarge                237           1           237
r8id.2xlarge               474           1           474
r8id.4xlarge               950           1           950
r8id.8xlarge              1900           1          1900
r8id.12xlarge             2850           1          2850
r8id.16xlarge             3800           1          3800
r8id.24xlarge             2850           2          5700
r8id.32xlarge             3800           2          7600
```

```
r8id.48xlarge             3800          3         11400
r8id.metal-48xl           3800          3         11400
r8id.96xlarge             3800          6         22800
r8id.metal-96xl           3800          6         22800
```

Untuk mendapatkan detail penyimpanan instance lengkap untuk jenis instans

Gunakan Get-EC2InstanceTypecmdlet.

```
(Get-EC2InstanceType `
    -Filter @{Name="instance-type"; Values="r8id.32xlarge"}).InstanceStorageInfo |
    Format-List *,
        @{Name="Disks.Count";Expression={$_.Disks[0].Count}},
        @{Name="Disks.SizeInGB";Expression={$_.Disks[0].SizeInGB}},
        @{Name="Disks.Type";Expression={$_.Disks[0].Type.Value}}
```

Contoh output menunjukkan bahwa jenis instance ini memiliki dua volume NVMe SSD 3800 GB, dengan total penyimpanan instans 7600 GB.

```
Disks             : {Amazon.EC2.Model.DiskInfo}
EncryptionSupport : required
NvmeSupport       : required
TotalSizeInGB     : 7600
Disks.Count       : 2
Disks.SizeInGB    : 3800
Disks.Type        : ssd
```

Volume penyimpanan instans SSD untuk instans EC2

Seperti volume penyimpanan instans lainnya, Anda harus memetakan volume penyimpanan instans SSD untuk instans Anda saat meluncurkannya. Data di SSD merupakan volume instans SSD yang hanya bertahan selama masa pakai instans terkait. Untuk informasi selengkapnya, lihat Tambahkan volume penyimpanan instans ke instans EC2.

NVMe Volume SSD

Beberapa instance menawarkan volume penyimpanan instans solid state drive (SSDNVMe) non-volatile memory express (). Untuk informasi selengkapnya tentang tipe volume penyimpanan instans yang didukung oleh setiap tipe instans, lihat Batas volume penyimpanan instans untuk instans EC2.

Data pada penyimpanan NVMe instance dienkripsi menggunakan cipher blok XTS-AES-256 yang diimplementasikan dalam modul perangkat keras pada instance. Kunci enkripsi dihasilkan menggunakan modul perangkat keras dan unik untuk setiap perangkat penyimpanan NVMe instance. Semua kunci enkripsi tersebut akan dihancurkan saat instans dihentikan atau diakhiri dan tidak dapat dipulihkan. Anda tidak dapat menonaktifkan enkripsi ini dan Anda tidak dapat menyediakan kunci enkripsi Anda sendiri.

Instans Linux

Untuk mengakses NVMe volume, NVMe driver harus diinstal. Berikut ini AMIs memenuhi persyaratan ini:

- AL2023
- Amazon Linux 2
- Amazon Linux AMI 2018.03 dan setelahnya
- Ubuntu 14.04 atau setelahnya dengan kernel `linux-aws`

> **Note**
>
> AWS Jenis instance berbasis Graviton memerlukan Ubuntu 18.04 atau yang lebih baru dengan kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 atau setelahnya
- SUSE Linux Enterprise Server 12 SP2 atau yang lebih baru
- CentOS 7.4.1708 atau setelahnya
- FreeBSD 11.1 atau yang lebih baru
- Debian GNU/Linux 9 atau yang lebih baru

- Bottlerocket

Setelah Anda terhubung ke instans Anda, Anda dapat membuat daftar NVMe perangkat menggunakan lspci perintah. Berikut ini adalah contoh output untuk sebuah `i3.8xlarge` instance, yang mendukung empat NVMe perangkat.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
```

```
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Jika Anda menggunakan sistem operasi yang didukung tetapi Anda tidak melihat NVMe perangkat, verifikasi bahwa NVMe modul dimuat menggunakan perintah berikut.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

  ```
  $ lsmod | grep nvme
  nvme           48813  0
  ```

- Ubuntu 18

  ```
  $ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
  s/nvme/host/nvme-core.ko
  kernel/drivers/nvme/host/nvme.ko
  kernel/drivers/nvmem/nvmem_core.ko
  ```

NVMe Volume sesuai dengan spesifikasi NVMe 1.0e. Anda dapat menggunakan NVMe perintah dengan NVMe volume Anda. Dengan Amazon Linux, Anda dapat menginstal paket `nvme-cli` dari repo menggunakan perintah yum install. Dengan versi Linux lain yang didukung, Anda dapat mengunduh paket `nvme-cli` jika tidak tersedia pada citra.

Instans Windows

AWS Windows terbaru AMIs untuk sistem operasi berikut berisi AWS NVMe driver yang digunakan untuk berinteraksi dengan volume penyimpanan instans SSD yang diekspos sebagai perangkat NVMe blok untuk kinerja yang lebih baik:

- Windows Server 2025
- Windows Server 2022

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Setelah Anda terhubung ke instans Anda, Anda dapat memverifikasi bahwa Anda melihat NVMe volume di Disk Manager. Pada bilah tugas, buka menu konteks (klik kanan) untuk logo Windows dan pilih Manajemen Disk.

AWS Windows yang AMIs disediakan oleh Amazon termasuk AWS NVMe driver. Jika Anda tidak menggunakan AWS Windows terbaru AMIs, Anda dapat menginstal AWS NVMe driver saat ini.

Volume NVMe non-SSD

Instans berikut mendukung volume penyimpanan instans yang menggunakan non- NVMe SSDs untuk memberikan kinerja I/O acak yang tinggi: C3, I2, M3, R3, dan X1. Untuk informasi selengkapnya tentang volume penyimpanan instans yang didukung oleh setiap tipe instans, lihat Batas volume penyimpanan instans untuk instans EC2.

Kinerja volume penyimpanan instans berbasis SSD I/O

Saat Anda mengisi volume penyimpanan instans berbasis SSD untuk instans Anda, jumlah IOPS tulis yang dapat Anda capai akan menurun. Hal ini disebabkan kerja ekstra yang harus dilakukan pengontrol SSD untuk menemukan ruang yang tersedia, menulis ulang data yang ada, dan menghapus ruang yang tidak digunakan agar dapat ditulis ulang. Proses pengumpulan sampah ini menghasilkan amplifikasi tulis internal ke SSD, yang dinyatakan sebagai rasio operasi tulis SSD terhadap operasi tulis pengguna. Penurunan performa ini bahkan lebih besar jika operasi tulis tidak dalam kelipatan 4.096 byte atau tidak diselaraskan dengan batas 4.096 byte. Jika Anda menulis jumlah byte yang lebih kecil yang tidak selaras, pengontrol SSD harus membaca data di sekitarnya dan menyimpan hasilnya di lokasi baru. Pola ini menghasilkan peningkatan amplifikasi tulis yang signifikan, peningkatan latensi, dan penurunan I/O kinerja secara dramatis.

Pengontrol SSD dapat menggunakan beberapa strategi untuk mengurangi dampak amplifikasi tulis. Salah satu strateginya adalah mencadangkan ruang dalam penyimpanan instans SSD sehingga pengontrol dapat mengelola ruang yang tersedia untuk operasi tulis dengan lebih efisien. Hal ini disebut penyediaan berlebih. Volume penyimpanan instans berbasis SSD yang disediakan untuk sebuah instans tidak memiliki ruang yang disediakan untuk penyediaan berlebih. Untuk mengurangi amplifikasi tulis, sebaiknya Anda membiarkan 10 persen volume tidak dipartisi sehingga pengontrol

SSD dapat menggunakannya untuk penyediaan berlebih. Hal ini akan mengurangi penyimpanan yang dapat Anda gunakan, tetapi meningkatkan performa meskipun kapasitas disk hampir penuh.

Misalnya menyimpan volume yang mendukung TRIM, Anda dapat menggunakan perintah TRIM untuk memberi tahu pengontrol SSD kapan pun Anda tidak lagi membutuhkan data yang telah Anda tulis. Hal ini memberikan lebih banyak ruang kosong bagi pengontrol, yang dapat mengurangi amplifikasidan meningkatkan performa. Untuk informasi selengkapnya, lihat Dukungan TRIM volume penyimpanan instans.

Dukungan TRIM volume penyimpanan instans

Beberapa tipe instans mendukung volume SSD dengan TRIM. Untuk informasi selengkapnya, lihat Batas volume penyimpanan instans untuk instans EC2.

> **Note**
>
> (Hanya instance Windows) Instans yang menjalankan Windows Server 2012 R2 mendukung TRIM pada AWS PV Driver versi 7.3.0. Instans yang menjalankan versi Windows Server sebelumnya tidak mendukung TRIM.

Volume penyimpanan instans yang mendukung TRIM sepenuhnya dipangkas sebelum dialokasikan ke instans Anda. Volume ini tidak diformat dengan sistem file saat instans diluncurkan, jadi Anda harus memformatnya sebelum dapat dipasang dan digunakan. Untuk akses yang lebih cepat ke volume ini, Anda harus melewati operasi TRIM saat Anda memformatnya.

(Instans Windows) Untuk menonaktifkan sementara dukungan TRIM selama pemformatan awal, gunakan perintah. `fsutil behavior set DisableDeleteNotify 1` Setelah pemformatan selesai, aktifkan kembali dukungan TRIM dengan menggunakan. `fsutil behavior set DisableDeleteNotify 0`

Untuk volume penyimpanan instans yang mendukung TRIM, Anda dapat menggunakan perintah TRIM untuk memberi tahu kontroler SSD setiap kali Anda tidak lagi membutuhkan data yang telah Anda tulis. Hal ini memberikan lebih banyak ruang kosong bagi kontroler, yang dapat mengurangi amplifikasi dan meningkatkan performa. Pada instance Linux, gunakan `fstrim` perintah untuk mengaktifkan TRIM periodik. Pada instance Windows, gunakan `fsutil behavior set DisableDeleteNotify 0` perintah untuk memastikan dukungan TRIM diaktifkan selama operasi normal.

Tambahkan volume penyimpanan instans ke instans EC2

Untuk tipe NVMe instance dengan volume penyimpanan instance, semua volume penyimpanan instans yang didukung secara otomatis dilampirkan ke instance saat peluncuran. Volume tersebut secara otomatis dilakukan enumerasi dan diberi nama perangkat saat peluncuran instans.

Misalnya jenis dengan volume penyimpanan NVMe non-instance, seperti C1, C3, M1, M2, M3, R3, D2, H1, I2, X1, dan X1e, Anda harus secara manual menentukan pemetaan perangkat blok untuk volume penyimpanan instance yang ingin Anda lampirkan saat peluncuran. Pemetaan perangkat blok dapat ditentukan dalam permintaan peluncuran instans atau dalam AMI yang digunakan untuk meluncurkan instans. Pemetaan perangkat blok mencakup nama perangkat dan volume yang dipetakannya. Untuk informasi selengkapnya, lihat Blokir pemetaan perangkat untuk volume di instans Amazon EC2

> **Important**
>
> Volume penyimpanan instans dapat dilampirkan ke instans hanya saat Anda meluncurkannya. Anda tidak dapat melampirkan volume penyimpanan instans ke instans setelah Anda meluncurkannya.

Setelah Anda meluncurkan suatu instans, Anda harus memastikan bahwa volume penyimpanan instans untuk instans Anda diformat dan dipasang sebelum Anda dapat menggunakannya. Volume root penyimpanan instance dipasang secara otomatis.

Pertimbangan untuk volume root

Pemetaan perangkat blok selalu menentukan volume root untuk instans tersebut. Volume root selalu dipasang secara otomatis.

Instance Linux — Volume root adalah volume Amazon EBS atau volume penyimpanan instans. Untuk instans dengan volume penyimpanan instans untuk volume root, ukuran volume ini bervariasi berdasarkan AMI, tetapi ukuran maksimumnya adalah 10 GB. Untuk informasi selengkapnya, lihat Tipe volume root.

Instans Windows — Volume root harus berupa volume Amazon EBS. Penyimpanan instance tidak didukung untuk volume root.

Daftar Isi

- Tambahkan volume penyimpanan instans ke Amazon EC2 AMI
- Tambahkan volume penyimpanan instans ke instans EC2 selama peluncuran
- Jadikan volume penyimpanan instans tersedia untuk digunakan pada instans EC2

Tambahkan volume penyimpanan instans ke Amazon EC2 AMI

Anda dapat membuat AMI dengan pemetaan perangkat blok yang mencakup volume penyimpanan instans.

Jika Anda meluncurkan instance yang mendukung volume penyimpanan NVMe non-instance menggunakan AMI yang menentukan pemetaan perangkat blok volume penyimpanan instance, instance tersebut menyertakan volume penyimpanan instans. Jika jumlah pemetaan perangkat blok volume penyimpanan instans di AMI melebihi jumlah volume penyimpanan instans yang tersedia untuk instans, pemetaan perangkat blok volume penyimpanan instans tambahan akan diabaikan.

Jika Anda meluncurkan instance yang mendukung volume penyimpanan NVMe instance menggunakan AMI yang menentukan pemetaan perangkat blok volume penyimpanan instance, pemetaan perangkat blok volume penyimpanan instance akan diabaikan. Instans yang mendukung volume penyimpanan NVMe instans mendapatkan semua volume penyimpanan instans yang didukung, terlepas dari pemetaan perangkat blok yang ditentukan dalam permintaan peluncuran instance dan AMI. Pemetaan perangkat volume ini tergantung pada urutan di mana sistem operasi menghitung volume.

Pertimbangan-pertimbangan

- Jumlah volume penyimpanan instans yang tersedia bergantung pada tipe instans. Untuk informasi selengkapnya, lihat the section called “Volume penyimpanan instans yang tersedia”.
- Anda harus menentukan nama perangkat untuk setiap perangkat blok. Untuk informasi selengkapnya, lihat Nama perangkat untuk volume di EC2 instans Amazon.
- Saat meluncurkan instance, Anda dapat menghilangkan volume penyimpanan NVMe non-instance yang ditentukan dalam pemetaan perangkat blok AMI atau menambahkan volume penyimpanan instans.
- Untuk instans M3, tentukan volume penyimpanan instans dalam pemetaan perangkat blok instans, bukan AMI. Amazon EC2 dapat mengabaikan pemetaan perangkat blok volume penyimpanan instans di AMI.

Console

Untuk menambahkan volume penyimpanan instans ke AMI yang didukung Amazon EBS-backed

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans dan pilih instans.
3. Pilih Tindakan, Citra dan templat, Buat citra.
4. Di halaman Buat citra, masukkan nama dan deskripsi yang berarti untuk citra Anda.
5. Untuk setiap volume penyimpanan instans yang akan ditambahkan, pilih Tambahkan volume, dari Tipe volume pilih volume penyimpanan instan, dan dari Perangkat pilih nama perangkat.
6. Pilih Buat citra.

AWS CLI

Untuk menambahkan volume penyimpanan instance ke AMI

Gunakan perintah create-image dengan `--block-device-mappings` opsi untuk menentukan pemetaan perangkat blok untuk AMI yang didukung EBS. Gunakan perintah register-image dengan `--block-device-mappings` opsi untuk menentukan pemetaan perangkat blok untuk AMI yang didukung iAmazon S3.

```
--block-device-mappings file://mapping.json
```

Pemetaan perangkat blok berikut menambahkan dua volume penyimpanan instance.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral0"
    },
    {
        "DeviceName": "/dev/sdd",
        "VirtualName": "ephemeral1"
    }
]
```

PowerShell

Untuk menambahkan volume penyimpanan instance ke AMI

Gunakan New-EC2Imagecmdlet dengan `-BlockDeviceMapping` parameter untuk menentukan pemetaan perangkat blok untuk AMI yang didukung EBS. Gunakan Register-EC2Imagecmdlet dengan `-BlockDeviceMapping` parameter untuk menentukan pemetaan perangkat blok untuk AMI yang didukung Amazon S3.

```
-BlockDeviceMapping $bdm
```

Pemetaan perangkat blok berikut menambahkan dua volume penyimpanan instance.

```
$bdm = @()

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral0"
$bdm += $sdc

$sdd = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdd.DeviceName = "/dev/sdd"
$sdd.VirtualName = "ephemeral1"
$bdm += $sdd
```

Tambahkan volume penyimpanan instans ke instans EC2 selama peluncuran

Saat meluncurkan jenis instans dengan volume penyimpanan NVMe non-instans, seperti C1, C3, M1, M2, M3, R3, D2, H1, I2, X1, dan X1e, Anda harus menentukan pemetaan perangkat blok untuk volume penyimpanan instans yang ingin Anda lampirkan saat peluncuran. Pemetaan perangkat blok harus ditentukan dalam permintaan peluncuran instans atau dalam AMI yang digunakan untuk meluncurkan instans.

Jika AMI menyertakan pemetaan perangkat blok untuk volume penyimpanan instans, Anda tidak perlu menentukan pemetaan perangkat blok dalam permintaan peluncuran instans, kecuali jika Anda membutuhkan lebih banyak volume penyimpanan instans daripada yang disertakan dalam AMI.

Jika AMI tidak menyertakan pemetaan perangkat blok untuk volume penyimpanan instans, Anda harus menentukan pemetaan perangkat blok dalam permintaan peluncuran instans.

Untuk tipe NVMe instance dengan volume penyimpanan instance, semua volume penyimpanan instans yang didukung secara otomatis dilampirkan ke instance saat peluncuran.

Pertimbangan-pertimbangan

- Jumlah volume penyimpanan instans yang tersedia bergantung pada tipe instans. Untuk informasi selengkapnya, lihat the section called “Volume penyimpanan instans yang tersedia”.
- Anda harus menentukan nama perangkat untuk setiap perangkat blok. Untuk informasi selengkapnya, lihat Nama perangkat untuk volume di EC2 instans Amazon.
- Untuk instans M3, Anda dapat menerima volume penyimpanan instans bahkan jika Anda tidak menentukannya dalam pemetaan perangkat blok untuk instans tersebut.

Console

Untuk menentukan pemetaan perangkat blok dalam permintaan peluncuran instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari dasbor, pilih Luncurkan instans.
3. Di bagian Citra Aplikasi dan OS, pilih AMI yang akan digunakan.
4. Di bagian Konfigurasikan penyimpanan, bagian Volume penyimpanan Instans mencantumkan volume penyimpanan instans yang dapat dilampirkan ke instans.
5. Untuk setiap volume penyimpanan instans yang akan dilampirkan, untuk Nama perangkat, pilih nama perangkat yang akan digunakan.
6. Konfigurasikan pengaturan instans yang tersisa sesuai kebutuhan, lalu pilih Luncurkan instans.

AWS CLI

Untuk menentukan pemetaan perangkat blok dalam permintaan peluncuran instance

Gunakan perintah run-instance dengan opsi. `--block-device-mappings`

```
--block-device-mappings file://mapping.json
```

Pemetaan perangkat blok berikut menambahkan dua volume penyimpanan instance.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral0"
```

```
    },
    {
        "DeviceName": "/dev/sdd",
        "VirtualName": "ephemeral1"
    }
]
```

PowerShell

Untuk menentukan pemetaan perangkat blok dalam permintaan peluncuran instance

Gunakan New-EC2Instancecmdlet dengan opsi. `-BlockDeviceMapping`

```
-BlockDeviceMapping $bdm
```

Pemetaan perangkat blok berikut menambahkan dua volume penyimpanan instance.

```
$bdm = @()

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral0"
$bdm += $sdc

$sdd = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdd.DeviceName = "/dev/sdd"
$sdd.VirtualName = "ephemeral1"
$bdm += $sdd
```

Jadikan volume penyimpanan instans tersedia untuk digunakan pada instans EC2

Setelah meluncurkan instans dengan volume penyimpanan instans terlampir, Anda harus memasang volume sebelum dapat mengaksesnya.

Instans Linux

Anda dapat memformat volume dengan sistem file pilihan Anda setelah meluncurkan instance Anda.

Untuk membuat volume penyimpanan instans tersedia di Linux

1. Sambungkan ke instans Anda menggunakan SSH. Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..

2. Gunakan perintah `df -h` untuk melihat volume yang diformat dan dipasang.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Gunakan `lsblk` untuk melihat volume yang dipetakan saat peluncuran tetapi tidak diformat dan dipasang.

```
$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Untuk memformat dan memasang volume penyimpanan instans yang dipetakan saja, lakukan hal berikut:

   a. Buat sistem file di perangkat menggunakan perintah `mkfs`.

   ```
   $ sudo mkfs -t xfs /dev/nvme1n1
   ```

   b. Buat direktori tempat memasang perangkat menggunakan perintah `mkdir`.

   ```
   $ sudo mkdir /data
   ```

   c. Pasang perangkat di direktori yang baru dibuat dengan menggunakan perintah `mount`.

   ```
   $ sudo mount /dev/nvme1n1 /data
   ```

Instans Windows

Untuk instans Windows, kami memformat ulang volume penyimpanan instans dengan sistem file NTFS.

Anda dapat melihat volume penyimpanan instance menggunakan Windows Disk Management. Untuk informasi selengkapnya, lihat Daftar non- NVMe disk.

Untuk secara manual memasang volume penyimpanan instans

1. Pilih Mulai, masukkan Manajemen Komputer, lalu tekan Enter.
2. Di panel kiri, pilih Manajemen Disk.
3. Jika Anda diminta untuk menginisialisasi volume, pilih volume untuk inisialisasi, pilih jenis partisi yang diperlukan bergantung pada kasus penggunaan Anda, lalu pilih OKE.
4. Pada daftar volume, klik kanan volume yang akan dipasang, kemudian pilih Volume Sederhana Baru.
5. Di wizard, pilih Selanjutnya.
6. Pada layar Tetapkan Ukuran Volume, pilih Selanjutnya untuk menggunakan ukuran volume maksimum. Atau, pilih ukuran volume antara ruang disk minimum dan maksimum.
7. Pada layar Tetapkan Huruf Drive atau Jalur, lakukan salah satu hal berikut ini, lalu pilih Next.
   - Untuk memasang volume dengan huruf drive, pilih Tetapkan huruf drive berikut, lalu pilih huruf drive yang akan digunakan.
   - Untuk memasang volume sebagai folder, pilih Pasang di folder NTFS kosong berikut lalu pilih Jelajahi untuk membuat atau memilih folder yang akan digunakan.
   - Untuk memasang volume tanpa huruf drive atau jalur, pilih Jangan tetapkan huruf drive atau jalur drive.
8. Pada layar Format Partisi, tentukan apakah akan memformat volume atau tidak. Jika Anda memilih untuk memformat volume, pilih sistem file dan ukuran unit yang diperlukan, dan tentukan label volume.
9. Pilih Selanjutnya, Selesai.

Aktifkan volume swap penyimpanan instans untuk instans M1 dan C1 EC2

> **Note**
>
> Topik ini berlaku untuk `c1.medium` dan instance `m1.small` Linux saja.

Tipe `c1.medium` dan `m1.small` instance memiliki jumlah memori fisik yang terbatas. Oleh karena itu, mereka diberi volume swap 900 MiB pada waktu peluncuran untuk bertindak sebagai memori virtual, atau ruang swap, untuk sistem Linux. Ruang swap di Linux dapat digunakan ketika sistem

membutuhkan lebih banyak memori daripada yang dialokasikan secara fisik. Ketika ruang swap diaktifkan, sistem Linux dapat menukar halaman memori yang jarang digunakan dari memori fisik ke ruang swap (baik partisi khusus atau file swap pada sistem file yang ada) dan mengosongkan ruang tersebut untuk halaman memori yang membutuhkan akses berkecepatan tinggi.

> **Note**
>
> - Menggunakan ruang swap untuk paging memori tidak secepat atau seefisien menggunakan RAM. Jika beban kerja Anda secara teratur memindahkan memori ke ruang swap, Anda harus mempertimbangkan untuk bermigrasi ke tipe instans yang lebih besar dengan RAM yang lebih besar. Untuk informasi selengkapnya, lihat Perubahan jenis instans Amazon EC2.
> - Meskipun kernel Linux melihat ruang swap ini sebagai partisi pada volume root, sebenarnya ini adalah volume penyimpanan instance terpisah, terlepas dari jenis volume root Anda.

Amazon Linux secara otomatis mengaktifkan dan menggunakan ruang swap ini, tetapi AMI Anda mungkin memerlukan beberapa langkah tambahan untuk mengenali dan menggunakan ruang swap ini. Untuk melihat apakah instans Anda menggunakan ruang swap, Anda dapat menggunakan perintah swapon -s.

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

Instans di atas memiliki 900 MiB volume swap yang dilampirkan dan diaktifkan. Jika Anda tidak melihat volume swap yang tercantum dalam perintah ini, Anda mungkin perlu mengaktifkan ruang swap untuk perangkat. Periksa disk yang tersedia menggunakan perintah lsblk.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk
```

Di sini, volume swap `xvda3` tersedia untuk instans, tetapi tidak diaktifkan (perhatikan bahwa `MOUNTPOINT` bidang kosong). Anda dapat mengaktifkan volume swap dengan perintah swapon.

> **Note**
>
> Anda harus melakukan prepend `/dev/` ke nama perangkat yang terdaftar oleh lsblk. Perangkat Anda mungkin diberi nama berbeda, seperti `sda3`, `sde3`, atau `xvde3`. Gunakan nama perangkat untuk sistem Anda pada perintah di bawah ini.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

Sekarang, ruang swap akan muncul dalam output lsblk dan swapon -s.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

Anda juga harus mengedit file `/etc/fstab` sehingga ruang swap ini secara otomatis diaktifkan di setiap boot sistem.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Tambahkan baris berikut ke file `/etc/fstab` (menggunakan nama perangkat swap untuk sistem Anda):

```
/dev/xvda3       none    swap    sw  0       0
```

Untuk menggunakan volume penyimpanan instans sebagai ruang swap

Setiap volume penyimpanan instans dapat digunakan sebagai ruang swap. Misalnya, tipe instans `m3.medium` mencakup volume penyimpanan instans SSD 4 GB yang sesuai untuk ruang swap. Jika volume penyimpanan instans Anda jauh lebih besar (misalnya, 350 GB), Anda dapat mempertimbangkan untuk membagi volume tersebut dengan partisi pertukaran yang lebih kecil sebesar 4-8 GB dan sisanya untuk volume data.

> **Note**
>
> Prosedur ini hanya berlaku untuk tipe instans yang mendukung penyimpanan instans. Untuk daftar tipe instans yang didukung, lihat Batas volume penyimpanan instans untuk instans EC2.

1. Buat daftar perangkat blok yang dilampirkan ke instans Anda untuk mendapatkan nama perangkat untuk volume penyimpanan instans Anda.

```
[ec2-user ~]$ lsblk -p
NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0   8G  0 disk /
```

   Dalam contoh ini, volume penyimpanan instans adalah `/dev/xvdb`. Karena ini adalah instans Amazon Linux, volume penyimpanan instans diformat dan dipasang di `/media/ephemeral0`; tidak semua sistem operasi Linux melakukan ini secara otomatis.

2. (Opsional) Jika volume penyimpanan instans Anda dipasang (mencantumkan `MOUNTPOINT` dalam output perintah lsblk), lepaskan dengan perintah berikut ini.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Siapkan area swap Linux di perangkat dengan perintah mkswap.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Aktifkan ruang swap baru.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Verifikasi bahwa ruang swap baru sedang digunakan.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
/dev/xvdb                               partition 4188668 0 -1
```

6. Edit file `/etc/fstab` sehingga ruang swap ini secara otomatis diaktifkan di setiap boot sistem.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Jika file `/etc/fstab` memiliki entri untuk `/dev/xvdb` (atau `/dev/sdb`), ubah agar cocok dengan baris di bawah ini; jika tidak memiliki entri untuk perangkat ini, tambahkan baris berikut ke file `/etc/fstab` (menggunakan nama perangkat swap untuk sistem Anda):

```
/dev/xvdb       none    swap    sw  0       0
```

> **Important**
>
> Data volume penyimpanan instans hilang saat instans dihentikan atau dihibernasi; ini termasuk pemformatan ruang swap penyimpanan instans yang dibuat dalam file Step 3. Jika Anda berhenti dan memulai ulang suatu instans yang telah dikonfigurasi untuk menggunakan ruang swap penyimpanan instans, Anda harus mengulangi Step 1 melalui Step 5 pada volume penyimpanan instan baru.

Inisialisasi volume penyimpanan instans pada instans EC2

Karena cara Amazon EC2 dalam memvirtualisasi disk, penulisan pertama ke lokasi mana pun pada beberapa volume penyimpanan instans berjalan lebih lambat dibandingkan penulisan berikutnya. Untuk sebagian besar aplikasi, mengamortisasi biaya ini selama masa pakai instans dapat diterima. Namun, jika Anda membutuhkan performa disk yang tinggi, sebaiknya inisialisasi drive dengan menulis satu kali ke setiap lokasi drive sebelum digunakan dalam produksi.

> **Note**
>
> Jenis instans dengan solid state drive (SSD) yang terpasang langsung dan dukungan TRIM memberikan kinerja maksimum pada waktu peluncuran, tanpa inisialisasi. Untuk informasi tentang penyimpanan instans untuk setiap tipe instans, lihat Batas volume penyimpanan instans untuk instans EC2.

Jika Anda membutuhkan fleksibilitas yang lebih besar dalam hal latensi atau throughput, sebaiknya gunakan Amazon EBS.

Untuk menginisialisasi volume penyimpanan instans, gunakan perintah dd berikut, bergantung pada penyimpanan yang akan menginisialisasi (misalnya, `/dev/sdb` atau `/dev/nvme1n1`).

> **Note**
>
> Pastikan untuk melepaskan drive sebelum melakukan perintah ini.
> Inisialisasi dapat memakan waktu lama (sekitar 8 jam untuk instans sangat besar).

Untuk menginisialisasi volume penyimpanan instans, gunakan perintah berikut pada tipe instans `m1.large`, `m1.xlarge`, `c1.xlarge`, `m2.xlarge`, `m2.2xlarge`, dan `m2.4xlarge`:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Untuk melakukan inisialisasi pada semua volume penyimpanan instans pada saat bersamaan, gunakan perintah berikut:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

Mengonfigurasi drive untuk RAIDdengan melakukanke setiap lokasi drive. Saat mengonfigurasi RAID berbasis perangkat lunak, pastikan untuk mengubah kecepatan rekonstruksi minimum:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Statistik performa terperinci untuk volume penyimpanan instans Amazon EC2

Amazon EC2 menyediakan statistik kinerja resolusi tinggi real-time untuk volume penyimpanan instans NVMe yang dilampirkan ke instans Amazon EC2 berbasis Nitro. Statistik ini disajikan sebagai penghitung agregat yang dipertahankan selama masa hidup instans. Statistik memberikan rincian tentang jumlah kumulatif operasi, byte yang dikirim dan diterima, waktu yang dihabiskan untuk operasi baca dan tulis, dan histogram untuk I/O operasi baca dan tulis. I/O Meskipun statistik ini mempertahankan konsistensi dengan statistik kinerja terperinci Amazon EBS, statistik ini juga menyertakan histogram latensi terperinci yang dipecah berdasarkan I/O ukuran, yang dapat

memberikan wawasan yang lebih terperinci tentang pola kinerja penyimpanan Anda. Visibilitas yang ditingkatkan ini memungkinkan Anda mengidentifikasi secara tepat I/O ukuran spesifik mana yang mengalami masalah latensi, memungkinkan Anda mengoptimalkan kinerja aplikasi dan memecahkan masalah dengan lebih efektif.

Anda dapat mengumpulkan statistik ini dengan perincian hingga interval 1 detik. Jika permintaan dibuat lebih sering dari interval 1 detik, NVMe pengemudi mungkin mengantri permintaan, bersama dengan perintah admin lainnya, untuk diproses di lain waktu.

Pertimbangan-pertimbangan

- Statistik hanya didukung untuk volume penyimpanan NVMe misalnya yang dilampirkan ke instance berbasis Nitro.
- Penghitung tidak persisten di seluruh instance stop dan restart.
- Statistik tersedia tanpa biaya tambahan.

Statistik

Perangkat NVMe blok menjual statistik berikut:

Nama statistik	Nama lengkap	Tipe	Deskripsi
`total_rea d_ops`	Total operasi baca	Penghitun g	Jumlah total operasi baca yang selesai.
`total_wr te_ops`	Total operasi tulis	Penghitun g	Jumlah total operasi penulisan yang diselesai kan.
`total_rea d_bytes`	Total byte baca	Penghitun g	Jumlah total byte baca yang ditransfer.
`total_wr te_bytes`	Total byte tulis	Penghitun g	Jumlah total byte tulis yang ditransfer.
`total_rea d_time`	Total waktu baca	Penghitun g	Total waktu yang dihabiskan, dalam mikrodetik, oleh semua operasi baca yang diselesaikan.

Nama statistik	Nama lengkap	Tipe	Deskripsi
`total_wr` `te_time`	Total waktu tulis	Penghitung	Total waktu yang dihabiskan, dalam mikrodetik, oleh semua operasi penulisan yang diselesaikan.
`instance_` `store_vo` `ume_perf` `rmance_e` `ceeded_i` `ps`	Total permintaan waktu melebihi IOPS maksimum volume	Penghitung	Total waktu, dalam mikrodetik, permintaan IOPS melebihi IOPS maksimum volume. Nilai apa pun di atas `0` menunjukkan bahwa beban kerja Anda menuntut lebih banyak IOPS daripada yang dapat diberikan volume. Idealnya, jumlah tambahan metrik ini, antara dua waktu snapshot, harus minimal.
`instance_` `store_vo` `ume_perf` `rmance_e` `ceeded_t`	Total permintaan waktu melebihi throughput maksimum volume	Penghitung	Total waktu, dalam mikrodetik, permintaan throughput melebihi throughput maksimum volume. Nilai apa pun di atas `0` menunjukkan bahwa beban kerja Anda menuntut lebih banyak throughput daripada yang dapat diberikan volume. Idealnya, jumlah tambahan metrik ini, antara dua waktu snapshot, harus minimal.
`volume_q` `eue_leng` `h`	Panjang antrian volume	Titik waktu	Jumlah operasi baca dan tulis yang menunggu untuk diselesaikan.
`read_io_` `atency_h` `stogram`	Baca I/O histogram	Histogram *	Jumlah operasi baca yang diselesaikan dalam setiap bin latensi, dalam mikrodetik.
`write_io_` `latency_` `istogram`	Tulis I/O histogram	Histogram *	Jumlah operasi tulis yang diselesaikan dalam setiap bin latensi, dalam mikrodetik.

> **Note**
>
> * Statistik histogram hanya mewakili I/O operasi yang telah selesai dengan sukses. I/O Operasi yang macet atau terganggu tidak termasuk, tetapi akan terbukti dalam `volume_queue_length` statistik, yang disajikan sebagai point-in-time statistik.

Mengakses statistik

Statistik harus diakses langsung dari instance dimana volume penyimpanan instance dilampirkan. Anda dapat mengakses statistik menggunakan salah satu metode berikut.

Instans Linux

Amazon CloudWatch

Anda dapat mengonfigurasi CloudWatch agen Amazon untuk mengumpulkan statistik dari instans Anda dan membuatnya tersedia sebagai metrik khusus di CloudWatch. Anda kemudian dapat menggunakan metrik CloudWatch untuk menganalisis I/O pola, melacak tren kinerja, membuat dasbor khusus, dan mengatur alarm otomatis berdasarkan ambang kinerja.

Untuk informasi selengkapnya tentang mengonfigurasi CloudWatch agen, lihat Mengumpulkan metrik volume penyimpanan instans Amazon EC2.

nvme-cli tool

Untuk mengakses statistik

1. Hubungkan ke instance tempat volume terpasang.
2. Amazon Linux 2023 AMIs dirilis setelah 15 September 2025 menyertakan versi terbaru dari alat ininvme-cli. Jika Anda menggunakan AMI Amazon Linux yang lebih lama, perbarui `nvme-cli` alat ini.

   ```
   sudo yum install nvme-cli
   ```

3. Jalankan perintah berikut dan tentukan nama perangkat untuk volume.

   ```
   sudo nvme amzn stats /dev/nvme0n1
   ```

Statistik juga menyediakan histogram latensi terperinci yang dipecah berdasarkan ukuran. I/O Untuk melihat statistik yang dipecah berdasarkan I/O ukuran, sertakan `--details` opsi. Contoh:

```
sudo nvme amzn stats --details /dev/nvme0n1
```

Anda bisa mendapatkan informasi lebih lanjut tentang cara menggunakan alat ini dengan menentukan `--help` opsi. Contoh:

```
sudo nvme amzn stats --help
```

Instans Windows

nvme_amzn.exe tool

Untuk mengakses statistik

1. Hubungkan ke instance tempat volume terpasang.
2. Pastikan Anda menggunakan versi AWSNVMe driver `1.7.0` atau yang lebih baru. Untuk informasi lebih lanjut tentang memperbarui AWSNVMe driver, lihat AWS NVMe driver.
3. Dapatkan nomor disk untuk volume. Untuk informasi selengkapnya, lihat Memetakan disk NVMe di Amazon EC2 Windows instans ke volume.
4. Jalankan perintah berikut sebagai Administrator dan tentukan nomor disk untuk volume.

   ```
   .\nvme_amzn.exe stats disk_number
   ```

Statistik juga menyediakan histogram latensi terperinci yang dipecah berdasarkan ukuran. I/O Untuk melihat statistik yang dipecah berdasarkan I/O ukuran, sertakan `--details` opsi. Contoh:

```
.\nvme_amzn.exe stats --details disk_number
```

Volume root untuk instans Amazon EC2

Saat Anda meluncurkan instans, kami membuat volume root untuk instans tersebut. Volume root berisi gambar yang digunakan untuk booting instans tersebut. Setiap instans memiliki volume root

tunggal. Anda dapat menambahkan volume penyimpanan ke instans Anda selama atau setelah peluncuran.

AMI yang Anda gunakan untuk meluncurkan instance menentukan jenis volume root. Anda dapat meluncurkan instans dari AMI yang didukung Amazon EBS-backed (instans Linux dan Windows) atau AMI yang didukung Amazon S3 (hanya instans Linux). Ada perbedaan signifikan antara apa yang dapat Anda lakukan dengan setiap jenis AMI. Untuk informasi selengkapnya tentang metrik ini, lihat Tipe volume root.

Kami menyarankan Anda menggunakan AMIs didukung oleh Amazon EBS, karena instans ini diluncurkan lebih cepat dan menggunakan penyimpanan persisten.

Kami mencadangkan nama perangkat khusus untuk volume root. Untuk informasi selengkapnya, lihat Nama perangkat untuk volume di EC2 instans Amazon.

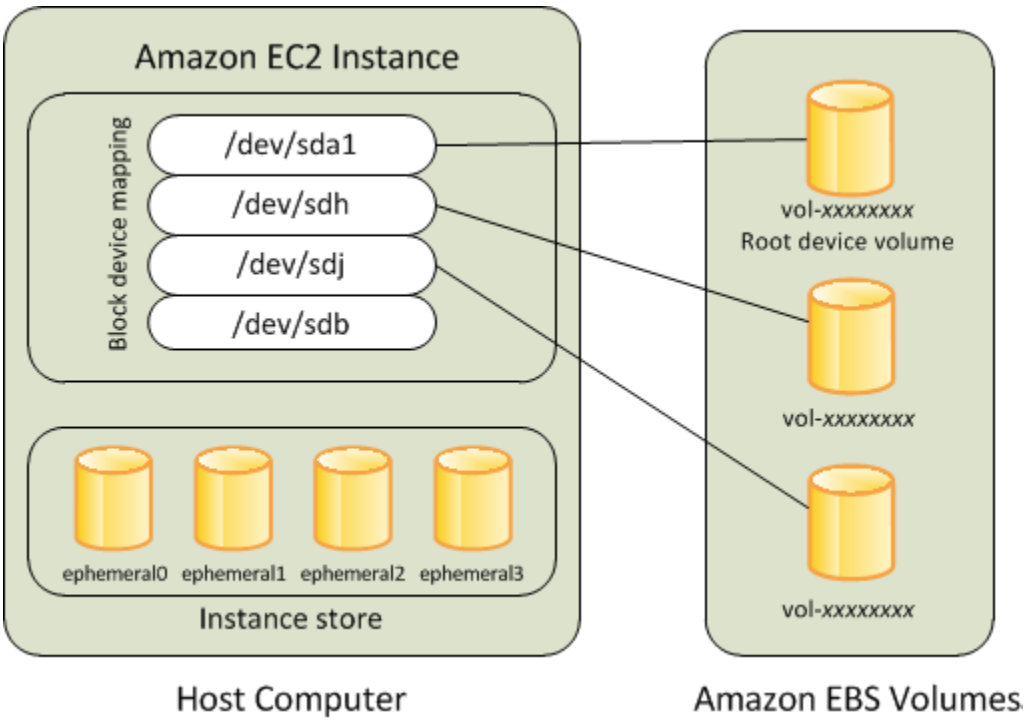
Daftar Isi

- Instans dengan volume root Amazon EBS
- Instance dengan volume root penyimpanan instance (hanya instance Linux)
- Pertahankan volume root Amazon EBS setelah instans Amazon EC2 dihentikan
- Ganti volume root untuk instans Amazon EC2 tanpa menghentikannya

Instans dengan volume root Amazon EBS

Instans yang menggunakan Amazon EBS untuk volume root secara otomatis memiliki volume Amazon EBS yang terlampir. Saat Anda meluncurkan instans dengan Amazon EBS-AMI, kami membuat volume Amazon EBS untuk setiap snapshot Amazon EBS yang direferensikan oleh AMI. Anda dapat menggunakan volume Amazon EBS lain atau volume penyimpanan instans, bergantung pada tipe instans.

Sebuah instance dengan volume root EBS dapat dihentikan dan kemudian dimulai ulang tanpa mempengaruhi data yang disimpan dalam volume terlampir. Ada berbagai tugas terkait instance dan volume yang dapat Anda lakukan saat instance dengan volume root EBS dalam keadaan berhenti. Misalnya, Anda dapat memodifikasi properti instance, mengubah ukurannya, atau memperbarui kernel yang digunakannya, atau Anda dapat melampirkan volume root ke instance berjalan yang berbeda untuk debugging atau tujuan lainnya. Untuk informasi selengkapnya, lihat volume Amazon EBS.



Batasan

Anda tidak dapat menggunakan volume EBS `st1` atau `sc1` sebagai volume root.

Kegagalan instans

Jika instance dengan volume root EBS gagal, Anda dapat memulihkan sesi dengan mengikuti salah satu metode berikut:

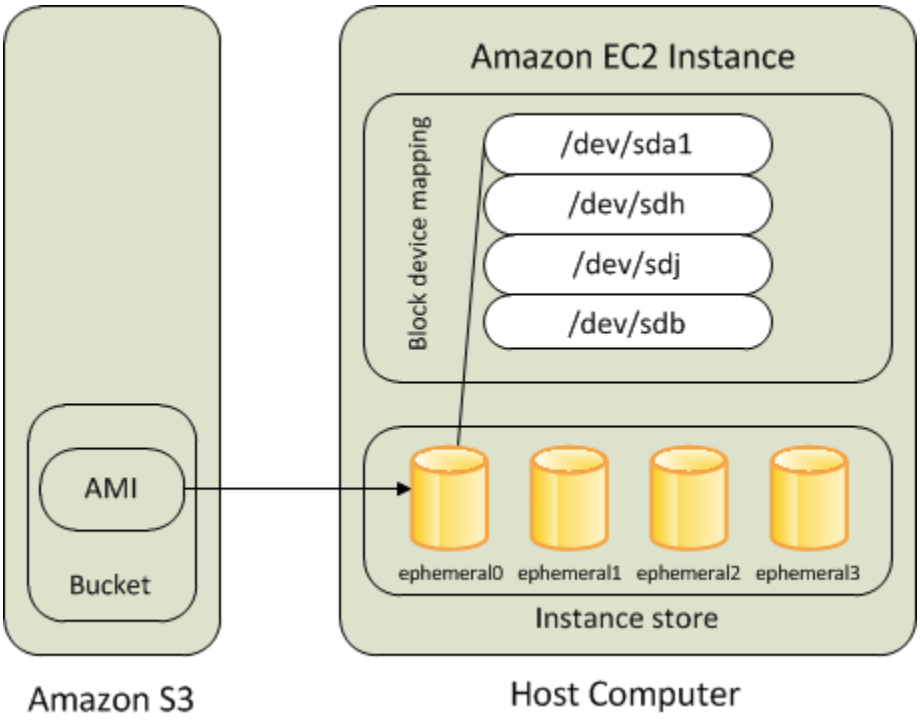
- Hentikan dan mulai lagi (coba metode ini terlebih dahulu).
- Ambil semua volume yang relevan dan buat AMI baru secara otomatis. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.
- Lampirkan volume ke instans baru dengan mengikuti langkah-langkah ini:
  1. Buat snapshot dari volume root.
  2. Daftarkan AMI baru menggunakan snapshot.
  3. Luncurkan instans baru dari AMI baru.
  4. Lepaskan volume Amazon EBS yang tersisa dari instans lama.
  5. Lampirkan kembali volume Amazon EBS ke instans baru.

Instance dengan volume root penyimpanan instance (hanya instance Linux)

> **Note**
>
> Instans Windows tidak mendukung volume root penyimpanan instance.

Instans yang menggunakan penyimpanan instance untuk volume root secara otomatis memiliki satu atau beberapa volume penyimpanan instans yang tersedia, dengan satu volume berfungsi sebagai volume root. Saat instance diluncurkan dari AMI yang didukung Amazon S3, AMI disalin ke volume root. Perhatikan bahwa Anda dapat menggunakan volume penyimpanan instans tambahan, bergantung pada tipe instans.

Data apa pun pada volume penyimpanan instans tetap ada selama instance berjalan, tetapi data ini dihapus saat instance dihentikan (instance dengan volume root penyimpanan instance tidak mendukung tindakan Stop) atau jika gagal (seperti jika drive yang mendasarinya memiliki masalah). Untuk informasi selengkapnya, lihat Instans menyimpan penyimpanan blok sementara untuk instans EC2.



Tipe instans yang didukung

Hanya jenis instance berikut yang mendukung volume penyimpanan instance sebagai volume root: C1, C3, D2, I2, M1, M2, M3, R3, dan X1.

Kegagalan Instans

Setelah instance dengan volume root penyimpanan instance gagal atau berakhir, itu tidak dapat dipulihkan. Jika Anda berencana untuk menggunakan instance dengan volume root penyimpanan instans, sebaiknya Anda mendistribusikan data pada volume penyimpanan instans di beberapa Availability Zone. Anda juga harus mencadangkan data penting dari volume penyimpanan instans Anda ke penyimpanan persisten secara teratur.

Pertahankan volume root Amazon EBS setelah instans Amazon EC2 dihentikan

Secara default, volume root Amazon EBS untuk sebuah instans dihapus saat instance berakhir. Anda dapat mengubah perilaku default untuk memastikan bahwa volume root Amazon EBS tetap ada setelah instance dihentikan. Untuk mengubah perilaku default, setel `DeleteOnTermination` atribut ke`false`. Anda dapat melakukannya baik saat peluncuran instance atau nanti.

Tugas

- Mengonfigurasi volume root agar tetap ada selama peluncuran instans
- Konfigurasikan volume root agar tetap ada untuk instans yang ada
- Konfirmasikan bahwa volume root dikonfigurasi agar tetap ada

Mengonfigurasi volume root agar tetap ada selama peluncuran instans

Anda dapat mengonfigurasi volume root agar tetap ada saat meluncurkan instance.

Console

Untuk mengonfigurasi volume root agar tetap ada saat Anda meluncurkan instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans lalu pilih Luncurkan instans.
3. Pilih Amazon Machine Image (AMI), pilih tipe instans, pilih pasangan kunci, dan konfigurasikan pengaturan jaringan Anda.
4. Untuk Konfigurasikan penyimpanan, pilih Lanjutan.
5. Perluas volume root.
6. Untuk Hapus saat pengakhiran, pilih Tidak.
7. Setelah Anda selesai mengonfigurasi instans, pilih Luncurkan instans.

AWS CLI

Untuk mengonfigurasi volume root agar tetap ada saat Anda meluncurkan instance

Gunakan perintah run-instance dan sertakan opsi berikut.

```
--block-device-mappings file://mapping.json
```

Dalam`mapping.json`, tentukan pemetaan perangkat blok yang menyetel `DeleteOnTermination` atribut ke`false`.

```
[
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

PowerShell

Untuk mengonfigurasi volume root agar tetap ada saat Anda meluncurkan instance

Gunakan New-EC2Instancecmdlet dan sertakan parameter berikut.

```
-BlockDeviceMapping $bdm
```

Buat pemetaan perangkat blok yang menyetel `DeleteOnTermination` atribut ke`$false`.

```
$ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs.DeleteOnTermination = $false
$bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "dev/xvda"
$bdm.Ebs = $ebs
```

Konfigurasikan volume root agar tetap ada untuk instans yang ada

Anda dapat mengonfigurasi volume root untuk bertahan untuk instance yang sedang berjalan. Perhatikan bahwa Anda tidak dapat menyelesaikan tugas ini menggunakan konsol Amazon EC2.

AWS CLI

Untuk mengonfigurasi volume root agar tetap ada untuk instance yang ada

Gunakan modify-instance-attributeperintah dengan pemetaan perangkat blok yang menyetel `DeleteOnTermination` atribut ke`false`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --block-device-mappings file://mapping.json
```

Tentukan hal berikut dalam `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

PowerShell

Untuk mengonfigurasi volume root agar tetap ada untuk instance yang ada

Gunakan Edit-EC2InstanceAttributecmdlet dengan pemetaan perangkat blok yang menyetel atribut ke. `DeleteOnTermination` `$false`

```
$ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
$ebs.DeleteOnTermination = $false
$bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
$bdm.DeviceName = "/dev/xvda"
$bdm.Ebs = $ebs
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -BlockDeviceMapping $bdm
```

Konfirmasikan bahwa volume root dikonfigurasi agar tetap ada

Anda dapat mengonfirmasi bahwa volume root dikonfigurasi untuk bertahan.

Console

Untuk mengonfirmasi bahwa volume root dikonfigurasi untuk bertahan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans kemudian pilih instans Anda.
3. Di tab Penyimpanan, pada Perangkat blok, cari entri untuk volume root. Jika Hapus saat pengakhiran adalah No, volume dikonfigurasi untuk dipertahankan.

AWS CLI

Untuk mengonfirmasi bahwa volume root dikonfigurasi untuk bertahan

Gunakan perintah describe-instance dan verifikasi bahwa `DeleteOnTermination` atribut disetel ke. `false`

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query "Reservations[].Instances[].BlockDeviceMappings"
```

Berikut ini adalah output contoh.

```
[
    [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "AttachTime": "2024-07-12T04:05:33.000Z",
                "DeleteOnTermination": false,
                "Status": "attached",
                "VolumeId": "vol-1234567890abcdef0"

        }
    ]
]
```

PowerShell

Untuk mengonfirmasi bahwa volume root dikonfigurasi untuk bertahan

Gunakan Get-EC2Instancecmdlet dan verifikasi bahwa `DeleteOnTermination` atribut disetel ke. `False`

```
(Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Berikut ini adalah output contoh.

```
AssociatedResource  :
AttachTime          : 7/12/2024 4:05:33 AM
DeleteOnTermination : False
Operator            :
Status              : attached
VolumeId            : vol-1234567890abcdef0
```

Ganti volume root untuk instans Amazon EC2 tanpa menghentikannya

Amazon EC2 memungkinkan Anda untuk mengganti volume root Amazon EBS untuk instans yang berjalan sambil mempertahankan hal berikut:

- Data yang disimpan di volume penyimpanan instans — Volume penyimpanan instans tetap dilampirkan ke instans setelah volume root dipulihkan.
- Data yang disimpan pada volume Amazon EBS data (non-root) — Volume Amazon EBS non-root tetap dilampirkan ke instans setelah volume root dipulihkan.
- Konfigurasi jaringan — Semua antarmuka jaringan tetap melekat pada instance dan mereka mempertahankan alamat IP, pengidentifikasi, dan lampiran mereka. IDs Ketika instans menjadi tersedia, semua lalu lintas jaringan yang tertunda dibersihkan. Selain itu, instans tetap pada host fisik yang sama, sehingga mempertahankan alamat IP publik dan privat serta nama DNS.
- Kebijakan IAM — profil dan kebijakan IAM (seperti kebijakan berbasis tanda) yang terkait dengan instans dipertahankan dan diberlakukan.

Daftar Isi

- Cara kerja penggantian volume root
- Pertimbangan-pertimbangan
- Mengganti volume root

Cara kerja penggantian volume root

Saat Anda mengganti volume root untuk sebuah instance, kami membuat tugas penggantian volume root. Volume root asli dilepaskan dari instans, dan volume root baru dilampirkan ke instans sebagai gantinya. Pemetaan perangkat blok instans diperbarui untuk mencerminkan ID volume root pengganti.

Saat Anda mengganti volume root untuk sebuah instance, Anda harus menentukan sumber snapshot untuk volume baru. Berikut ini adalah opsi yang memungkinkan.

Kembalikan volume root ke keadaan semula

Opsi ini menggantikan volume root saat ini dengan volume yang didasarkan pada snapshot yang digunakan untuk membuatnya.

Pertimbangan untuk menggunakan status peluncuran

Volume root pengganti mendapatkan tipe, ukuran, dan atribut pengakhiran yang sama dengan volume root asli.

Ganti volume root menggunakan snapshot

Opsi ini menggantikan volume root saat ini dengan volume pengganti yang didasarkan pada snapshot yang Anda tentukan. Misalnya, snapshot spesifik yang sebelumnya Anda buat dari volume root ini. Ini berguna jika Anda perlu memulihkan dari masalah yang disebabkan oleh korupsi volume root atau kesalahan konfigurasi jaringan di sistem operasi tamu.

Volume root pengganti mendapatkan tipe, ukuran, dan atribut pengakhiran yang sama dengan volume root asli.

Pertimbangan untuk menggunakan snapshot

- Anda hanya dapat menggunakan snapshot yang dibuat langsung dari volume root instans saat ini atau sebelumnya.
- Anda tidak dapat menggunakan salinan snapshot yang dibuat dari snapshot yang diambil dari volume root.
- Setelah berhasil mengganti volume root, Anda masih dapat menggunakan snapshot yang diambil dari volume root asli untuk mengganti volume root (pengganti) yang baru.

Ganti volume root menggunakan AMI

Opsi ini menggantikan volume root saat ini menggunakan AMI yang Anda tentukan. Ini berguna jika Anda perlu melakukan penambalan atau peningkatan sistem operasi dan aplikasi. AMI harus memiliki kode produk, informasi penagihan, tipe arsitektur, dan jenis virtualisasi yang sama dengan instance.

Jika instance diaktifkan untuk ENA atau sriov-net, maka Anda harus menggunakan AMI yang mendukung fitur-fitur tersebut. Jika instans tidak diaktifkan untuk ENA atau sriov-net, maka Anda dapat memilih AMI yang tidak menyertakan dukungan untuk fitur tersebut, atau Anda dapat menambahkan dukungan secara otomatis jika Anda memilih AMI yang mendukung ENA atau sriov-net.

Jika instance diaktifkan untuk NitRotPM, maka Anda harus menggunakan AMI yang mengaktifkan NitRotPM. Dukungan NitroTPM tidak diaktifkan jika instance tidak dikonfigurasi untuk itu, terlepas dari AMI yang Anda pilih.

Anda dapat memilih AMI dengan mode boot yang berbeda dari instans, selama instans mendukung mode boot AMI. Jika instans tidak mendukung mode boot, permintaan gagal. Jika instans mendukung mode boot, mode boot baru disebarkan ke instans dan data UEFI-nya diperbarui sesuai dengan itu. Jika Anda memodifikasi urutan boot secara manual atau menambahkan kunci Boot Aman UEFI pribadi untuk memuat modul kernel pribadi, perubahan akan hilang selama penggantian volume root.

Volume root pengganti mendapatkan tipe volume yang sama dan atribut hapus saat pengakhiran seperti volume root asli, dan mendapatkan ukuran pemetaan perangkat blok volume root AMI.

> **Note**
>
> Ukuran pemetaan perangkat blok volume root AMI harus sama dengan atau lebih besar dari ukuran volume root asli. Jika ukuran pemetaan perangkat blok volume root AMI lebih kecil dari ukuran volume root asli, permintaan gagal.

Setelah tugas penggantian volume root selesai, informasi baru dan yang diperbarui berikut akan tercermin saat Anda menjelaskan instance menggunakan konsol, AWS CLI atau AWS SDKs:

- ID AMI Baru
- ID volume baru untuk volume root
- Konfigurasi mode boot yang diperbarui (jika diubah oleh AMI)

- Konfigurasi NitroTPM yang diperbarui (jika diaktifkan oleh AMI)
- Konfigurasi ENA yang diperbarui (jika diaktifkan oleh AMI)
- Konfigurasi sriov-net yang diperbarui (jika diaktifkan oleh AMI)

ID AMI baru juga tercermin dalam metadata instans.

Pertimbangan untuk menggunakan AMI:

- Jika Anda menggunakan AMI yang memiliki beberapa pemetaan perangkat blok, hanya volume root AMI yang digunakan. Volume lainnya (non-root) diabaikan.
- Anda hanya dapat menggunakan fitur ini jika Anda memiliki izin untuk AMI dan snapshot volume root terkait. Anda tidak dapat menggunakan fitur ini dengan AWS Marketplace AMIs.
- Anda hanya dapat menggunakan AMI tanpa kode produk hanya jika instans tidak memiliki kode produk.
- Ukuran pemetaan perangkat blok volume root AMI harus sama dengan atau lebih besar dari ukuran volume root asli. Jika ukuran pemetaan perangkat blok volume root AMI lebih kecil dari ukuran volume root asli, permintaan gagal.
- Dokumen identitas instans untuk instans diperbarui secara otomatis.
- Jika instans mendukung NitroTPM, data NitroTPM untuk instans direset dan kunci baru dihasilkan.

Anda dapat memilih apakah akan menyimpan volume root asli setelah proses penggantian volume root selesai. Jika Anda memilih menghapus volume root asli setelah proses penggantian selesai, volume root asli secara otomatis dihapus dan menjadi tidak dapat dipulihkan. Jika Anda memilih untuk menyimpan volume root asli setelah proses selesai, volume tetap disediakan di akun Anda; Anda harus menghapus volume secara manual saat Anda tidak lagi membutuhkannya.

Tugas penggantian volume root bertransisi melalui status berikut:

- `pending`— Volume pengganti sedang dibuat.
- `in-progress`— Volume asli sedang dilepas dan volume pengganti sedang dilampirkan.
- `succeeded`— Volume pengganti telah berhasil dilampirkan ke instance dan instance tersedia.
- `failing`— Tugas penggantian sedang dalam proses kegagalan.
- `failed`— Tugas penggantian telah gagal, tetapi volume root masih terpasang.
- `failing-detached`— Tugas penggantian sedang dalam proses kegagalan dan instance mungkin tidak memiliki volume root yang terpasang.

- `failed-detached`— Tugas penggantian telah gagal dan instance tidak memiliki volume root yang terpasang.

Jika tugas penggantian volume root gagal, instans di-boot ulang dan volume root asli tetap melekat pada instans.

Pertimbangan-pertimbangan

Sebelum Anda mulai, pertimbangkan hal berikut.

Persyaratan

- Instans harus berada dalam status `running`.
- Instans secara otomatis di-reboot selama proses. Isi memori (RAM) dihapus saat boot ulang. Tidak diperlukan boot ulang manual.
- Anda tidak dapat mengganti volume root jika merupakan volume penyimpanan instans. Hanya instans dengan volume root Amazon EBS yang didukung.
- Anda dapat mengganti volume root untuk semua tipe instans virtual dan instans bare metal EC2. Tidak ada jenis instans logam telanjang lainnya yang didukung.
- Anda hanya dapat menggunakan snapshot yang dibuat langsung dari volume root instans saat ini atau sebelumnya.
- Jika akun Anda diaktifkan untuk enkripsi Amazon EBS secara default di Wilayah saat ini, volume root pengganti yang dibuat oleh tugas penggantian volume root selalu dienkripsi, terlepas dari status enkripsi snapshot yang ditentukan atau volume root AMI yang ditentukan.

Hasil enkripsi

Tabel berikut merangkum kemungkinan hasil enkripsi.

	Volume root asli	Snapshot atau AMI yang ditentukan	Enkripsi secara default	Volume root pengganti	Kunci enkripsi yang digunakan untuk penggantian volume root
Mengembalikan volume root pengganti ke status peluncuran awal	Dienkripsi	Tidak berlaku	Tidak dipertimbangkan	Dienkripsi	Kunci KMS yang sama dengan volume root asli
	Tidak terenkripsi	Tidak berlaku	Nonaktif	Tidak terenkripsi	Tidak berlaku
	Tidak terenkripsi	Tidak berlaku	Aktif	Dienkripsi	Kunci KMS default akun untuk enkripsi Amazon EBS
Mengembalikan volume root pengganti dari snapshot atau AMI	Dienkripsi	Tidak terenkripsi	Tidak dipertimbangkan	Dienkripsi	Kunci KMS yang sama dengan volume root asli
	Dienkripsi	Dienkripsi	Tidak dipertimbangkan	Dienkripsi	Kunci KMS yang sama dengan volume root asli
	Tidak terenkripsi	Tidak terenkripsi	Nonaktif	Tidak terenkripsi	Tidak berlaku
	Tidak terenkripsi	Tidak terenkripsi	Aktif	Dienkripsi	Kunci KMS default akun

	Volume root asli	Snapshot atau AMI yang ditentukan	Enkripsi secara default	Volume root pengganti	Kunci enkripsi yang digunakan untuk penggantian volume root
					untuk enkripsi Amazon EBS
	Tidak terenkripsi	Dienkripsi	Tidak dipertimbangkan	Dienkripsi	Jika AMI atau snapshot dimiliki oleh akun, volume pengganti dienkripsi dengan AMI atau kunci KMS snapshot. Jika AMI atau snapshot dibagikan dengan akun, volume pengganti dienkripsi dengan kunci KMS default akun untuk enkripsi Amazon EBS.

Mengganti volume root

Saat Anda mengganti volume root untuk suatu instans, tugas penggantian volume root dibuat. Anda dapat menggunakan tugas penggantian volume root untuk memantau kemajuan dan hasil dari proses penggantian.

Console

Untuk mengganti volume root

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans untuk menggantikan volume root dan pilih Tindakan, Memantau dan memecahkan masalah, Ganti volume root.

   > **Note**
   >
   > Tindakan Ganti volume root dinonaktifkan jika instans yang dipilih tidak dalam status `running`.

4. Untuk Restore, pilih salah satu opsi berikut:
   - Status peluncuran — Kembalikan volume root pengganti dari snapshot yang digunakan untuk membuat volume root saat ini.
   - Snapshot — Kembalikan volume root pengganti ke snapshot yang Anda tentukan. Untuk Snapshot, pilih snapshot yang akan digunakan.
   - Gambar — Kembalikan volume root pengganti menggunakan AMI yang Anda tentukan. Untuk Gambar, pilih AMI yang akan digunakan.
5. (Opsional) Untuk tingkat inisialisasi Volume, Anda dapat menentukan Amazon EBS Provisioned Rate for Volume Initialization (tingkat inisialisasi volume), di MIB/s, di mana blok snapshot akan diunduh dari Amazon S3 ke volume. Untuk informasi selengkapnya, lihat Menggunakan Tarif yang Disediakan Amazon EBS untuk Inisialisasi Volume. Untuk menggunakan tingkat inisialisasi default atau pemulihan snapshot cepat (jika diaktifkan untuk snapshot yang dipilih), jangan tentukan tarif.
6. (Opsional) Untuk menghapus volume root yang Anda ganti, pilih Hapus volume root yang diganti.
7. Pilih Buat tugas pengganti.

8. Untuk memantau tugas penggantian, pilih tab Penyimpanan untuk instance dan perluas tugas penggantian volume root terbaru.

AWS CLI

Untuk mengembalikan volume root pengganti ke status peluncuran awal

Gunakan perintah create-replace-root-volume-task. Untuk `--instance-id`, tentukan ID dari instans yang untuk menggantikan volume root. Hilangkan parameter `--snapshot-id` dan `--image-id`. Untuk menghapus volume root asli setelah diganti, sertakan `--delete-replaced-root-volume` dan tentukan`true`. Untuk menentukan tingkat inisialisasi volume di mana blok snapshot diunduh dari Amazon S3 ke volume, `--volume-initialization-rate` untuk, tentukan nilai `100` antara dan MIB/s. `300`

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Untuk memulihkan volume root pengganti ke snapshot tertentu

Gunakan perintah create-replace-root-volume-task. Untuk `--instance-id`, tentukan ID dari instans yang untuk menggantikan volume root. Untuk `--snapshot-id`, tentukan ID snapshot yang akan digunakan. Untuk menghapus volume root asli setelah diganti, sertakan `--delete-replaced-root-volume` dan tentukan`true`. Untuk menentukan tingkat inisialisasi volume di mana blok snapshot diunduh dari Amazon S3 ke volume, `--volume-initialization-rate` untuk, tentukan nilai `100` antara dan MIB/s. `300`

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Untuk mengembalikan volume root pengganti menggunakan AMI

Gunakan perintah create-replace-root-volume-task. Untuk `--instance-id`, tentukan ID dari instans yang untuk menggantikan volume root. Untuk `--image-id`, tentukan ID snapshot yang akan digunakan. Untuk menghapus volume root asli setelah diganti, sertakan `--delete-replaced-root-volume` dan tentukan`true`. Untuk menentukan tingkat inisialisasi volume di

mana blok snapshot diunduh dari Amazon S3 ke volume, `--volume-initialization-rate` untuk, tentukan nilai `100` antara dan MIB/s. `300`

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Untuk melihat status tugas penggantian volume root

Gunakan perintah describe-replace-root-volume-tasks dan tentukan IDs tugas penggantian volume root untuk dilihat.

```
aws ec2 describe-replace-root-volume-tasks \
    --replace-root-volume-task-ids replacevol-1234567890abcdef0 \
    --query ReplaceRootVolumeTasks[].TaskState
```

Berikut ini adalah output contoh.

```
[
    "succeeded"
]
```

Atau, tentukan filter `instance-id` untuk menyaring hasil menurut instans.

```
$ aws ec2 describe-replace-root-volume-tasks \
    --filters Name=instance-id,Values=i-1234567890abcdef0
```

PowerShell

Untuk mengembalikan volume root pengganti ke status peluncuran awal

Gunakan perintah New-EC2ReplaceRootVolumeTask. Untuk `-InstanceId`, tentukan ID dari instans yang untuk menggantikan volume root. Hilangkan parameter `-SnapshotId` dan `-ImageId`. Untuk menghapus volume root asli setelah diganti, sertakan `-DeleteReplacedRootVolume` dan tentukan`$true`. Untuk menentukan tingkat inisialisasi volume di mana blok snapshot diunduh dari Amazon S3 ke volume, `-VolumeInitializationRate` untuk, tentukan nilai `100` antara dan MIB/s. `300`

```
New-EC2ReplaceRootVolumeTask `
```

```
    -InstanceId i-1234567890abcdef0 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Untuk memulihkan volume root pengganti ke snapshot tertentu

Gunakan perintah New-EC2ReplaceRootVolumeTask. Untuk `--InstanceId`, tentukan ID dari instans yang untuk menggantikan volume root. Untuk `-SnapshotId`, tentukan ID snapshot yang akan digunakan. Untuk menghapus volume root asli setelah diganti, sertakan `-DeleteReplacedRootVolume` dan tentukan`$true`. Untuk menentukan tingkat inisialisasi volume di mana blok snapshot diunduh dari Amazon S3 ke volume, `-VolumeInitializationRate` untuk, tentukan nilai `100` antara dan MIB/s. `300`

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -SnapshotId snap-9876543210abcdef0 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Untuk mengembalikan volume root pengganti menggunakan AMI

Gunakan perintah New-EC2ReplaceRootVolumeTask. Untuk `-InstanceId`, tentukan ID dari instans yang untuk menggantikan volume root. Untuk `-ImageId`, tentukan ID snapshot yang akan digunakan. Untuk menghapus volume root asli setelah diganti, sertakan `-DeleteReplacedRootVolume` dan tentukan`$true`. Untuk menentukan tingkat inisialisasi volume di mana blok snapshot diunduh dari Amazon S3 ke volume, `-VolumeInitializationRate` untuk, tentukan nilai `100` antara dan MIB/s. `300`

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -ImageId ami-0abcdef1234567890 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Untuk melihat status tugas penggantian volume root

Gunakan Get-EC2ReplaceRootVolumeTaskperintah dan tentukan IDs tugas penggantian volume root untuk dilihat.

```
(Get-EC2ReplaceRootVolumeTask `
```

```
    -ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0).TaskState.Value
```

Berikut ini adalah output contoh.

```
Succeeded
```

Atau, tentukan filter `instance-id` untuk menyaring hasil menurut instans.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Nama perangkat untuk volume di EC2 instans Amazon

Saat Anda memasang volume ke instans, Anda menyertakan nama perangkat untuk volume tersebut. Nama perangkat ini digunakan oleh Amazon EC2. Driver perangkat blok untuk instance menetapkan nama volume aktual saat memasang volume, dan nama yang ditetapkan dapat berbeda dari nama yang EC2 digunakan Amazon.

Jumlah volume yang dapat didukung oleh instans Anda mendukung ditentukan oleh sistem operasi. Untuk informasi selengkapnya, lihat Batas volume Amazon EBS untuk instans Amazon EC2.

Daftar Isi

- Nama perangkat yang tersedia
- Pertimbangan nama perangkat

Nama perangkat yang tersedia

Instans Linux

Ada dua jenis virtualisasi yang tersedia untuk instans Linux: paravirtual (PV) dan mesin virtual perangkat keras (HVM). Jenis virtualisasi suatu instans ditentukan oleh AMI yang digunakan untuk meluncurkan instans. Semua jenis instance mendukung AMIs HVM. Beberapa jenis instance generasi sebelumnya mendukung PV AMIs. Pastikan untuk mencatat jenis virtualisasi AMI Anda karena nama perangkat yang disarankan dan tersedia yang dapat Anda gunakan bergantung pada jenis virtualisasi instans Anda. Untuk informasi selengkapnya, lihat Tipe virtualisasi.

Tabel berikut mencantumkan nama perangkat yang tersedia yang dapat Anda tentukan dalam pemetaan perangkat blok atau saat melampirkan volume EBS.

Tipe virtualisasi	Available	Terpesan untuk volume root	Direkomendasikan untuk volume data EBS	Volume penyimpanan instans
Paravirtual	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hh[a-z] /dev/hh[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM	/dev/sd[a-z] /dev/xvd [a-c] [a-z] /dev/xvdd [a-x]	Dibedakan berdasarkan AMI /dev/sda1 or /dev/xvda	/dev/sd [b-z] /dev/xvdb [b-z] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge) **

* Nama perangkat yang Anda tentukan untuk volume NVMe EBS dalam pemetaan perangkat blok diganti namanya menggunakan nama NVMe perangkat (). `/dev/nvme[0-26]n1` Driver perangkat blok dapat menetapkan nama NVMe perangkat dalam urutan yang berbeda dari yang Anda tentukan untuk volume dalam pemetaan perangkat blok.

** Volume penyimpanan NVMe instance secara otomatis disebutkan dan diberi nama perangkat. NVMe

Instans Windows

AWS Windows AMIs menggunakan salah satu set driver berikut untuk mengizinkan akses ke perangkat keras virtual:

- AWS PV: Driver paravirtual untuk instans Windows
- AWS NVMe: AWS NVMe driver

Nama perangkat untuk instance berbasis Nitro

Tabel berikut mencantumkan nama perangkat yang tersedia yang dapat Anda tentukan dalam pemetaan perangkat blok atau saat melampirkan volume EBS ke instance berbasis Nitro.

Jenis driver	Available	Terpesan untuk volume root	Direkomendasikan untuk volume EBS	Volume penyimpanan instans
AWS NVMe	xvd[a-e] xvd [a-c] [a-z] xvdd [a-x] /dev/sda1	/dev/sda1	xvd[b-z] xvdb [b-z]	*

* Volume penyimpanan NVMe instance secara otomatis disebutkan dan diberi huruf drive Windows.

Nama perangkat untuk instance berbasis Xen

Tabel berikut mencantumkan nama perangkat yang tersedia yang dapat Anda tentukan dalam pemetaan perangkat blok atau saat melampirkan volume EBS ke instance berbasis Xen.

Jenis driver	Available	Terpesan untuk volume root	Direkomendasikan untuk volume EBS	Volume penyimpanan instans
AWS PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd [f-z]	xvdc[a-x] xvd[a-e]

Jenis driver	Available	Terpesan untuk volume root	Direkomen dasikan untuk volume EBS	Volume penyimpanan instans
Citrix PV (tidak lagi didukung)	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd [f-z]	xvdc[a-x] xvd[a-e]
Red Hat PV (tidak lagi didukung)	xvd[a-e] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z] *	xvdc[a-x] xvd[a-e]

Untuk informasi selengkapnya tentang volume penyimpanan instans, lihat Instans menyimpan penyimpanan blok sementara untuk instans EC2. Untuk informasi selengkapnya tentang volume NVMe EBS (instans berbasis Nitro), termasuk cara mengidentifikasi perangkat EBS, lihat Amazon EBS dan di NVMe Panduan Pengguna Amazon EBS.

Pertimbangan nama perangkat

Ingatlah hal-hal berikut ini saat memilih nama perangkat:

- Bagian akhir dari nama perangkat yang Anda gunakan tidak boleh tumpang tindih karena dapat menyebabkan masalah saat Anda memulai instance Anda. Misalnya, hindari menggunakan kombinasi seperti `/dev/xvdf` dan `xvdf` untuk volume yang dilampirkan pada instance yang sama.
- Meskipun Anda dapat memasang volume EBS menggunakan nama perangkat yang digunakan untuk lampirkan volume penyimpanan instans, kami sangat menyarankan agar Anda tidak melakukannya karena perilaku tersebut tidak dapat diprediksi.
- Jumlah volume penyimpanan NVMe instance untuk sebuah instance tergantung pada ukuran instance. NVMe volume penyimpanan instance secara otomatis disebutkan dan diberi nama NVMe perangkat (instance Linux) atau huruf drive Windows (instance Windows).

- (Instans Windows) AWS Windows AMIs dilengkapi dengan perangkat lunak tambahan yang menyiapkan instance saat pertama kali boot. Ini adalah layanan EC2 Config (Windows AMIs sebelum Windows Server 2016) atau EC2 Launch (Windows Server 2016 dan yang lebih baru). Setelah perangkat dipetakan ke drive, perangkat diinisialisasi dan dipasang. Drive root diinisialisasi dan dipasang sebagai `C:\`. Secara default, ketika volume EBS dipasang ke instans Windows,dapat muncul sebagai huruf pendorong pada instans tersebut. Anda dapat mengubah pengaturan untuk mengatur huruf drive volume sesuai dengan spesifikasi Anda. Misalnya volume toko, defaultnya tergantung pada driver. AWS Driver PV dan driver Citrix PV menetapkan volume penyimpanan instance huruf drive dari Z: ke A:. Driver Red Hat menetapkan volume penyimpanan instans huruf drive dari D: ke Z:. Untuk informasi selengkapnya, lihat Agen peluncuran Windows di instans Amazon EC2 Windows, dan Cara volume dilampirkan dan dipetakan untuk instans Windows Amazon EC2.
- (Instance Linux) Tergantung pada driver perangkat blok kernel, perangkat dapat dilampirkan dengan nama yang berbeda dari yang Anda tentukan. Misalnya, jika Anda menentukan nama perangkat `/dev/sdh`, perangkat Anda dapat diganti namanya `/dev/xvdh` atau `/dev/hdh`. Dalam kebanyakan kasus, huruf di belakangnya tetap sama. Pada beberapa versi Red Hat Enterprise Linux (dan variannya, seperti CentOS), huruf di belakangnya dapat berubah (`/dev/sda` dapat menjadi `/dev/xvde`). Dalam hal ini, huruf yang ada dari setiap nama perangkat bertambah beberapa kali. Misalnya, jika `/dev/sdb` berganti nama `/dev/xvdf`, kemudian `/dev/sdc` berganti nama `/dev/xvdg`. Amazon Linux membuat tautan simbolis untuk nama yang Anda tetapkan ke perangkat yang diubah namanya. Sistem operasi lainnya dapat berperilaku berbeda.
- (Instance Linux) HVM AMIs tidak mendukung penggunaan nomor tambahan pada nama perangkat, kecuali untuk`/dev/sda1`, yang dicadangkan untuk volume root, dan. `/dev/sda2` Meskipun `/dev/sda2` dapat digunakan, kami tidak menyarankan penggunaan pemetaan perangkat ini dengan instans HVM.
- (Instance Linux) Saat menggunakan PV AMIs, Anda tidak dapat melampirkan volume yang berbagi huruf perangkat yang sama baik dengan maupun tanpa digit tambahan. Misalnya, jika Anda memasang volume sebagai `/dev/sdc` dan volume lainnya `/dev/sdc1`, hanya `/dev/sdc` dapat dilihat oleh instans. Untuk menggunakan digit akhir pada nama perangkat, Anda harus menggunakan digit akhir pada semua nama perangkat yang menggunakan huruf dasar yang sama (seperti `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Instance Linux) Beberapa kernel kustom mungkin memiliki batasan yang membatasi penggunaan untuk `/dev/sd[f-p]` atau. `/dev/sd[f-p][1-6]` Jika Anda mengalami masalah saat menggunakan `/dev/sd[q-z]` atau `/dev/sd[q-z][1-6]`, coba beralih ke `/dev/sd[f-p]` atau `/dev/sd[f-p][1-6]`.

Sebelum Anda menentukan nama perangkat yang telah Anda pilih, verifikasi bahwa itu tersedia. Jika tidak, Anda akan mendapatkan kesalahan bahwa nama perangkat sudah digunakan. Untuk melihat perangkat disk dan titik pemasangannya, gunakan lsblk perintah (instance Linux), atau utilitas Manajemen Disk atau diskpart perintah (instance Windows).

Blokir pemetaan perangkat untuk volume di instans Amazon EC2

Setiap instance yang Anda luncurkan memiliki volume root terkait, yaitu volume Amazon EBS atau volume penyimpanan instans. Anda dapat menggunakan pemetaan perangkat blokir untuk menentukan volume EBS tambahan atau volume penyimpanan instans untuk dilampirkan ke instance saat diluncurkan. Anda juga dapat melampirkan volume EBS tambahan ke instance yang sedang berjalan. Namun, satu-satunya cara untuk melampirkan volume penyimpanan instance ke sebuah instance adalah dengan menggunakan pemetaan perangkat blok untuk melampirkan volume saat instance diluncurkan.

Daftar Isi

- Konsep pemetaan perangkat blok
- Menambahkan pemetaan perangkat blok ke AMI
- Tambahkan pemetaan perangkat blok ke instans Amazon EC2

Konsep pemetaan perangkat blok

Perangkat blok adalah perangkat penyimpanan yang memindahkan data dalam urutan byte atau(blok). Perangkat ini mendukung akses acak dan umumnya menggunakan I/O buffer. Contohnya termasuk hard disk, drive CD-ROM, dan flash drive. Perangkat blok dapat dipasang secara fisik ke komputer atau diakses dari jarak jauh seolah-olah perangkat tersebut terpasang secara fisik ke komputer.

Amazon EC2 mendukung dua jenis perangkat blok:

- Volume penyimpanan instans (perangkat virtual yang perangkat keras yang mendasari secara fisik terpasang ke komputer host untuk instans)
- Volume EBS (perangkat penyimpanan jarak jauh)

pemetaan perangkat blok menentukan perangkat blok (volume penyimpanan instans dan volume EBS) untuk dilampirkan ke suatu instans. Anda dapat menentukan pemetaan perangkat blok

sebagai bagian dari pembuatan AMI sehingga pemetaan tersebut digunakan oleh semua instans yang diluncurkan dari AMI. Atau, Anda dapat menentukan pemetaan perangkat blok ketika Anda meluncurkan instans, sehingga pemetaan ini menimpa pemetaan yang ditentukan dalam AMI tempat Anda meluncurkan instans. Perhatikan bahwa semua volume penyimpanan NVMe instans yang didukung oleh tipe instans secara otomatis dihitung dan diberi nama perangkat pada peluncuran instance; memasukkannya ke dalam pemetaan perangkat blokir tidak berpengaruh.

Daftar Isi

- Entri pemetaan perangkat blok
- Peringatan penyimpanan instans pemetaan perangkat pemetaan perangkat blok
- Contoh pemetaan perangkat blok
- Cara perangkat disediakan dalam sistem operasi

Entri pemetaan perangkat blok

Ketika Anda membuat pemetaan perangkat blok, Anda menentukan informasi berikut untuk setiap perangkat blok yang perlu dilampirkan ke instans:

- Nama perangkat yang digunakan Amazon EC2. Driver perangkat blok untuk instans menetapkan nama volume aktual saat melakukan pemasangan volume. Nama yang diberikan dapat berbeda dari nama yang direkomendasikan oleh Amazon EC2. Untuk informasi selengkapnya, lihat Nama perangkat untuk volume di EC2 instans Amazon.

Untuk volume penyimpanan instans, Anda juga menentukan informasi berikut:

- Perangkat virtual: `ephemeral[0-23]`. Perhatikan bahwa jumlah dan ukuran volume penyimpanan instans yang tersedia untuk instans Anda berbeda-beda menurut tipe instans.

NVMe Misalnya volume toko, informasi berikut juga berlaku:

- Volume ini secara otomatis dienumerasi dan diberi nama perangkat; menyertakannya dalam pemetaan perangkat blok Anda tidak akan berpengaruh.

Untuk volume EBS, Anda juga menentukan informasi berikut:

- ID snapshot yang digunakan untuk membuat perangkat blok (snap-xxxxxxxx). Nilai ini opsional selama Anda menentukan ukuran volume. Anda tidak dapat menentukan ID snapshot yang diarsipkan.
- Ukuran volume, dalam GiB. Ukuran yang ditentukan harus lebih besar atau sama dengan ukuran snapshot yang ditentukan.
- Apakah akan menghapus volume pada saat pengakhiran instans (`true` atau `false`). Nilai default adalah `true` untuk volume root dan `false` volume terlampir. Saat Anda membuat AMI, sistem pemetaan perangkat blok mewarisi pengaturan ini dari instans. Saat diluncurkan, instans akan mewarisi pengaturan ini dari AMI.
- Tipe volume, yang bisa berupa `gp2` dan `gp3` untuk SSD Tujuan Umum, `io1` dan `io2` untuk SSD IOPS yang Tersedia, `st1` untuk HDD Throughput Dioptimalkan, `sc1` untuk Cold HDD, atau `standard` untuk Magnetik.
- Jumlah input/output operasi per detik (IOPS) yang didukung volume. (Hanya digunakan dengan volume `io1` dan `io2`.)
- Beberapa jenis contoh mendukung lebih dari satu kartu EBS. Anda dapat memilih kartu EBS untuk volume yang akan dilampirkan dengan menentukan indeks kartu EBS. Untuk informasi selengkapnya, lihat Kartu EBS.

Peringatan penyimpanan instans pemetaan perangkat pemetaan perangkat blok

Ada beberapa peringatan yang perlu dipertimbangkan saat meluncurkan instance AMIs yang memiliki volume penyimpanan instance dalam pemetaan perangkat bloknya.

- Beberapa tipe instans menyertakan lebih banyak volume penyimpanan instans daripada yang lain, dan beberapa tipe instans tidak mengandung volume penyimpanan instans sama sekali. Jika tipe instans Anda mendukung satu volume penyimpanan instans, dan AMI Anda memiliki pemetaan untuk dua volume penyimpanan instans, instans akan meluncurkan dengan satu volume penyimpanan instans.
- Volume penyimpanan instans hanya dapat dipetakan pada waktu peluncuran. Anda tidak dapat menghentikan instans tanpa volume penyimpanan instans (seperti `t2.micro`), mengubah instans ke tipe yang mendukung volume penyimpanan instans, lalu memulai ulang instans dengan volume penyimpanan instans. Namun, Anda dapat membuat AMI dari instans dan meluncurkannya pada tipe instans yang mendukung volume penyimpanan instans, dan memetakan volume penyimpanan instans tersebut ke instans.

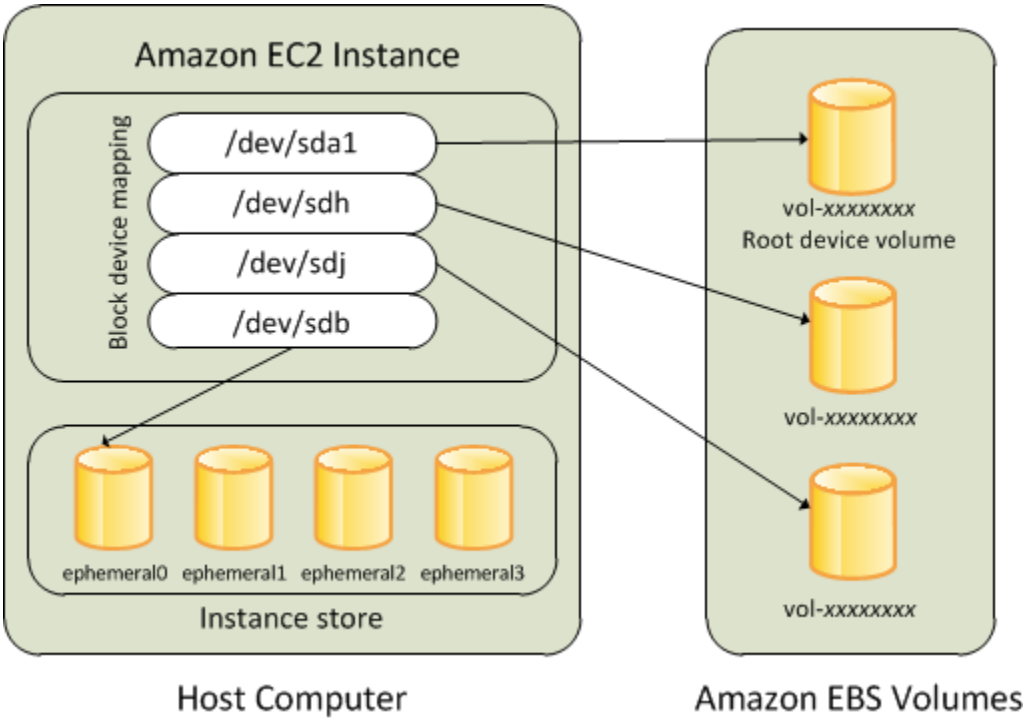
- Jika Anda meluncurkan instans dengan volume penyimpanan instans yang dipetakan, lalu menghentikan instans dan mengubahnya menjadi tipe instans dengan volume penyimpanan instans yang lebih sedikit, lalu memulai ulang instans tersebut, pemetaan volume penyimpanan instans dari peluncuran awal akan tetap muncul di metadata instans. Namun, hanya jumlah maksimum volume penyimpanan instans yang didukung untuk tipe instans tersebut yang tersedia untuk instans tersebut.

  > **Note**
  >
  > Saat instans dihentikan atau diakhiri, semua data pada volume penyimpanan instans akan hilang.

- Bergantung pada kapasitas penyimpanan instans pada saat peluncuran, instans M3 dapat mengabaikan pemetaan perangkat blok penyimpanan instans AMI pada saat peluncuran kecuali jika ditentukan pada saat peluncuran. Anda harus menentukan instans pemetaan perangkat blok penyimpanan pada saat peluncuran, bahkan jika AMI yang Anda luncurkan memiliki volume penyimpanan yang dipetakan di AMI, untuk memastikan bahwa volume penyimpanan instans tersedia saat peluncuran.

Contoh pemetaan perangkat blok

Gambar ini menunjukkan contoh pemetaan perangkat blok untuk instans yang didukung EBS. Gambar ini memetakan `/dev/sdb` ke `ephemeral0` dan memetakan dua volume EBS, satu untuk `/dev/sdh` dan yang lainnya ke `/dev/sdj`. Ini juga menunjukkan volume EBS yang merupakan volume root,`/dev/sda1`.



Perhatikan bahwa contoh pemetaan perangkat blok ini digunakan dalam perintah contoh dan APIs dalam topik ini. Anda dapat menemukan perintah contoh dan APIs yang membuat pemetaan perangkat blok di Tentukan pemetaan perangkat blok untuk AMI dan. Memperbarui pemetaan perangkat blok saat meluncurkan suatu instans

Cara perangkat disediakan dalam sistem operasi

Nama perangkat seperti `/dev/sdh` dan `xvdh` digunakan oleh Amazon EC2 untuk menjelaskan perangkat blok. Pemetaan perangkat blok digunakan oleh Amazon EC2 untuk menentukan perangkat blok yang akan dilampirkan di instans EC2. Setelah dilampirkan pada suatu instans, perangkat blok harus dipasang oleh sistem operasi sebelum Anda dapat mengakses perangkat penyimpanan. Ketika dilepaskan dari suatu instans, perangkat blok dilepaskan oleh sistem operasi dan Anda tidak dapat lagi mengakses perangkat penyimpanan.

Instance Linux — Nama perangkat yang ditentukan dalam pemetaan perangkat blok dipetakan ke perangkat blok yang sesuai saat instance pertama kali melakukan booting. Tipe instans menentukan volume penyimpanan instans mana yang diformat dan dipasang secara default. Anda dapat memasang volume penyimpanan instans tambahan saat peluncuran, selama Anda tidak melebihi jumlah volume penyimpanan instans yang tersedia untuk tipe instans Anda. Untuk informasi selengkapnya, lihat Instans menyimpan penyimpanan blok sementara untuk instans EC2. Driver perangkat blok untuk instans menentukan perangkat yang digunakan saat volume diformat dan dipasang.

Instans Windows - Nama perangkat yang ditentukan dalam pemetaan perangkat blok dipetakan ke perangkat blok yang sesuai saat instance pertama kali melakukan boot, dan kemudian layanan Ec2Config menginisialisasi dan memasang drive. Volume root dipasang sebagai`C:\`. Volume penyimpanan instans dipasang sebagai `Z:\`, `Y:\`, dan sebagainya. Saat dipasang, volume EBS dapat dipasang menggunakan huruf drive yang tersedia. Namun, Anda dapat mengonfigurasi bagaimana huruf drive ditetapkan ke volume EBS; untuk informasi selengkapnya, lihatthe section called “Agen peluncuran Windows”.

Menambahkan pemetaan perangkat blok ke AMI

Setiap AMI memiliki pemetaan perangkat blok yang menentukan perangkat blok yang akan dipasang ke suatu instans ketika diluncurkan dari AMI. Untuk menambahkan lebih banyak perangkat blok ke AMI, Anda harus membuat AMI sendiri.

Daftar Isi

- Tentukan pemetaan perangkat blok untuk AMI
- Lihat volume EBS dalam pemetaan perangkat blok AMI

Tentukan pemetaan perangkat blok untuk AMI

Ada dua cara untuk menentukan volume sebagai tambahan pada volume root saat Anda membuat AMI. Jika Anda telah melampirkan volume ke instans yang sedang berjalan sebelum membuat AMI dari instans, pemetaan perangkat blok untuk AMI akan menyertakan volume yang sama. Untuk volume EBS, data yang ada disimpan ke snapshot baru, dan snapshot baru inilah yang ditentukan dalam pemetaan perangkat blok. Untuk volume penyimpanan instans, data tidak disimpan.

Untuk AMI yang didukung EBS, Anda dapat menambahkan volume EBS dan volume penyimpanan instans menggunakan pemetaan perangkat blok. Untuk AMI yang didukung Amazon S3, Anda dapat menambahkan volume penyimpanan instance hanya dengan memodifikasi entri pemetaan perangkat blok dalam file manifes gambar saat mendaftarkan gambar.

> **Note**
>
> Untuk instans M3, Anda harus menentukan volume penyimpanan instans dalam pemetaan perangkat blok untuk instans ketika Anda meluncurkannya. Saat Anda meluncurkan instans M3, volume penyimpanan instans yang ditentukan dalam pemetaan perangkat blok untuk

AMI dapat diabaikan jika tidak ditentukan sebagai bagian dari pemetaan perangkat blok instans.

Console

Untuk menambahkan volume ke AMI

1. Buka konsol Amazon EC2.
2. Di panel navigasi, pilih Instans.
3. Pilih suatu instans dan pilih Tindakan, Citra dan templat, Buat citra.
4. Masukkan nama dan deskripsi untuk citra.
5. Volume instans muncul di bawah Volume instans. Untuk menambahkan volume lainnya, pilih Tambahkan volume.
6. Untuk Tipe volume, pilih tipe volume. Untuk Perangkat pilih nama perangkat. Untuk volume EBS, Anda dapat menentukan detail tambahan, seperti snapshot, ukuran volume, tipe volume, IOPS, dan status enkripsi.
7. Pilih Buat citra.

AWS CLI

Untuk menambahkan volume ke AMI

Gunakan perintah create-image untuk menentukan pemetaan perangkat blok untuk AMI yang didukung EBS. Gunakan perintah register-image untuk menentukan pemetaan perangkat blok untuk AMI yang didukung Amazon S3.

Tentukan pemetaan perangkat blok menggunakan parameter `--block-device-mappings`. Anda dapat menentukan argumen yang dikodekan dalam JSON langsung pada baris perintah atau dengan mereferensikan file JSON, seperti yang ditunjukkan di sini.

```
--block-device-mappings file://mapping.json
```

Untuk menambahkan volume penyimpanan instans, gunakan pemetaan berikut. Perhatikan bahwa volume penyimpanan NVMe instance ditambahkan secara otomatis.

```
{
    "DeviceName": "device_name",
```

```
    "VirtualName": "ephemeral0"
}
```

Untuk menambahkan volume kosong 100 GiB, gunakan pemetaan berikut ini.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Untuk menambahkan volume EBS berdasarkan snapshot, gunakan pemetaan berikut.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-1234567890abcdef0"
    }
}
```

Untuk pemetaan perangkat, gunakan pemetaan berikut.

```
{
    "DeviceName": "device_name",
    "NoDevice": ""
}
```

PowerShell

Gunakan New-EC2Imagecmdlet untuk menentukan pemetaan perangkat blok untuk AMI yang didukung EBS. Gunakan Register-EC2Imagecmdlet untuk menentukan pemetaan perangkat blok untuk AMI yang didukung Amazon S3.

Tambahkan `-BlockDeviceMapping` opsi, tentukan pembaruan dibdm:

```
-BlockDeviceMapping $bdm
```

Pemetaan berikut menambahkan volume berdasarkan snapshot.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.SnapshotId = "snap-1234567890abcdef0"
```

```
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "device_name"
$bdm.Ebs = $ebd
```

Pemetaan berikut menambahkan volume 100 GB kosong.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.VolumeSize = 100
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "device_name"
$bdm.Ebs = $ebd
```

Lihat volume EBS dalam pemetaan perangkat blok AMI

Anda dapat dengan mudah mengenumerasi volume EBS dalam pemetaan perangkat blok untuk AMI.

Console

Untuk melihat volume EBS untuk AMI

1. Buka konsol Amazon EC2.
2. Di panel navigasi, pilih AMIs.
3. Pilih gambar EBS dari daftar Filter untuk mendapatkan daftar AMIs EBS yang didukung.
4. Pilih AMI yang diinginkan, dan lihat tab Detail. Minimal, informasi berikut tersedia untuk volume root (di mana istilah perangkat root setara dengan volume root):
   - Jenis Perangkat Root (`ebs`)
   - Nama Perangkat Root (misalnya, `/dev/sda1`)
   - Perangkat blok (misalnya, `/dev/sda1=snap-1234567890abcdef0:8:true`)

   Jika AMI dibuat dengan volume EBS tambahan menggunakan pemetaan perangkat blok, Perangkat Blok menampilkan pemetaan untuk volume tambahan juga. Jika AMI dibuat dengan volume EBS tambahan menggunakan pemetaan perangkat blok, Perangkat Blok menampilkan pemetaan untuk volume tambahan juga.

AWS CLI

Untuk melihat volume EBS untuk AMI

Gunakan perintah describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Image[0].BlockDeviceMappings
```

PowerShell

Untuk melihat volume EBS untuk AMI

Gunakan Get-EC2Imagecmdlet.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).BlockDeviceMappings
```

Tambahkan pemetaan perangkat blok ke instans Amazon EC2

Secara default, instans yang Anda luncurkan menyertakan perangkat penyimpanan apa pun yang ditentukan dalam pemetaan perangkat blok AMI tempat Anda meluncurkan instans. Anda dapat menentukan perubahan pada pemetaan perangkat blok untuk sebuah instans saat Anda meluncurkannya, dan pembaruan ini akan menimpa atau bergabung dengan pemetaan perangkat blok AMI.

Batasan

- Untuk volume root, Anda hanya dapat memodifikasi hal berikut: ukuran volume, tipe volume, dan tanda Hapus saat Pengakhiran.
- Saat Anda memodifikasi volume EBS, Anda tidak dapat mengurangi ukuran. Oleh karena itu, Anda harus menentukan snapshot yang ukurannya sama atau lebih besar dari ukuran snapshot yang ditentukan dalam pemetaan perangkat blok AMI.

Tugas

- Memperbarui pemetaan perangkat blok saat meluncurkan suatu instans
- Perbarui pemetaan perangkat blok instans yang berjalan
- Lihat volume EBS dalam pemetaan perangkat blok instans
- Lihat pemetaan perangkat blok instans untuk volume penyimpanan instans

Memperbarui pemetaan perangkat blok saat meluncurkan suatu instans

Anda dapat menambahkan volume EBS dan volume penyimpanan instans ke instans pada saat Anda meluncurkannya. Perhatikan bahwa pembaruan pemetaan perangkat blok untuk suatu instans tidak membuat perubahan permanen pada pemetaan perangkat blok AMI tempatnya diluncurkan.

Console

Untuk memperbarui volume untuk sebuah instance saat peluncuran

1. Ikuti prosedur untuk meluncurkan instance, tetapi jangan meluncurkan instance sampai Anda menyelesaikan langkah-langkah berikut untuk memperbarui volume.
2. (Opsional) Untuk menambahkan volume, pilih Konfigurasi penyimpanan, Tambahkan volume baru. Pilih ukuran volume dan jenis volume.
3. (Opsional) Untuk menekan volume yang ditentukan oleh pemetaan perangkat blok AMI, pilih Konfigurasi penyimpanan, Hapus.
4. (Opsional) Untuk mengubah konfigurasi volume EBS, pada panel Configure storage, pilih Advanced. Perluas informasi untuk volume, dan buat perubahan apa pun yang Anda butuhkan.
5. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

AWS CLI

Untuk memperbarui volume untuk sebuah instance saat peluncuran

Gunakan perintah run-instance dengan opsi. `--block-device-mappings`

```
--block-device-mappings file://mapping.json
```

Misalnya, misalkan pemetaan perangkat blok AMI menentukan hal berikut:

- `/dev/xvda`- Volume akar EBS
- `/dev/sdh`- Volume EBS dibuat dari `snap-1234567890abcdef0`
- `/dev/sdj`- Volume EBS kosong dengan ukuran `100`
- `/dev/sdb`- Volume toko instans `ephemeral0`

Misalkan berikut ini adalah pemetaan perangkat blok instance di`mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 100
        }
    },
    {
        "DeviceName": "/dev/sdj",
        "NoDevice": ""
    },
    {
        "DeviceName": "/dev/sdh",
        "Ebs": {
            "VolumeSize": 300
        }
    },
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral1"
    }
]
```

Pemetaan perangkat blok instance melakukan hal berikut:

- Mengesampingkan ukuran volume root,`/dev/xvda`, meningkatkannya menjadi 100 GiB.
- Mencegah `/dev/sdj` dari melampirkan ke instance.
- Mengesampingkan ukuran`/dev/sdh`, meningkatkannya menjadi 300 GiB. Perhatikan bahwa Anda tidak perlu menentukan ID snapshot lagi.
- Menambahkan volume fana,. `/dev/sdc` Jika jenis instance tidak mendukung beberapa volume penyimpanan instance, ini tidak berpengaruh. Jika tipe instans mendukung volume penyimpanan NVMe instance, maka secara otomatis disebutkan dan disertakan dalam pemetaan perangkat blok instance dan tidak dapat diganti.

PowerShell

Untuk memperbarui volume untuk sebuah instance saat peluncuran

Gunakan `-BlockDeviceMapping` parameter dengan New-EC2Instancecmdlet dengan parameter. `-BlockDeviceMapping`

```
-BlockDeviceMapping $bdm
```

Misalkan berikut ini adalah pemetaan perangkat blok instance di`$bdm`.

```
$bdm = @()

$root = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$root.DeviceName = "/dev/xvda"
$ebs1 = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebs1.VolumeSize = 100
$root.Ebs = $ebs1
$bdm += $root

$sdj = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdj.DeviceName = "/dev/sdj"
$sdj.NoDevice = ""
$bdm += $sdj

$sdh = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdh.DeviceName = "/dev/sdh"
$ebs2 = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebs2.VolumeSize = 300
$sdh.Ebs = $ebs2
$bdm += $sdh

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral1"
$bdm += $sdc
```

Pemetaan perangkat blok instance melakukan hal berikut:

- Mengesampingkan ukuran volume root,`/dev/xvda`, meningkatkannya menjadi 100 GiB.
- Mencegah `/dev/sdj` dari melampirkan ke instance.
- Mengesampingkan ukuran`/dev/sdh`, meningkatkannya menjadi 300 GiB. Perhatikan bahwa Anda tidak perlu menentukan ID snapshot lagi.
- Menambahkan volume fana,. `/dev/sdc` Jika jenis instance tidak mendukung beberapa volume penyimpanan instance, ini tidak berpengaruh. Jika tipe instans mendukung volume

penyimpanan NVMe instance, maka secara otomatis disebutkan dan disertakan dalam pemetaan perangkat blok instance dan tidak dapat diganti.

Perbarui pemetaan perangkat blok instans yang berjalan

Anda tidak perlu menghentikan instans sebelum mengubah atribut ini.

AWS CLI

Untuk memperbarui pemetaan perangkat blok dari instance yang sedang berjalan

Gunakan perintah modify-instance-attribute.

Tambahkan `--block-device-mappings` opsi:

```
--block-device-mappings file://mapping.json
```

Di`mapping.json`, tentukan pembaruan. Misalnya, pembaruan berikut mengubah volume root untuk bertahan.

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

Untuk memperbarui pemetaan perangkat blok dari instance yang sedang berjalan

Gunakan Edit-EC2InstanceAttributecmdlet.

Tambahkan `-BlockDeviceMapping` opsi:

```
-BlockDeviceMapping $bdm
```

Di`bdm`, tentukan pembaruan. Misalnya, pembaruan berikut mengubah volume root untuk bertahan.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Lihat volume EBS dalam pemetaan perangkat blok instans

Anda dapat dengan mudah mengenumerasi volume EBS yang dipetakan sebagai instans.

Console

Untuk melihat volume EBS untuk sebuah instance

1. Buka konsol Amazon EC2.
2. Di panel navigasi, pilih Instans.
3. Pilih instance dan lihat detail yang ditampilkan di tab Penyimpanan. Minimal, informasi berikut tersedia untuk volume root (di mana istilah perangkat root setara dengan volume root):
   - Jenis perangkat root (misalnya, EBS)
   - Nama perangkat root (misalnya, `/dev/xvda`)
   - Perangkat blok (misalnya, `/dev/xvda`, `/dev/sdf`, dan `/dev/sdj`)

   Jika instans diluncurkan dengan volume EBS tambahan menggunakan pemetaan perangkat blok, maka akan muncul di bawah Perangkat blok. Volume penyimpanan instans tidak muncul di tab ini.
4. Untuk menampilkan informasi tambahan tentang volume EBS, pilih ID volumenya untuk membuka halaman volume.

AWS CLI

Untuk melihat volume EBS untuk sebuah instance

Gunakan perintah describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
```

```
    --query Reservations[*].Instances[0].BlockDeviceMappings
```

PowerShell

Untuk melihat volume EBS untuk sebuah instance

Gunakan Get-EC2Instancecmdlet.

```
(Get-EC2Instance -InstanceId i-0bac57d7472c89bac).Instances.BlockDeviceMappings
```

Lihat pemetaan perangkat blok instans untuk volume penyimpanan instans

Jenis instance menentukan jumlah dan jenis volume penyimpanan instance yang tersedia untuk instance. Jika jumlah volume penyimpanan instans dalam pemetaan perangkat blok melebihi jumlah volume penyimpanan instans yang tersedia untuk sebuah instans, volume tambahan akan diabaikan. Untuk melihat volume penyimpanan instance untuk instans Anda, jalankan lsblk perintah (instance Linux) atau buka Windows Disk Management (instance Windows). Untuk mempelajari berapa banyak volume penyimpanan instans yang didukung oleh setiap jenis instans, lihat spesifikasi jenis instans Amazon EC2.

Saat Anda melihat pemetaan perangkat blok untuk instans Anda, Anda hanya dapat melihat volume EBS, bukan volume penyimpanan instans. Metode yang Anda gunakan untuk melihat volume penyimpanan instans untuk instans tergantung pada tipe volume.

NVMe volume toko contoh

Instans Linux

Anda dapat menggunakan paket baris NVMe perintah, nvme-cli, untuk menanyakan volume penyimpanan NVMe instance dalam pemetaan perangkat blok. Unduh dan instal paket di instans Anda, lalu jalankan perintah berikut.

```
[ec2-user ~]$ sudo nvme list
```

Berikut ini contoh output untuk suatu instans. Teks di kolom Model menunjukkan apakah volume adalah volume EBS atau volume penyimpanan instans. Dalam contoh ini, `/dev/nvme1n1` dan `/dev/nvme2n1` adalah volume penyimpanan instans.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store              1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage        1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage        1
  ...
```

Instans Windows

Anda dapat menggunakan Manajemen Disk atau PowerShell untuk mencantumkan NVMe volume penyimpanan EBS dan instans. Untuk informasi selengkapnya, lihat the section called “Peta disk NVME ke volume”.

Volume penyimpanan instans HDD atau SSD

Anda dapat menggunakan metadata instance untuk menanyakan volume penyimpanan instans HDD atau SSD dalam pemetaan perangkat blok. NVMe volume penyimpanan instance tidak disertakan.

URI dasar untuk semua permintaan untuk metadata instans adalah `http://169.254.169.254/latest/`. Untuk informasi selengkapnya, lihat Gunakan metadata instans untuk mengelola instans EC2.

Instans Linux

Pertama, hubungkan ke instans berjalan Anda. Dari instans, gunakan kueri ini untuk mendapatkan pemetaan perangkat blok.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

Responsnya mencakup nama-nama perangkat blok untuk instans tersebut. Misalnya, output untuk instans yang didukung oleh instans `m1.small` yang didukung penyimpanan instans terlihat seperti ini.

```
ami
ephemeral0
root
swap
```

`ami`Perangkat adalah volume root seperti yang terlihat oleh instance. Volume penyimpanan instans diberi nama `ephemeral[0-23]`. Parameter perangkat `swap` adalah untuk file halaman. Jika Anda juga telah memetakan volume EBS, volume tersebut muncul sebagai `ebs1`, `ebs2`, dan seterusnya.

Untuk mendapatkan detail tentang perangkat blok individu dalam pemetaan perangkat blok, tambahkan namanya ke kueri sebelumnya, seperti yang ditunjukkan di sini.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Instans Windows

Pertama, hubungkan ke instans berjalan Anda. Dari instans, gunakan kueri ini untuk mendapatkan pemetaan perangkat blok.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/
```

Responsnya mencakup nama-nama perangkat blok untuk instans tersebut. Misalnya, output untuk instans yang didukung oleh instans `m1.small` yang didukung penyimpanan instans terlihat seperti ini.

```
ami
ephemeral0
root
swap
```

`ami`Perangkat adalah volume root seperti yang terlihat oleh instance. Volume penyimpanan instans diberi nama `ephemeral[0-23]`. Parameter perangkat `swap` adalah untuk file halaman. Jika Anda juga telah memetakan volume EBS, volume tersebut muncul sebagai `ebs1`, `ebs2`, dan seterusnya.

Untuk mendapatkan detail tentang perangkat blok individu dalam pemetaan perangkat blok, tambahkan namanya ke kueri sebelumnya, seperti yang ditunjukkan di sini.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Cara volume dilampirkan dan dipetakan untuk instans Windows Amazon EC2

> **Note**
>
> Topik ini hanya berlaku untuk instance Windows.

Instans Windows Anda dilengkapi dengan volume EBS yang berfungsi sebagai volume root. Jika instans Windows Anda menggunakan driver AWS PV atau Citrix PV, Anda dapat menambahkan hingga 25 volume secara opsional, membuat total 26 volume. Untuk informasi selengkapnya, lihat Batas volume Amazon EBS untuk instans Amazon EC2.

Bergantung pada tipe instans, Anda akan memiliki dari 0 hingga 24 kemungkinan volume penyimpanan instans yang tersedia untuk instans. Untuk menggunakan volume penyimpanan instans yang tersedia untuk instans, Anda harus menentukannya saat Anda membuat AMI atau meluncurkan instans. Anda juga dapat menambahkan volume EBS saat Anda membuat AMI atau meluncurkan instans, atau melampirkannya saat instans berjalan.

Saat Anda menambahkan volume ke instans, Anda menentukan nama perangkat yang digunakan Amazon EC2. Untuk informasi lebih lanjut, lihatNama perangkat untuk volume di EC2 instans Amazon. AWS Windows Amazon Machine Image (AMI) berisi sekumpulan driver yang digunakan oleh Amazon EC2 untuk memetakan instans store dan volume EBS ke disk Windows dan huruf drive.

Metode untuk memetakan disk ke volume EBS

- Peta disk NVMe di instans Windows Amazon EC2 ke volume
- Petakan disk non-NVME di instans Amazon EC2 Windows ke volume

Peta disk NVMe di instans Windows Amazon EC2 ke volume

Dengan instans berbasis Nitro, volume EBS diekspos sebagai perangkat. NVMe Topik ini menjelaskan cara melihat NVMe disk yang tersedia untuk sistem operasi Windows pada instans Anda. Ini juga menunjukkan cara memetakan disk NVMe tersebut ke volume Amazon EBS yang mendasarinya dan nama perangkat yang ditentukan untuk pemetaan perangkat blok yang digunakan oleh Amazon EC2.

Topik

- Daftar NVMe disk
- Peta NVMe disk ke volume

Daftar NVMe disk

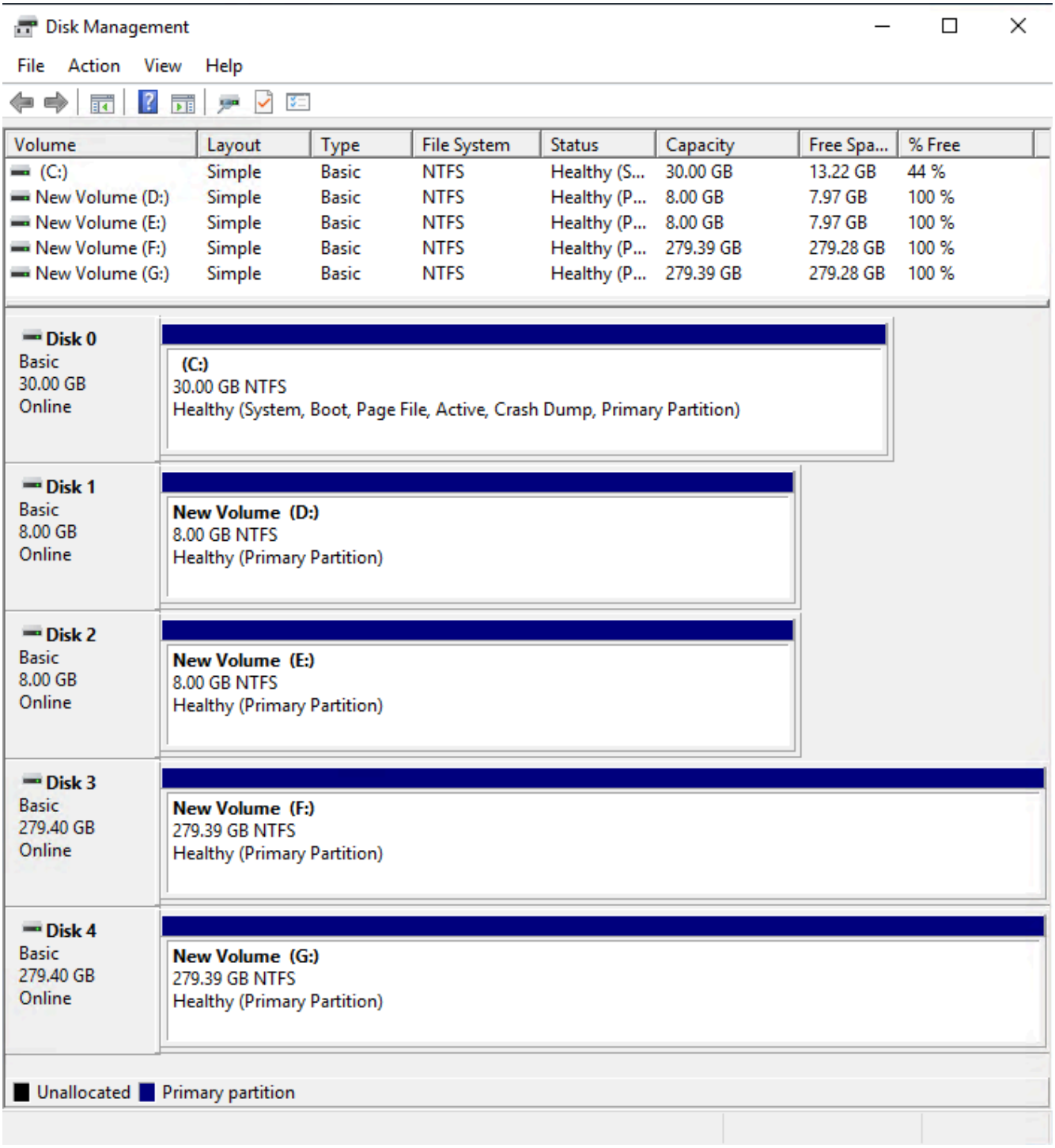
Anda dapat menemukan disk di instans Windows menggunakan Manajemen Disk atau Powershell.

Disk Management

Untuk menemukan disk di instans Windows Anda

1. Masuk ke instans Windows menggunakan Remote Desktop. Untuk informasi selengkapnya, lihat Hubungkan ke instans Windows Anda menggunakan RDP.
2. Mulai utilitas Manajemen Disk.
3. Tinjau disk. Volume root adalah volume EBS yang dipasang sebagai `C:\`. Jika tidak ada disk lain yang ditampilkan, berarti Anda tidak menentukan volume tambahan saat membuat AMI atau meluncurkan instans.

   Berikut ini adalah contoh yang menunjukkan disk yang tersedia jika Anda meluncurkan instans `r5d.4xlarge` dengan dua volume EBS tambahan.



PowerShell

PowerShell Skrip berikut mencantumkan setiap disk dan nama dan volume perangkat yang sesuai. Ini dimaksudkan untuk digunakan dengan instance berbasis Nitro, yang menggunakan volume penyimpanan NVMe EBS dan instance.

Hubungkan ke instans Windows Anda dan jalankan perintah berikut untuk mengaktifkan PowerShell pelaksanaan skrip.

```
Set-ExecutionPolicy RemoteSigned
```

Salin skrip berikut dan simpan sebagai `mapping.ps1` di instans Windows Anda.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber =  (Get-Disk -Path $Path).Number
```

```
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
      VolumeName= $VolumeName
    }
 $Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Jalankan skrip sebagai berikut:

```
PS C:\> .\mapping.ps1
```

Berikut ini adalah contoh output untuk sebuah instans dengan volume root, dua volume EBS, dan dua volume penyimpanan instans.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Jika Anda tidak mengonfigurasi kredensi Anda untuk Alat untuk Windows PowerShell pada instance Windows, skrip tidak dapat memperoleh ID volume EBS dan digunakan N/A di kolom. `EbsVolumeId`

Peta NVMe disk ke volume

Anda dapat menggunakan perintah Get-Disk untuk memetakan nomor disk Windows ke volume Amazon EBS dan volume penyimpanan instans Amazon EC2.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                    HealthStatus
 OperationalStatus      Total Size Partition

                      Style
------ ------------- -------------                    ------------
 -----------------      ---------- ----------
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy              Online
              279.4 GB MBR
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy              Online
              279.4 GB MBR
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy              Online
                  8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy              Online
                 30 GB MBR
```

```
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy             Online
                  8 GB MBR
```

Anda juga dapat menjalankan ebsnvme-id perintah untuk memetakan nomor NVMe disk ke volume EBS IDs dan nama perangkat.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Petakan disk non-NVME di instans Amazon EC2 Windows ke volume

Untuk instance yang diluncurkan dari AMI Windows yang menggunakan driver AWS PV atau Citrix PV, Anda dapat menggunakan hubungan yang dijelaskan di halaman ini untuk memetakan disk Windows ke penyimpanan instans dan volume EBS Anda. Topik ini menjelaskan cara melihat NVMe non-disk yang tersedia untuk sistem operasi Windows pada instance Anda. Ini juga menunjukkan cara memetakan disk non-NVME tersebut ke volume Amazon EBS yang mendasarinya dan nama perangkat yang ditentukan untuk pemetaan perangkat blok yang digunakan oleh Amazon EC2.

> **Note**
>
> Jika Anda meluncurkan instance Jika AMI Windows Anda menggunakan driver Red Hat PV, Anda dapat memperbarui instans Anda untuk menggunakan driver Citrix. Untuk informasi selengkapnya, lihat the section called “Mutakhirkan driver PV”.

Topik

- Daftar non- NVMe disk
- Petakan NVMe non-disk ke volume

Daftar non- NVMe disk

Anda dapat menemukan disk pada instance Windows Anda menggunakan Manajemen Disk atau PowerShell.

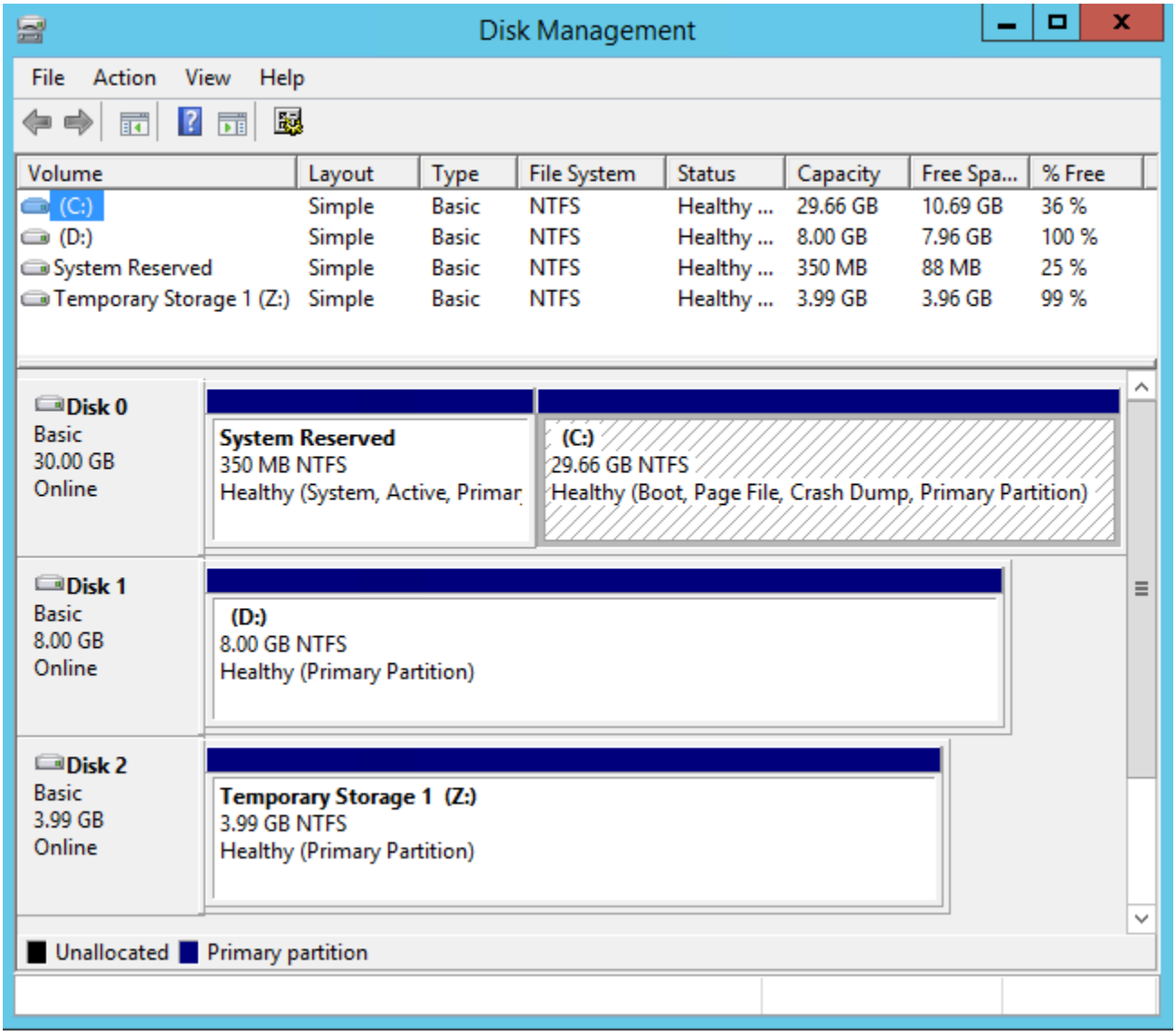
Disk Management

Untuk menemukan disk di instans Windows Anda

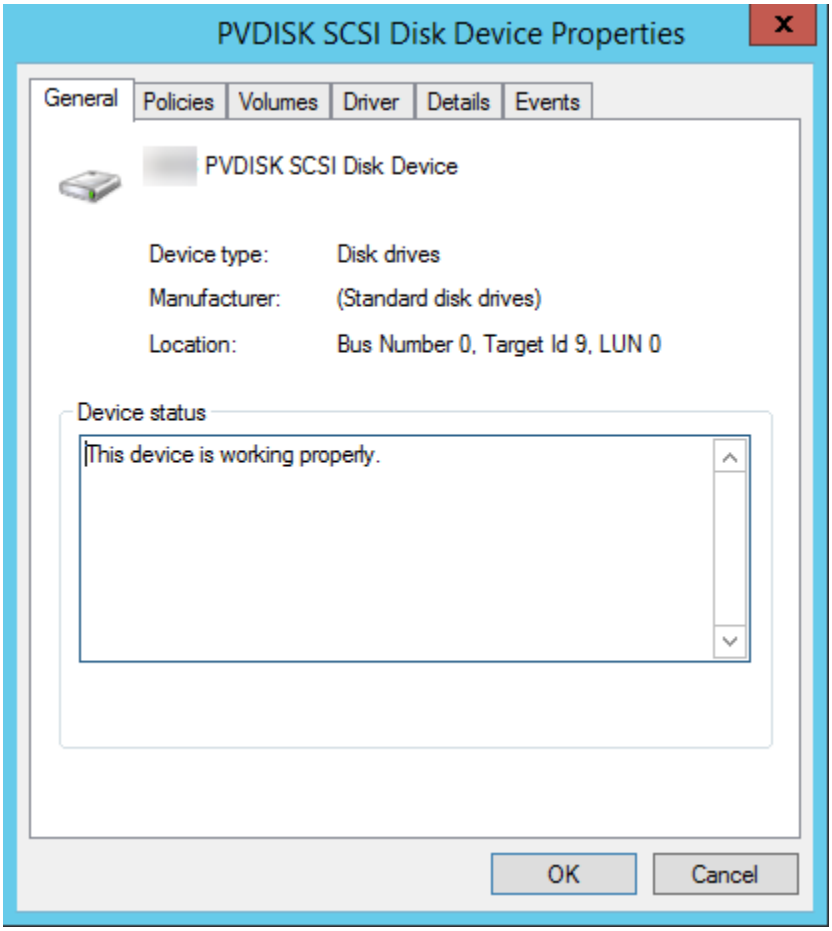
1. Masuk ke instans Windows menggunakan Remote Desktop. Untuk informasi selengkapnya, lihat Hubungkan ke instans Windows Anda menggunakan RDP.
2. Mulai utilitas Manajemen Disk.

   Pada bilah tugas, klik kanan logo Windows, lalu pilih Manajemen Disk.
3. Tinjau disk. Volume root adalah volume EBS yang dipasang sebagai `C:\`. Jika tidak ada disk lain yang ditampilkan, berarti Anda tidak menentukan volume tambahan saat membuat AMI atau meluncurkan instans.

   Berikut ini adalah instans yang menunjukkan disk yang tersedia jika Anda meluncurkan instans `m3.medium` dengan volume penyimpanan instans (Disk 2) dan volume EBS tambahan (Disk 1).



4. Klik kanan panel abu-abu dengan label Disk 1, lalu pilih Properti. Perhatikan nilai Lokasi dan cari dalam tabel di Petakan NVMe non-disk ke volume. Misalnya, disk berikut memiliki lokasi Nomor Bus 0, Target Id 9, LUN 0. Menurut tabel untuk volume EBS, nama perangkat untuk lokasi ini adalah `xvdj`.



PowerShell

PowerShell Skrip berikut mencantumkan setiap disk dan nama dan volume perangkat yang sesuai.

Persyaratan dan batasan

- Memerlukan Windows Server 2012 atau yang lebih baru.
- Memerlukan kredensial untuk mendapatkan ID volume EBS. Anda dapat mengonfigurasi profil menggunakan Alat untuk PowerShell, atau melampirkan peran IAM ke instance.
- Tidak mendukung NVMe volume.
- Tidak mendukung disk dinamis.

Hubungkan ke instans Windows Anda dan jalankan perintah berikut untuk mengaktifkan PowerShell pelaksanaan skrip.

```
Set-ExecutionPolicy RemoteSigned
```

Salin skrip berikut dan simpan sebagai `mapping.ps1` di instans Windows Anda.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}

[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).SerialNumber) -replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -
ExpandProperty SystemName
```

```
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-
EC2InstanceMetadata CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and
 Metadata is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}

Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*"
 + $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
```

```
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping")."ephemeral$((Get-WmiObject -Class Win32_Diskdrive | Where-
Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)"
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  Else {
    $BlockDeviceName = $null
```

```
    $BlockDevice = $null
  }
  New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
 { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
  }
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Jalankan skrip sebagai berikut:

```
PS C:\> .\mapping.ps1
```

Berikut ini adalah output contoh.

```
Disk  Partitions  DriveLetter   EbsVolumeId             Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------             ------      -------------
 ----------              ----------
   0           1            C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1            D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1            E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Jika Anda tidak memberikan kredensi Anda pada instance Windows, skrip tidak bisa mendapatkan ID volume EBS dan digunakan N/A di kolom. `EbsVolumeId`

Petakan NVMe non-disk ke volume

Driver perangkat blok untuk instans menetapkan nama volume aktual saat melakukan pemasangan volume.

Pemetaan

- Volume penyimpanan instans
- EBS volume

Volume penyimpanan instans

Tabel berikut menjelaskan bagaimana driver Citrix PV dan AWS PV memetakan volume penyimpanan NVMe non-instance ke volume Windows. Jumlah volume penyimpanan instans yang tersedia ditentukan oleh tipe instans. Untuk informasi selengkapnya, lihat Batas volume penyimpanan instans untuk instans EC2.

Lokasi	Nama perangkat
Nomor Bus 0, ID Target 78, LUN 0	xvdca
Nomor Bus 0, ID Target 79, LUN 0	xvdcb
Nomor Bus 0, ID Target 80, LUN 0	xvdcc
Nomor Bus 0, ID Target 81, LUN 0	xvdcd
Nomor Bus 0, ID Target 82, LUN 0	xvdce
Nomor Bus 0, ID Target 83, LUN 0	xvdcf
Nomor Bus 0, ID Target 84, LUN 0	xvdcg
Nomor Bus 0, ID Target 85, LUN 0	xvdch
Nomor Bus 0, ID Target 86, LUN 0	xvdci
Nomor Bus 0, ID Target 87, LUN 0	xvdcj
Nomor Bus 0, ID Target 88, LUN 0	xvdck
Nomor Bus 0, ID Target 89, LUN 0	xvdcl

EBS volume

Tabel berikut menjelaskan bagaimana driver Citrix PV dan PV memetakan AWS volume EBS non-NVME ke volume Windows.

Lokasi	Nama perangkat
Nomor Bus 0, ID Target 0, LUN 0	/dev/sda1
Nomor Bus 0, ID Target 1, LUN 0	xvdb
Nomor Bus 0, ID Target 2, LUN 0	xvdc
Nomor Bus 0, ID Target 3, LUN 0	xvdd
Nomor Bus 0, ID Target 4, LUN 0	xvde
Nomor Bus 0, ID Target 5, LUN 0	xvdf
Nomor Bus 0, ID Target 6, LUN 0	xvdg
Nomor Bus 0, ID Target 7, LUN 0	xvdh
Nomor Bus 0, ID Target 8, LUN 0	xvdi
Nomor Bus 0, ID Target 9, LUN 0	xvdj
Nomor Bus 0, ID Target 10, LUN 0	xvdk
Nomor Bus 0, ID Target 11, LUN 0	xvdl
Nomor Bus 0, ID Target 12, LUN 0	xvdm
Nomor Bus 0, ID Target 13, LUN 0	xvdn
Nomor Bus 0, ID Target 14, LUN 0	xvdo
Nomor Bus 0, ID Target 15, LUN 0	xvdp
Nomor Bus 0, ID Target 16, LUN 0	xvdq
Nomor Bus 0, ID Target 17, LUN 0	xvdr

Lokasi	Nama perangkat
Nomor Bus 0, ID Target 18, LUN 0	xvds
Nomor Bus 0, ID Target 19, LUN 0	xvdt
Nomor Bus 0, ID Target 20, LUN 0	xvdu
Nomor Bus 0, ID Target 21, LUN 0	xvdv
Nomor Bus 0, ID Target 22, LUN 0	xvdw
Nomor Bus 0, ID Target 23, LUN 0	xvdx
Nomor Bus 0, ID Target 24, LUN 0	xkertas
Nomor Bus 0, ID Target 25, LUN 0	xvdz

Pencegahan menulis robek pada instans Amazon EC2 Linux

> **Note**
>
> Pencegahan penulisan robek hanya didukung dengan instance Linux.

Pencegahan penulisan robek adalah fitur penyimpanan blok yang dirancang AWS untuk meningkatkan kinerja beban kerja database relasional intensif I/O Anda dan mengurangi latensi tanpa berdampak negatif pada ketahanan data. Basis data relasional yang menggunakan InnoDB atau XtraDB sebagai mesin basis data, seperti MySQL dan MariaDB, akan mendapat manfaat dari pencegahan penulisan yang rusak.

Biasanya, basis data relasional yang menggunakan halaman yang lebih besar dari daya gagal atomisitas perangkat penyimpanan menggunakan mekanisme pencatatan data untuk melindungi dari tumpang tindih. MariaDB dan MySQL menggunakan file buffer doublewrite untuk mencatat data sebelum menulisnya ke tabel data. Jika terjadi penulisan yang tidak lengkap atau sobek, sebagai akibat dari kerusakan sistem operasi atau kehilangan daya selama transaksi penulisan, basis data dapat memulihkan data dari buffer penulisan ganda. I/O Overhead tambahan yang terkait dengan penulisan ke buffer doublewrite berdampak pada kinerja database dan latensi aplikasi, dan

mengurangi jumlah transaksi yang dapat diproses per detik. Untuk informasi selengkapnya tentang buffer doublewrite, lihat dokumentasi MariaDB dan MySQL.

Dengan pencegahan penulisan robek, data ditulis ke penyimpanan dalam transaksi all-or-nothingtulis, yang menghilangkan kebutuhan untuk menggunakan buffer doublewrite. Hal ini mencegah data parsial, atau tumpang tindih, ditulis ke penyimpanan jika terjadi crash sistem operasi atau kehilangan daya selama transaksi tulis. Jumlah transaksi yang diproses per detik dapat ditingkatkan hingga 30 persen, dan latensi penulisan dapat dikurangi hingga 50 persen, tanpa mengorbankan ketahanan beban kerja Anda.

Harga

Tidak ada biaya tambahan untuk menggunakan pencegahan tumpang tindih.

Daftar Isi

- Ukuran blok untuk pencegahan menulis sobek di Amazon EC2
- Persyaratan untuk menggunakan pencegahan tulis sobek di Amazon EC2
- Periksa dukungan EC2 instans Amazon untuk pencegahan penulisan sobek
- Konfigurasikan beban kerja Anda di Amazon EC2 untuk pencegahan penulisan sobek

Ukuran blok untuk pencegahan menulis sobek di Amazon EC2

Pencegahan tumpang tindih mendukung operasi penulisan untuk blok data 4 KiB, 8 KiB, dan 16 KiB. Alamat blok logis awal blok data (LBA) harus disejajarkan dengan ukuran batas blok masing-masing yaitu 4 KiB, 8 KiB, atau 16 KiB. Misalnya, untuk operasi penulisan 16 KiB, LBA awal blok data harus disejajarkan dengan ukuran batas blok 16 KiB.

Tabel berikut menunjukkan dukungan di seluruh tipe penyimpanan dan instans.

	4 KiB blok	8 KiB blok	16 KiB blok
Volume penyimpanan instans	Semua volume penyimpanan NVMe instans yang dilampirkan ke instance i-Family generasi saat ini.	Instans i4i, iM4GN, IS4gen, i7i, i7ie, i8G, dan i8GE yang didukung oleh Nitro SSD. AWS	

	4 KiB blok	8 KiB blok	16 KiB blok
Volume Amazon EBS	Semua volume Amazon EBS dilampirkan ke instans berbasis Nitro.		

Untuk mengonfirmasi apakah instans dan volume Anda mendukung pencegahan tumpang tindih, lakukan kueri untuk memeriksa apakah instans mendukung pencegahan penulisan sobek dan detail lainnya, seperti ukuran blok dan batas yang didukung. Untuk informasi selengkapnya, lihat Periksa dukungan EC2 instans Amazon untuk pencegahan penulisan sobek.

Persyaratan untuk menggunakan pencegahan tulis sobek di Amazon EC2

Agar pencegahan penulisan robek berfungsi dengan baik, I/O operasi harus memenuhi persyaratan ukuran, keselarasan, dan batas, sebagaimana ditentukan dalam, bidang. `NTWPU` `NTWGU` `NTWBU` Anda harus mengonfigurasi sistem operasi Anda untuk memastikan bahwa subsistem penyimpanan tertentu (sistem file, LVM, RAID, dll) tidak mengubah I/O properti di tumpukan penyimpanan, termasuk penggabungan blok, pemisahan, atau relokasi alamat blok, sebelum dikirim ke perangkat.

Pencegahan tumpang tinding telah diuji dengan konfigurasi berikut:

- Tipe instans dan tipe penyimpanan yang mendukung ukuran blok yang diperlukan.
- Amazon Linux 2 dengan kernel versi 5.10 atau yang lebih baru.
- ext4 dengan `bigalloc` diaktifkan dan ukuran klaster 16 KiB, serta utilitas ext4 terbaru (e2fsprogs 1.46.5 atau yang lebih baru).
- mode akses file `O_DIRECT` untuk melakukan bypass cache buffer kernel Linux.

> **Note**
>
> Anda tidak perlu menonaktifkan I/O penggabungan untuk beban kerja MySQL dan MariaDB.

Periksa dukungan EC2 instans Amazon untuk pencegahan penulisan sobek

Untuk mengonfirmasi apakah instans dan volume Anda mendukung pencegahan penulisan robek, dan untuk melihat data spesifik vendor NVMe namespace yang berisi informasi pencegahan penulisan yang robek, gunakan perintah berikut.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> Perintah ini mengembalikan informasi khusus vendor dalam heksa dengan interpretasi ASCII. Anda mungkin perlu membuat alat yang mirip dengan `ebsnvme-id`, ke dalam aplikasi Anda yang dapat membaca dan mengurai output.

Misalnya, perintah berikut mengembalikan data spesifik vendor NVMe namespace yang berisi informasi pencegahan penulisan yang robek. `/dev/nvme1n1`

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Jika instans dan volume Anda mendukung pencegahan penulisan yang robek, ini mengembalikan informasi pencegahan penulisan AWS robek berikut di data spesifik vendor NVMe namespace.

> **Note**
>
> Byte dalam tabel berikut mewakili offset dalam byte dari awal data spesifik vendor NVMe namespace.

Byte	Deskripsi
`0:31`	Nama titik pemasangan lampiran perangkat, misalnya `/dev/xvda` . Anda memberikan ini selama permintaan lampiran volume dan dapat digunakan oleh EC2 instance Amazon untuk membuat symlink ke perangkat NVMe blok (`nvmeXn1`).

Byte	Deskripsi
32:63	ID volume. Misalnya, `vol01234567890abcdef` . Bidang ini dapat digunakan untuk memetakan NVMe perangkat ke volume terlampir.
64:255	Terpesan untuk digunakan di masa mendatang.
256:257	Ukuran Unit Pencegahan Tumpang Tindih Namespace (NTWPU). Bidang ini menunjukkan ukuran spesifik ruang nama dari operasi penulisan yang dijamin akan ditulis secara atomik ke NVM selama terjadi kegagalan daya atau kondisi kesalahan. Bidang ini ditentukan dalam blok logis yang direpresentasikan dalam nilai berbasis nol.
258:259	Ukuran Perincian Pencegahan Tumpang Tindih Namespace (NTWPG). Bidang ini menunjukkan kenaikan ukuran spesifik namespace di bawah `NTWPU` operasi tulis yang dijamin akan ditulis secara atomik ke NVM selama kegagalan daya atau kondisi kesalahan. Artinya, ukuran harus `NTWPG * n <= NTWPU`, yaitu n adalah bilangan bulat positif. Operasi tulis offset LBA juga harus diselaraskan dengan bidang ini. Bidang ini ditentukan dalam blok logis yang direpresentasikan dalam nilai berbasis nol.
260:263	Ukuran Batas Pencegahan Tumpang Tindih Namespace (NTWPB). Bidang ini menunjukkan ukuran batas atom untuk namespace ini untuk nilai `NTWPU`. Menulis ke namespace ini yang melintasi batas atom tidak dijamin akan ditulis secara atomik ke NVM selama kondisi kegagalan daya atau kesalahan. Nilai `0h` menunjukkan bahwa tidak ada batas atomis untuk kegagalan daya atau kondisi kesalahan. Semua nilai lainnya menentukan ukuran dalam hal blok logis menggunakan pengodean yang sama dengan bidang `NTWPU`.

Konfigurasikan beban kerja Anda di Amazon EC2 untuk pencegahan penulisan sobek

Pencegahan tumpang tindih diaktifkan secara default pada tipe instans yang didukung dengan volume yang didukung. Anda tidak perlu mengaktifkan pengaturan tambahan apa pun untuk mengaktifkan volume atau instans Anda untuk pencegahan tumpang tindih.

> **Note**
>
> Tidak ada dampak performa pada beban kerja yang tidak mendukung pencegahan tumpang tindih. Anda tidak perlu melakukan perubahan apa pun untuk beban kerja ini.
> Beban kerja yang mendukung pencegahan tumpang tindih, tetapi tidak dikonfigurasi untuk menggunakannya, terus menggunakan buffer penulisan ganda dan tidak menerima manfaat performa apa pun.

Untuk mengonfigurasi tumpukan perangkat lunak MySQL atau MariaDB Anda guna menonaktifkan buffer penulisan ganda dan menggunakan pencegahan tumpang tindih, selesaikan langkah-langkah berikut:

1. Konfigurasikan volume Anda untuk menggunakan sistem file ext4 dengan BigAlloc opsi dan atur ukuran cluster ke 4 KiB, 8 KiB, atau 16 KiB. Menggunakan BigAlloc dengan ukuran cluster 4 KiB, 8 KiB, atau 16 KiB memastikan bahwa sistem file mengalokasikan file yang sejajar dengan batas masing-masing.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > Untuk MySQL dan MariaDB, Anda harus menggunakan `-C 16384` untuk mencocokkan ukuran halaman basis data. Mengatur perincian alokasi ke nilai selain kelipatan ukuran halaman dapat mengakibatkan alokasi yang mungkin tidak cocok dengan batasan pencegahan tumpang tindih pada perangkat penyimpanan.

   Misalnya:

   ```
   $  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
   ```

2. Konfigurasikan InnoDB untuk menggunakan metode flush `O_DIRECT` dan matikan doublewrite InnoDB. Gunakan editor teks pilihan Anda untuk membuka `/etc/my.cnf`, dan perbarui parameter `innodb_flush_method` dan `innodb_doublewrite` sebagai berikut:

   ```
   innodb_flush_method=O_DIRECT
   ```

```
innodb_doublewrite=0
```

Important

Jika Anda menggunakan Logical Volume Manager (LVM) atau lapisan virtualisasi penyimpanan lainnya, pastikan offset awal volume disejajarkan pada kelipatan 16 KiB. Ini relatif terhadap NVMe penyimpanan yang mendasari untuk memperhitungkan header metadata dan superblok yang digunakan oleh lapisan virtualisasi penyimpanan. Jika Anda menambahkan offset ke volume fisik LVM, itu dapat menyebabkan ketidaksejajaran antara alokasi sistem file dan offset NVMe perangkat, yang akan membatalkan pencegahan penulisan robek. Untuk informasi selengkapnya, lihat `--dataalignmentoffset` di halaman manual Linux.

Snapshot Amazon EBS berbasis Windows VSS yang konsisten dengan aplikasi

Anda dapat mengambil snapshot yang konsisten dengan aplikasi dari semua volume Amazon EBS yang dilampirkan ke instans Windows Amazon EC2 Anda menggunakan Run Command.AWS Systems Manager Proses snapshot menggunakan Layanan Salinan Snapshot (VSS) Volume Windows untuk melakukan pencadangan tingkat volume EBS pada aplikasi sadar VSS. Snapshot mencakup data dari transaksi yang tertunda antara aplikasi ini dan disk. Anda tidak perlu mematikan instans atau memutusnya saat Anda perlu mencadangkan semua volume yang terlampir.

Tidak ada biaya tambahan untuk menggunakan snapshot EBS berbasis VSS. Anda hanya perlu membayar snapshot EBS yang dibuat oleh proses pencadangan. Untuk informasi selengkapnya, lihat Bagaimana cara saya ditagih untuk snapshot Amazon EBS saya?

Note

Snapshot berbasis Windows VSS yang konsisten aplikasi hanya didukung dengan instance Windows.

Daftar Isi

- Apa itu VSS?

- Cara kerja solusi snapshot Amazon EBS berbasis VSS
- Prasyarat untuk membuat snapshot EBS berbasis Windows VSS
- Buat snapshot EBS berbasis VSS untuk instans Windows EC2 Anda
- Memecahkan masalah snapshot EBS berbasis Windows VSS
- Gunakan solusi AWS VSS untuk memulihkan data untuk instans Anda
- AWS riwayat versi VSS solution

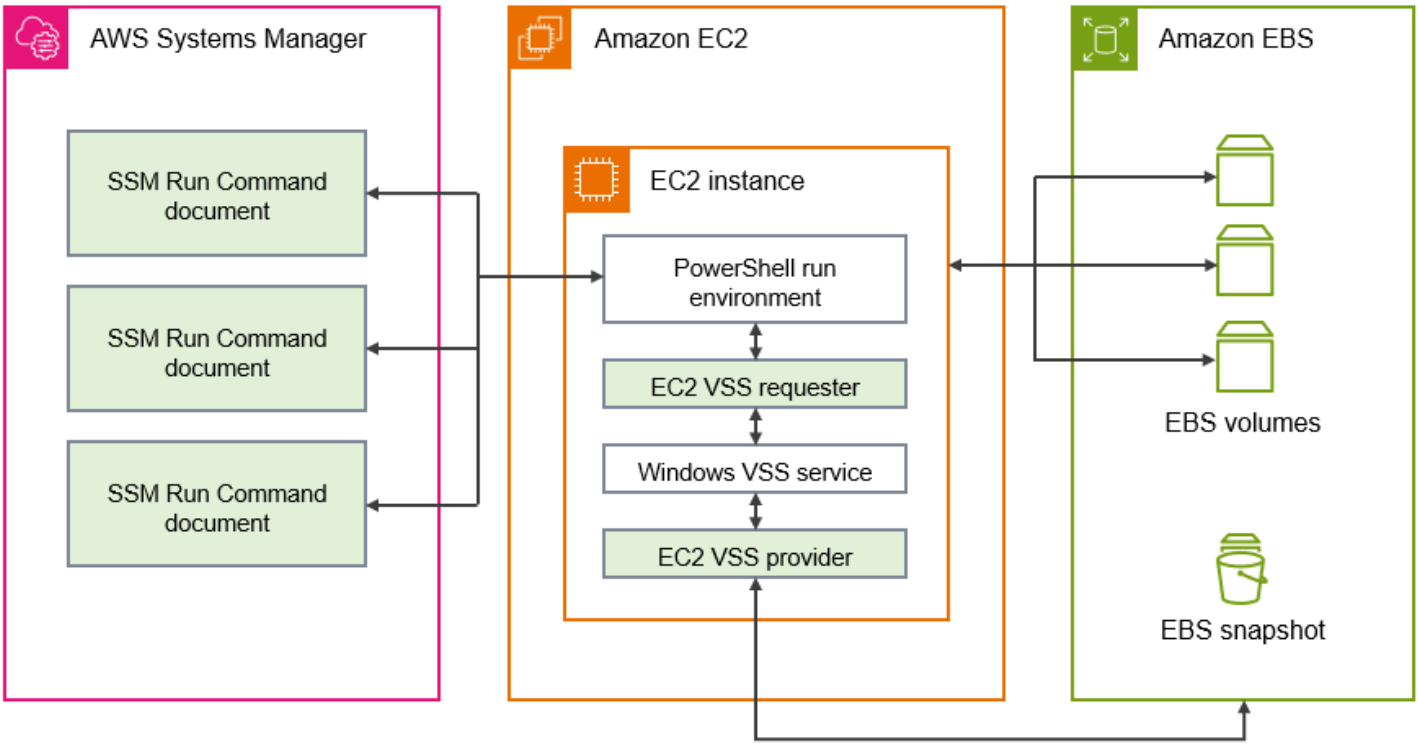
Apa itu VSS?

Volume Shadow Copy Service (VSS) adalah teknologi cadangan dan pemulihan yang termasuk dalam Microsoft Windows. Layanan ini dapat membuat salinan cadangan, atau snapshot dari file komputer atau volume saat sedang digunakan. Untuk informasi selengkapnya, lihat Layanan Salinan Snapshot Volume.

Untuk membuat snapshot yang konsisten dengan aplikasi, komponen perangkat lunak berikut ini terlibat.

- Layanan VSS — Bagian dari sistem operasi Windows
- Pemohon VSS — Perangkat lunak yang meminta pembuatan salinan bayangan
- Penulis VSS — Biasanya disediakan sebagai bagian dari aplikasi, seperti SQL Server, untuk memastikan set data yang konsisten untuk dicadangkan
- Penyedia VSS — Komponen yang membuat salinan bayangan dari volume yang mendasarinya

Solusi snapshot Amazon EBS berbasis Windows VSS terdiri dari beberapa dokumen Run Command Systems Manager (SSM) yang memfasilitasi pembuatan cadangan, dan paket Distributor Systems Manager, yang disebut*`AwsVssComponents`*, yang mencakup pemohon VSS EC2 dan penyedia VSS EC2. Paket `AwsVssComponents` harus diinstal pada instans Windows EC2 untuk mengambil snapshot volume EBS yang konsisten dengan aplikasi. Diagram berikut menggambarkan hubungan antara komponen perangkat lunak ini.



Cara kerja solusi snapshot Amazon EBS berbasis VSS

Proses untuk mengambil skrip snapshot EBS berbasis VSS yang konsisten aplikasi terdiri dari langkah-langkah berikut.

1. Selesaikan Prasyarat untuk membuat snapshot EBS berbasis Windows VSS.
2. Masukkan parameter untuk dokumen SSM `AWSEC2-VssInstallAndSnapshot` dan jalankan dokumen ini menggunakan Run Command. Untuk informasi selengkapnya, lihat Jalankan dokumen VssInstallAndSnapshot perintah AWSEC2 - (disarankan).
3. Layanan Windows VSS pada instans Anda mengoordinasikan semua I/O operasi yang sedang berlangsung untuk menjalankan aplikasi.
4. Sistem menyiram semua I/O buffer dan menghentikan sementara semua operasi. I/O Jeda bertahan, paling sering, sepuluh detik.
5. Selama jeda, sistem membuat snapshot dari semua volume yang terlampir pada instans.
6. Jeda diangkat dan I/O melanjutkan operasi.
7. Sistem menambahkan semua snapshot yang baru dibuat ke daftar snapshot EBS. Sistem menandai semua snapshot EBS berbasis VSS yang berhasil dibuat oleh proses ini dengan:true. AppConsistent

8. Jika Anda perlu memulihkan dari snapshot, Anda dapat menggunakan proses EBS standar untuk membuat volume dari snapshot, atau Anda dapat memulihkan semua volume ke instans dengan menggunakan skrip contoh, seperti yang dijelaskan dalam Gunakan solusi AWS VSS untuk memulihkan data untuk instans Anda.

Prasyarat untuk membuat snapshot EBS berbasis Windows VSS

Anda dapat membuat snapshot EBS berbasis VSS dengan Systems Manager Run Command AWS Backup, atau Amazon Data Lifecycle Manager. Prasyarat berikut berlaku untuk semua solusi.

Persyaratan sistem

Pastikan instans EC2 Windows Anda memenuhi semua persyaratan sistem untuk membuat snapshot berbasis VSS, termasuk versi yang didukung dari sistem operasi Windows, .NET framework, PowerShell AWS Tools for Windows PowerShell, dan Agen. AWS Systems Manager

Izin IAM

Peran IAM yang dilampirkan ke instans Amazon EC2 Windows Anda harus memiliki izin untuk membuat snapshot yang konsisten dengan aplikasi dengan VSS. Untuk memberikan izin yang diperlukan, Anda dapat melampirkan kebijakan `AWSEC2VssSnapshotPolicy` terkelola ke profil instans Anda.

Komponen VSS

Untuk membuat snapshot yang konsisten aplikasi pada sistem operasi Windows, paket `AwsVssComponents` harus diinstal pada instans. Paket ini berisi Agen VSS EC2 pada instans yang berfungsi sebagai pemohon VSS, dan penyedia VSS EC2 untuk volume EBS.

Persyaratan sistem

Instal Agen Systems Manager

VSS diatur oleh Agen Systems Manager menggunakan. PowerShell Pastikan Anda telah menginstal SSM Agent versi `3.0.502.0` atau versi yang lebih baru pada instans EC2 Anda. Jika Anda sudah menggunakan SSM Agent versi lama, perbarui menggunakan Run Command. Untuk informasi selengkapnya, lihat Menyiapkan Systems Manager untuk instans Amazon EC2 dan Bekerja dengan SSM Agent di instans Amazon EC2 untuk Windows Server di Panduan Pengguna AWS Systems Manager .

Persyaratan instans Windows Amazon EC2

Snapshot EBS berbasis VSS didukung untuk instance yang menjalankan Windows Server 2016 dan yang lebih baru.

Versi .NET Framework

Paket `AwsVssComponents` membutuhkan .NET Framework versi `4.6` atau yang lebih baru. Versi sistem operasi Windows sebelum Windows Server 2016 default ke versi sebelumnya dari .NET Framework. Jika instans Anda menggunakan versi sebelumnya dari .NET Framework, Anda harus menginstal versi `4.6` atau yang lebih baru menggunakan Windows Update.

AWS Tools for Windows PowerShell versi

Pastikan instans Anda menjalankan AWS Tools for Windows PowerShell versi `3.3.48.0` atau yang lebih baru. Untuk memeriksa versi Anda, jalankan perintah berikut di PowerShell terminal pada instance.

```
C:\> Get-AWSPowerShellVersion
```

Jika Anda perlu memperbarui AWS Tools for Windows PowerShell instans Anda, lihat Menginstal AWS Tools for Windows PowerShell di Panduan AWS Tools for PowerShell Pengguna.

PowerShell Versi Windows

Pastikan instans Anda menjalankan Windows versi PowerShell mayor`3`,`4`, atau`5`. Untuk memeriksa versi Anda, jalankan perintah berikut di PowerShell terminal pada instance.

```
C:\> $PSVersionTable.PSVersion
```

PowerShell modus bahasa

Pastikan instans Anda memiliki mode PowerShell bahasa yang disetel ke`FullLanguage`. Untuk informasi selengkapnya, lihat about_Language_Modes di dokumentasi Microsoft.

Menggunakan kebijakan terkelola IAM untuk memberikan izin untuk snapshot berbasis VSS

Kebijakan AWSEC2VssSnapshotPolicy terkelola memungkinkan Systems Manager untuk melakukan tindakan berikut pada instans Windows Anda:

- Buat dan beri tag snapshot EBS

- Membuat dan menandai Amazon Machine Images (AMIs)
- Lampirkan metadata, seperti ID perangkat, ke tag snapshot default yang dibuat VSS.

Topik ini mencakup detail izin untuk kebijakan terkelola VSS, dan cara melampirkannya ke peran IAM profil instans EC2 Anda.

Daftar Isi

- AWSEC2VssSnapshotPolicyrincian kebijakan terkelola
- Lampirkan kebijakan terkelola snapshot VSS ke peran profil instans Anda

AWSEC2VssSnapshotPolicyrincian kebijakan terkelola

Kebijakan AWS terkelola adalah kebijakan mandiri yang disediakan Amazon untuk AWS pelanggan. AWS kebijakan terkelola dirancang untuk memberikan izin untuk kasus penggunaan umum. Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Namun, Anda dapat menyalin kebijakan dan menggunakannya sebagai dasar untuk kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

Untuk menggunakan kebijakan AWSEC2VssSnapshotPolicyterkelola, Anda dapat melampirkannya ke peran IAM yang dilampirkan ke Instans Windows EC2 Anda. Kebijakan ini memungkinkan solusi EC2 VSS untuk membuat dan menambahkan tag ke Amazon Machine Images (AMIs) dan Snapshots EBS. Untuk melampirkan kebijakan, lihatLampirkan kebijakan terkelola snapshot VSS ke peran profil instans Anda.

Izin diberikan oleh AWSEC2VssSnapshotPolicy

AWSEC2VssSnapshotPolicyKebijakan ini mencakup izin Amazon EC2 berikut untuk mengizinkan Amazon EC2 membuat dan mengelola snapshot VSS atas nama Anda. Anda dapat melampirkan kebijakan terkelola ini ke peran profil instans IAM yang Anda gunakan untuk instans Windows EC2 Anda.

- ec2: CreateTags — Tambahkan tag ke snapshot EBS dan untuk membantu mengidentifikasi dan AMIs mengkategorikan sumber daya.
- ec2: DescribeInstanceAttribute — Ambil volume EBS dan pemetaan perangkat blok terkait yang dilampirkan ke instance target.

- ec2: CreateSnapshots — Buat snapshot volume EBS.
- ec2: CreateImage — Buat AMI dari instans EC2 yang sedang berjalan.
- ec2: DescribeImages — Ambil informasi untuk EC2 AMIs dan snapshot.
- ec2: DescribeSnapshots — Tentukan waktu pembuatan dan status snapshot untuk memverifikasi konsistensi aplikasi.

> **Note**
>
> Untuk melihat detail izin untuk kebijakan ini, lihat AWSEC2VssSnapshotPolicydi Referensi Kebijakan AWS Terkelola.

Merampingkan izin untuk kasus penggunaan tertentu - lanjutan

Kebijakan `AWSEC2VssSnapshotPolicy` terkelola menyertakan izin untuk semua cara Anda dapat membuat snapshot berbasis VSS. Anda dapat membuat kebijakan khusus yang hanya menyertakan izin yang Anda perlukan.

Kasus penggunaan: Buat AMI, Kasus penggunaan: Gunakan AWS Backup layanan

Jika Anda secara eksklusif menggunakan `CreateAmi` opsi, atau jika Anda membuat snapshot berbasis VSS hanya melalui AWS Backup layanan, maka Anda dapat merampingkan pernyataan kebijakan sebagai berikut.

- Menghilangkan pernyataan kebijakan yang diidentifikasi oleh pernyataan berikut IDs (SIDs):
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Sesuaikan `CreateTagsOnResourceCreation` pernyataan sebagai berikut:
  - Hapus `arn:aws:ec2:*:*:snapshot/*` dari sumber daya.
  - Hapus `CreateSnapshots` dari `ec2:CreateAction` kondisi.
- Sesuaikan `CreateTagsAfterResourceCreation` pernyataan untuk dihapus `arn:aws:ec2:*:*:snapshot/*` dari sumber daya.
- Sesuaikan `DescribeImagesAndSnapshots` pernyataan untuk dihapus `ec2:DescribeSnapshots` dari tindakan pernyataan.

Kasus penggunaan: Hanya snapshot

Jika Anda tidak menggunakan `CreateAmi` opsi, maka Anda dapat merampingkan pernyataan kebijakan sebagai berikut.

- Menghilangkan pernyataan kebijakan yang diidentifikasi oleh pernyataan berikut IDs (SIDs):
  - `CreateImageAccessInstance`
  - `CreateImageWithTag`
- Sesuaikan `CreateTagsOnResourceCreation` pernyataan sebagai berikut:
  - Hapus `arn:aws:ec2:*:*:image/*` dari sumber daya.
  - Hapus `CreateImage` dari `ec2:CreateAction` kondisi.
- Sesuaikan `CreateTagsAfterResourceCreation` pernyataan untuk dihapus `arn:aws:ec2:*:*:image/*` dari sumber daya.
- Sesuaikan `DescribeImagesAndSnapshots` pernyataan untuk dihapus `ec2:DescribeImages` dari tindakan pernyataan.

> **Note**
>
> Untuk memastikan bahwa kebijakan khusus Anda berjalan seperti yang diharapkan, kami sarankan Anda meninjau dan memasukkan pembaruan pada kebijakan terkelola secara berkala.

Lampirkan kebijakan terkelola snapshot VSS ke peran profil instans Anda

Untuk memberikan izin snapshot berbasis VSS untuk instans EC2 Windows, Anda dapat melampirkan kebijakan AWSEC2VssSnapshotPolicyterkelola ke peran profil instans Anda sebagai berikut. Penting untuk memastikan bahwa instans Anda memenuhi semuaPersyaratan sistem.

> **Note**
>
> Untuk menggunakan kebijakan terkelola, instans Anda harus memiliki versi `AwsVssComponents` paket `2.3.1` atau yang lebih baru diinstal. Untuk riwayat versi, lihatAwsVssComponents versi paket.

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.

2. Di panel navigasi, pilih Peran untuk melihat daftar peran IAM yang dapat Anda akses.
3. Pilih tautan nama peran untuk peran yang dilampirkan ke instance Anda. Ini membuka halaman detail peran.
4. Untuk melampirkan kebijakan terkelola, pilih Tambahkan izin, yang terletak di sudut kanan atas panel daftar. Kemudian pilih Lampirkan kebijakan dari daftar dropdown.
5. Untuk merampingkan hasil, masukkan nama kebijakan di bilah pencarian (`AWSEC2VssSnapshotPolicy`).
6. Pilih kotak centang di samping nama kebijakan yang akan dilampirkan, lalu pilih Tambahkan izin.

Kelola paket komponen VSS untuk snapshot EBS berbasis Windows VSS

Sebelum Anda membuat snapshot EBS berbasis VSS, pastikan Anda memiliki versi terbaru dari paket komponen VSS yang diinstal pada instance Windows Anda. Ada beberapa cara Anda dapat menginstal `AwsVssComponents` paket ke instance yang ada, sebagai berikut:

- (Direkomendasikan) Jalankan dokumen VssInstallAndSnapshot perintah AWSEC2 - (disarankan). Operasi ini secara otomatis menginstal atau memperbarui jika diperlukan setiap kali dijalankan.
- Instal komponen VSS secara manual pada instance EC2 Windows.
- Perbarui paket komponen VSS pada instans Windows EC2 Anda.

Anda juga dapat membuat AMI dengan EC2 Image Builder yang menggunakan komponen terkelola `aws-vss-components-windows` guna menginstal paket `AwsVssComponents` untuk gambar. Komponen yang dikelola menggunakan AWS Systems Manager Distributor untuk menginstal paket. Setelah Image Builder membuat gambar, setiap instans yang Anda luncurkan dari AMI terkait akan menginstal paket VSS di dalamnya. Untuk informasi selengkapnya tentang cara membuat AMI dengan paket VSS yang diinstal, lihat Komponen terkelola paket distributor untuk Windows di Panduan Pengguna EC2 Image Builder.

Daftar Isi

- Instal komponen VSS secara manual pada instance EC2 Windows
- Perbarui paket komponen VSS pada instans Windows EC2 Anda

Instal komponen VSS secara manual pada instance EC2 Windows

Instans EC2 Windows Anda harus memiliki komponen VSS yang diinstal sebelum Anda dapat membuat snapshot yang bersifat konsisten aplikasi dengan Systems Manager. Jika Anda tidak menjalankan dokumen perintah `AWSEC2-VssInstallAndSnapshot` untuk menginstal atau memperbarui paket secara otomatis setiap kali Anda membuat snapshot yang bersifat konsisten aplikasi, Anda harus menginstal paket secara manual.

Anda juga harus menginstal secara manual jika Anda berencana untuk menggunakan salah satu metode berikut guna membuat snapshot yang bersifat konsisten aplikasi dari instans EC2.

- Buat snapshot VSS menggunakan AWS Backup
- Membuat snapshot VSS menggunakan Amazon Data Lifecycle Manager

Jika Anda perlu melakukan instalasi manual, kami sarankan Anda menggunakan paket komponen AWS VSS terbaru untuk meningkatkan keandalan dan kinerja snapshot yang konsisten aplikasi pada instans Windows EC2 Anda.

> **Note**
>
> Untuk menginstal atau memperbarui paket `AwsVssComponents` secara otomatis setiap kali Anda membuat snapshot yang konsisten dengan aplikasi, sebaiknya gunakan Systems Manager untuk menjalankan dokumen `AWSEC2-VssInstallAndSnapshot`. Untuk informasi selengkapnya, lihat Jalankan dokumen VssInstallAndSnapshot perintah AWSEC2 - (disarankan).

Untuk menginstal komponen VSS pada instans Windows Amazon EC2, ikuti langkah-langkah untuk lingkungan pilihan Anda.

Console

Untuk memasang komponen VSS menggunakan Distributor SSM

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Jalankan Perintah.
3. Pilih Jalankan perintah.
4. Untuk dokumen Command, pilih tombol di sebelah AWS-configure AWSPackage.

5. Untuk Parameter perintah, lakukan hal berikut:

   a. Verifikasi bahwa Tindakan diatur menjadi Pasang.

   b. Untuk Nama, masukkan `AwsVssComponents`.

   c. Untuk Versi, masukkan versi atau kosongkan kolom sehingga System Manager menginstal versi terbaru.

6. Untuk Target, identifikasi instans di mana Anda ingin menjalankan operasi ini dengan menentukan tanda atau memilih instans secara manual.

   > **Note**
   >
   > Jika Anda memilih instans secara manual, dan instans yang ingin Anda lihat tidak disertakan dalam daftar, lihat Di Mana Instans Saya? dalam Panduan Pengguna AWS Systems Manager untuk kiat pemecahan masalah.

7. Untuk Parameter lainnya:

   - (Opsional) Untuk Komentar, ketik informasi tentang perintah ini.
   - Untuk Waktu habis (detik), tentukan jumlah detik untuk menunggu sistem sebelum gagal menjalankan perintah keseluruhan.

8. (Opsional) Untuk Kontrol laju:

   - Untuk Konkurensi, tentukan jumlah atau persentase instans untuk menjalankan perintah pada saat yang sama.

     > **Note**
     >
     > Jika Anda memilih target dengan memilih tanda Amazon EC2 dan Anda tidak yakin berapa banyak instans menggunakan tanda yang dipilih, batasi jumlah instans yang dapat menjalankan dokumen pada waktu yang sama dengan menentukan persentase.

   - Untuk Ambang kesalahan, tetapkan kapan harus berhenti menjalankan perintah pada instans lain setelah gagal pada jumlah atau persentase instans. Misalnya, jika Anda menentukan tiga kesalahan, Systems Manager berhenti mengirim perintah ketika kesalahan keempat diterima. Instans yang masih memproses perintah juga dapat mengirim kesalahan.

9. (Opsional) Untuk bagian Opsi output, jika Anda ingin menyimpan output perintah ke file, pilih kotak di samping Aktifkan penulisan ke bucket S3. Tentukan nama bucket dan nama prefiks (folder) (opsional).

   > **Note**
   >
   > Izin S3 yang memberikan kemampuan untuk menulis data ke bucket S3 berasal dari profil instans yang ditetapkan ke instans, bukan data pengguna yang melaksanakan tugas ini. Untuk informasi selengkapnya, lihat Mengonfigurasi izin instans EC2 di AWS Systems Manager Panduan Pengguna.

10. (Opsional) Tentukan opsi untuk Notifikasi SNS.

    Untuk informasi tentang konfigurasi notifikasi Amazon SNS untuk Run Command, lihat Mengonfigurasi Notifikasi Amazon SNS untuk AWS Systems Manager.

11. Pilih Jalankan.

AWS CLI

Gunakan prosedur berikut untuk mengunduh dan menginstal paket `AwsVssComponents` pada instans Anda dengan menggunakan Run Command dari AWS CLI. Paket menginstal dua komponen: pemohon VSS dan penyedia VSS. Sistem menyalin komponen ini ke direktori pada instans, lalu mendaftarkan penyedia DLL sebagai penyedia VSS.

Untuk menginstal paket VSS

Jalankan perintah berikut untuk mengunduh dan menginstal komponen VSS yang diperlukan untuk System Manager.

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "i-1234567890abcdef0" \
    --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Gunakan prosedur berikut untuk mengunduh dan menginstal `AwsVssComponents` paket pada instance Anda dengan menggunakan Run Command dari Tools for Windows PowerShell. Paket

menginstal dua komponen: pemohon VSS dan penyedia VSS. Sistem menyalin komponen ini ke direktori pada instans, lalu mendaftarkan penyedia DLL sebagai penyedia VSS.

Untuk menginstal paket VSS

Jalankan perintah berikut untuk mengunduh dan menginstal komponen VSS yang diperlukan untuk System Manager.

```
Send-SSMCommand `
    -DocumentName "AWS-ConfigureAWSPackage" `
    -InstanceId "i-1234567890abcdef0" `
    -Parameter @{'action'='Install';'name'='AwsVssComponents'}
```

Verifikasi tanda tangan pada AWS komponen VSS

Gunakan prosedur berikut untuk memverifikasi tanda tangan pada paket `AwsVssComponents`.

1. Hubungkan ke instans Windows Anda. Untuk informasi selengkapnya, lihat Hubungkan ke instans Windows Anda menggunakan RDP.
2. Arahkan ke C:\Program Files\ Amazon\AwsVssComponents.
3. Buka menu konteks (klik kanan) untuk `ec2-vss-agent.exe`, lalu pilih Properti.
4. Arahkan ke tab Tanda Tangan Digital dan verifikasi bahwa nama penandatangan adalah Amazon Web Services Inc.
5. Gunakan langkah-langkah sebelumnya untuk memverifikasi tanda tangan pada `Ec2VssInstaller` dan `Ec2VssProvider.dll`.

Perbarui paket komponen VSS pada instans Windows EC2 Anda

Kami merekomendasikan Anda untuk terus meningkatkan komponen VSS dengan versi terbaru yang direkomendasikan. Ada beberapa cara berbeda untuk memperbarui komponen saat versi baru paket `AwsVssComponents` dirilis.

Metode pembaruan

- Anda dapat mengulangi langkah-langkah yang dijelaskan Instal komponen VSS secara manual pada instance EC2 Windows saat versi baru komponen AWS VSS dirilis.

- Anda dapat mengonfigurasi kaitan Systems Manager State Manager untuk secara otomatis mengunduh dan menginstal komponen VSS baru atau yang diperbarui saat paket `AwsVssComponents` tersedia.
- Anda dapat menginstal atau memperbarui paket `AwsVssComponents` secara otomatis setiap kali Anda membuat snapshot yang konsisten dengan aplikasi, sebaiknya gunakan Systems Manager untuk menjalankan dokumen `AWSEC2-VssInstallAndSnapshot`.

> **Note**
>
> Kami sarankan Anda menggunakan Systems Manager untuk menjalankan dokumen perintah `AWSEC2-VssInstallAndSnapshot`, yang secara otomatis menginstal atau memperbarui paket `AwsVssComponents` sebelum membuat snapshot yang konsisten dengan aplikasi. Untuk informasi selengkapnya, lihat Jalankan dokumen VssInstallAndSnapshot perintah AWSEC2 - (disarankan).

Untuk membuat kaitan Systems Manager State Manager, ikuti langkah-langkah untuk lingkungan pilihan Anda.

Console

Saat Anda membuat asosiasi Manajer Negara Systems Manager, ada dua opsi untuk memperbarui `AwsVssComponents` paket, sebagai berikut:

Copot pemasangan dan instal ulang

Metode ini mengunduh dan menginstal paket tanpa prasyarat tambahan.

Pembaruan di tempat

Ini melakukan pembaruan di tempat untuk paket, dan memiliki prasyarat berikut:

- Versi Agen SSM yang diinstal pada instance harus versi `3.3.808.0` atau yang lebih baru. Untuk informasi selengkapnya, lihat Bekerja dengan SSM Agent di instans EC2 untuk Windows Server di Panduan Pengguna AWS Systems Manager .
- Jika ditentukan, versi `AwsVssComponents` paket harus versi `2.5.0` atau yang lebih baru. Versi sebelumnya tidak mendukung pembaruan di tempat.

> **Note**
>
> jika instans Anda tidak memenuhi prasyarat ini, pembaruan di tempat akan gagal. Gunakan opsi Uninstall dan instal ulang sebagai gantinya.

Untuk membuat asosiasi State Manager

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih State Manager.

   Atau, jika beranda Systems Manager terbuka terlebih dahulu, buka panel navigasi lalu pilih State Manager.
3. Pilih Buat asosiasi.
4. Di bidang Nama, masukkan nama deskriptif.
5. Dalam daftar Dokumen, pilih AWS-configure AWSPackage.
6. Di bagian Parameter, pilih Instal dari daftar Tindakan.
7. Untuk jenis Instalasi, pilih Uninstall dan instal ulang atau In-place update.
8. Di bidang Nama, masukkan `AwsVssComponents`. Anda dapat membuat bidang Versi dan Argumen Tambahan tetap kosong.
9. Di bagian Target, pilih opsi.

   > **Note**
   >
   > Jika Anda memilih untuk menargetkan instans dengan menggunakan tanda, dan Anda menentukan tanda yang memetakan ke instans Linux, kaitan berhasil pada instans Windows tetapi gagal pada instans Linux. Status keseluruhan asosiasi menunjukkan Gagal.
10. Di bagian Tentukan jadwal, pilih opsi.
11. Di bagian Opsi lanjutan, untuk Keparahan kepatuhan, pilih tingkat keparahan untuk kaitan. Untuk informasi selengkapnya, lihat Pelajari tentang kepatuhan asosiasi. Untuk Ubah Kalender, pilih kalender dengan perubahan yang telah dikonfigurasi sebelumnya. Untuk informasi selengkapnya, lihat tentang Kalender Perubahan AWS Systems Manager.
12. Untuk kontrol Tarif, lakukan hal berikut:

- Untuk Konkurensi, tentukan jumlah atau persentase dari simpul terkelola untuk menjalankan perintah pada saat yang sama.
- Untuk Ambang kesalahan, tentukan kapan harus berhenti menjalankan perintah pada simpul terkelola lain setelah gagal pada jumlah atau persentase simpul.

13. (Opsional) Untuk Opsi output, untuk menyimpan output perintah ke file, pilih Aktifkan output penulisan ke S3. Masukkan nama bucket dan prefiks (folder) di dalam kotak.
14. Pilih Buat asosiasi, lalu pilih Tutup. Sistem ini mencoba untuk membuat asosiasi pada instans dan segera menerapkan status.

> **Note**
>
> Jika instans EC2 untuk Windows Server menunjukkan status Gagal, verifikasi bahwa Agen SSM berjalan pada instance, dan verifikasi bahwa instance dikonfigurasi dengan peran AWS Identity and Access Management (IAM) untuk Systems Manager. Untuk informasi selengkapnya, lihat Menyiapkan AWS Systems Manager.

AWS CLI

Gunakan perintah create-association untuk memperbarui paket Distributor sesuai jadwal tanpa membuat aplikasi terkait offline. Hanya file baru atau yang diperbarui dalam paket yang diganti.

Untuk membuat asosiasi State Manager

Jalankan perintah berikut untuk membuat asosiasi. Nilai `--name`, nama dokumen, selalu `AWS-ConfigureAWSPackage`. Perintah berikut menggunakan kunci `InstanceIds` untuk menentukan instans target.

```
aws ssm create-association \
    --name "AWS-ConfigureAWSPackage" \
    --parameters action=Install,installationType="Uninstall and
 reinstall",name=AwsVssComponents \
    --targets Key=InstanceIds,Values=i-1234567890abcdef0,i-000011112222abcde
```

PowerShell

Untuk membuat asosiasi State Manager

Gunakan New- SSMAssociation cmdlet.

```
New-SSMAssociation `
    -Name "AWS-ConfigureAWSPackage" `
    -Parameter  @{
        "action" = "Install"
        "installationType" = "Uninstall and reinstall"
        "name" = "AwsVssComponents"
    } `
    -Target @{
        "Key" = "InstanceIds"
        "Values" = @("i-1234567890abcdef0", "i-000011112222abcde")
    }
```

Buat snapshot EBS berbasis VSS untuk instans Windows EC2 Anda

Setelah Anda memenuhi semuaPrasyarat untuk membuat snapshot EBS berbasis Windows VSS, Anda dapat menggunakan salah satu metode berikut untuk membuat snapshot berbasis VSS dari instans EC2 Anda.

AWS Systems Manager dokumen perintah

Gunakan dokumen perintah Systems Manageruntuk membuat snapshot berbasis VSS.

Untuk mengotomatiskan backup, Anda dapat membuat tugas jendela AWS Systems Manager pemeliharaan yang menggunakan dokumen perintah. `AWSEC2-VssInstallAndSnapshot` Untuk informasi selengkapnya, lihat Bekerja dengan Jendela Pemeliharaan (Konsol) dalam Panduan Pengguna AWS Systems Manager .

AWS Backup

Anda dapat membuat cadangan VSS saat menggunakan AWS Backup dengan mengaktifkan VSS di konsol atau CLI. Untuk informasi selengkapnya, lihat Membuat cadangan VSS Windows di Panduan Developer AWS Backup .

> **Note**
>
> AWS Backup tidak secara otomatis menginstal `AwsVssComponents` paket pada instance Anda. Anda harus melakukan instalasi manual pada instans. Untuk informasi selengkapnya, lihat Instal komponen VSS secara manual pada instance EC2 Windows.

Amazon Data Lifecycle Manager

Anda dapat membuat snapshot VSS menggunakan Amazon Data Lifecycle Manager dengan mengaktifkan skrip pra dan pasca dalam kebijakan siklus hidup snapshot Anda. Untuk informasi selengkapnya, lihat Mengotomatiskan snapshot yang konsisten dengan aplikasi di Panduan Pengguna Amazon EBS.

> **Note**
>
> Amazon Data Lifecycle Manager tidak secara otomatis menginstal paket `AwsVssComponents` pada instans Anda. Anda harus melakukan instalasi manual pada instans. Untuk informasi selengkapnya, lihat Instal komponen VSS secara manual pada instance EC2 Windows.

Gunakan dokumen perintah Systems Manager untuk membuat snapshot berbasis VSS

Anda dapat menggunakan dokumen AWS Systems Manager perintah untuk membuat snapshot berbasis VSS. Konten berikut memperkenalkan dokumen perintah yang tersedia, dan parameter runtime yang digunakan dokumen tersebut untuk membuat snapshot Anda.

Sebelum Anda menggunakan salah satu dokumen perintah Systems Manager, pastikan bahwa Anda telah memenuhi semua Prasyarat untuk membuat snapshot EBS berbasis Windows VSS.

Topik

- Parameter untuk dokumen snapshot VSS Systems Manager
- Jalankan dokumen perintah snapshot VSS Systems Manager

Parameter untuk dokumen snapshot VSS Systems Manager

Dokumen Systems Manager yang membuat snapshot VSS semuanya menggunakan parameter berikut, kecuali jika diberi catatan:

AmiName(string, opsional)

Jika CreateAmiopsi disetel ke`True`, tentukan nama AMI yang dibuat cadangan.

description (string, opsional)

Tentukan deskripsi untuk snapshot atau gambar yang dibuat proses ini.

CollectDiagnosticLogs(string, opsional)

Untuk mengumpulkan informasi lebih lanjut selama langkah pembuatan snapshot dan AMI, atur parameter ini ke "`True`". Nilai default untuk parameter ini adalah "`False`". Log diagnostik terkonsolidasi disimpan sebagai arsip `.zip` format di lokasi berikut pada instans Anda:

`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`

CopyOnly(string, opsional)

Jika Anda menggunakan cadangan SQL Server asli selain AWS VSS, melakukan pencadangan khusus Salin mencegah AWS VSS memutus rantai cadangan diferensial asli. Untuk melakukan operasi pencadangan hanya-salin, atur parameter ini ke `True`.

Nilai default untuk parameter ini adalah`False`, yang menyebabkan AWS VSS melakukan operasi pencadangan penuh.

CreateAmi(string, opsional)

Untuk membuat Amazon Machine Image (AMI) berbasis VSS untuk mencadangkan instance Anda, setel parameter ini ke`True`. Nilai default untuk parameter ini adalah `False`, yang mencadangkan instans Anda dengan snapshot EBS sebagai gantinya.

Untuk informasi selengkapnya tentang cara membuat AMI dari suatu instans, lihat Buat AMI yang didukung Amazon EBS-Backed.

executionTimeout (string, opsional)

Tentukan waktu maksimum dalam hitungan detik untuk menjalankan proses pembuatan snapshot pada instans, atau untuk membuat AMI dari instans. Meningkatkan batas waktu ini memungkinkan perintah menunggu lebih lama hingga VSS memulai pembekuan dan melengkapi penandaan sumber daya yang dibuatnya. Batas waktu ini hanya berlaku untuk langkah pembuatan snapshot atau AMI. Langkah awal untuk menginstal atau memperbarui paket `AwsVssComponents` tidak termasuk dalam batas waktu.

ExcludeBootVolume(string, opsional)

Pengaturan ini mengecualikan volume boot dari proses pencadangan jika Anda membuat snapshot. Untuk mengecualikan volume boot dari snapshot Anda, atur ExcludeBootVolumeke`True`, dan CreateAmike`False`.

Jika Anda membuat AMI untuk cadangan Anda, parameter ini harus diatur ke `False`. Nilai default untuk parameter ini adalah `False`.

NoWriters(string, opsional)

Untuk mengecualikan penulis VSS aplikasi dari proses snapshot, atur parameter ini ke `True`. Ini dapat membantu Anda mengatasi konflik dengan komponen cadangan VSS pihak ketiga. Nilai default untuk parameter ini adalah `False`.

Jika `SaveVssMetadata` ya`True`, parameter ini harus diatur ke`False`.

SaveVssMetadata(string, opsional)

Untuk menyimpan file metadata VSS selama setiap snapshot, atur parameter ini ke. `True` Nilai default-nya adalah `False`. File-file ini membantu memberikan wawasan tentang komponen atau penulis mana yang disertakan dalam operasi pencadangan, dan file serta volume terkait untuk setiap snapshot. File metadata digunakan saat memulihkan database SQL menggunakan solusi pemulihan VSS. Untuk informasi selengkapnya tentang cara memulihkan database SQL dari snapshot VSS, lihat Menggunakan runbook otomatisasi untuk memulihkan database Anda dari AWS snapshot solusi VSS.

File metadata memiliki id set snapshot terkait dalam namanya. Anda dapat menemukannya di lokasi berikut di instans Anda:

```
C:\ProgramData\Amazon\AwsVss\VssMetadata\
```

Warning

- Menyimpan file metadata VSS memerlukan `AwsVssComponents` paket versi 2.4.0 atau yang lebih baru. Jika instans Anda memiliki versi sebelumnya yang diinstal, pengaturan `SaveVssMetadata` untuk `True` menyebabkan pembuatan snapshot gagal.
- `SaveVssMetadata`Parameter `NoWriters` dan saling eksklusif. Jika keduanya disetel ke `True` maka pembuatan snapshot gagal.

tanda (string, opsional)

Kami menyarankan Anda menandai snapshot dan gambar Anda untuk membantu Anda menemukan dan mengelola sumber daya Anda, misalnya, untuk memulihkan volume dari daftar snapshot. Sistem menambahkan `Name` kunci, dengan nilai kosong di mana Anda dapat menentukan nama yang ingin Anda terapkan ke snapshot atau gambar keluaran Anda.

Jika Anda ingin menentukan tag tambahan, pisahkan tag dengan titik koma di antaranya. Misalnya, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

> **Note**
>
> Kunci dan nilai tag hanya boleh berisi karakter alfanumerik dan karakter khusus berikut:. `() ./\-"'@_+:={}`

Secara default, sistem menambahkan tag cadangan berikut untuk snapshot dan gambar berbasis VSS.

- Perangkat — Untuk snapshot berbasis VSS, ini adalah nama perangkat dari volume EBS yang ditangkap snapshot.
- AppConsistent— Tag ini menunjukkan keberhasilan pembuatan snapshot berbasis VSS atau AMI.
- AwsVssConfig— Ini mengidentifikasi snapshot dan AMIs yang dibuat dengan VSS diaktifkan. Tag mencakup informasi meta seperti `AwsVssComponents` versi, dan ID Set Snapshot.

> **Warning**
>
> Menentukan salah satu tag cadangan ini dalam daftar parameter Anda akan menyebabkan kesalahan.

VssVersion(string, opsional)

Khusus untuk dokumen `AWSEC2-VssInstallAndSnapshot`, Anda dapat menentukan parameter `VssVersion` guna menginstal versi paket `AwsVssComponents` tertentu pada instans. Biarkan parameter ini kosong untuk menginstal versi default yang direkomendasikan.

Jika versi paket `AwsVssComponents` yang ditentukan sudah diinstal, skrip melewatkan langkah penginstalan dan melanjutkan ke langkah pencadangan. Untuk daftar versi `AwsVssComponents` paket dan dukungan operasi, lihat AWS riwayat versi VSS solution.

Jalankan dokumen perintah snapshot VSS Systems Manager

Anda dapat membuat snapshot EBS berbasis VSS dengan dokumen AWS Systems Manager perintah sebagai berikut.

Jalankan dokumen VssInstallAndSnapshot perintah AWSEC2 - (disarankan)

Saat Anda menggunakan AWS Systems Manager untuk menjalankan `AWSEC2-VssInstallAndSnapshot` dokumen, skrip menjalankan langkah-langkah berikut.

1. Skrip terlebih dahulu menginstal atau memperbarui paket `AwsVssComponents` pada instans Anda, tergantung apakah sudah diinstal.
2. Skrip membuat snapshot yang konsisten dengan aplikasi setelah langkah pertama selesai.

Untuk menjalankan dokumen `AWSEC2-VssInstallAndSnapshot`, ikuti langkah-langkah untuk lingkungan pilihan Anda.

Console

Buat snapshot EBS berbasis VSS dari konsol

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Pilih Jalankan Perintah dari panel navigasi. Ini menunjukkan daftar perintah yang sedang berjalan di akun Anda, jika berlaku.
3. Pilih Jalankan perintah. Ini membuka daftar dokumen perintah yang dapat Anda akses.
4. Pilih `AWSEC2-VssInstallAndSnapshot` dari daftar dokumen perintah. Untuk merampingkan hasil, Anda dapat memasukkan semua atau sebagian dari nama dokumen. Anda juga dapat memfilter berdasarkan pemilik, berdasarkan jenis platform, atau dengan tanda.

   Saat Anda memilih dokumen perintah, detail terisi di bawah daftar.
5. Pilih `Default version at runtime` dari daftar Versi dokumen.
6. Konfigurasikan Parameter perintah untuk menentukan cara `AWSEC2-VssInstallAndSnapshot` akan menginstal paket `AwsVssComponents` dan membuat cadangan dengan snapshot VSS atau AMI. Untuk detail parameter, lihat Parameter untuk dokumen snapshot VSS Systems Manager.
7. Untuk pemilihan target, tentukan tanda atau pilih instans secara manual untuk mengidentifikasi instans untuk menjalankan operasi ini.

> **Note**
>
> Jika Anda memilih instans secara manual, dan instans yang ingin Anda lihat tidak disertakan dalam daftar, lihat Di Mana Instans Saya? untuk kiat pemecahan masalah.

8. Untuk parameter tambahan guna menentukan perilaku Run Command Systems Manager seperti Kontrol laju, masukkan nilai seperti yang dijelaskan dalam Menjalankan perintah dari konsol.
9. Pilih Jalankan.

   Jika berhasil, perintah tersebut akan mengisi daftar snapshot EBS dengan snapshot baru. Anda dapat menemukan snapshot ini di daftar snapshot EBS dengan mencari tanda yang Anda tentukan, atau dengan mencari `AppConsistent`. Jika pelaksanaan perintah gagal, lihat output perintah Systems Manager untuk detail tentang alasan pelaksanaan tersebut gagal. Jika perintah berhasil diselesaikan, tetapi pencadangan volume tertentu gagal, Anda dapat memecahkan masalah kegagalan tersebut dalam daftar volume EBS.

AWS CLI

Anda dapat menjalankan perintah berikut di AWS CLI untuk membuat snapshot EBS berbasis VSS dan mendapatkan status pembuatan snapshot Anda.

Buat snapshot EBS berbasis VSS

Jalankan perintah berikut untuk membuat snapshot EBS berbasis VSS. Untuk membuat snapshot, Anda harus mengidentifikasi instans dengan parameter `--instance-ids`. Untuk informasi selengkapnya tentang parameter lain yang dapat Anda gunakan, lihat Parameter untuk dokumen snapshot VSS Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

Jika berhasil, dokumen perintah tersebut mengisi daftar snapshot EBS dengan snapshot baru. Anda dapat menemukan snapshot ini di daftar snapshot EBS dengan mencari tanda yang Anda

tentukan, atau dengan mencari `AppConsistent`. Jika pelaksanaan perintah gagal, lihat output perintah untuk detail tentang alasan pelaksanaan tersebut gagal.

Dapatkan status perintah

Untuk mendapatkan status snapshot saat ini, jalankan perintah berikut menggunakan ID perintah yang dikembalikan dari send-command.

```
aws ssm get-command-invocation
 --instance-ids "i-01234567890abcdef" \
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Jalankan perintah berikut AWS Tools for Windows PowerShell untuk membuat snapshot EBS berbasis VSS dan dapatkan status runtime saat ini untuk pembuatan output Anda. Tentukan parameter yang dijelaskan dalam daftar sebelumnya untuk mengubah perilaku proses snapshot.

Buat snapshot EBS berbasis VSS dengan Tools untuk Windows PowerShell

Jalankan perintah berikut untuk membuat snapshot EBS berbasis VSS atau. AMIs

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Dapatkan status perintah

Untuk mendapatkan status snapshot saat ini, jalankan perintah berikut menggunakan ID perintah yang dikembalikan dari Send-SSMCommand.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

Jika berhasil, perintah tersebut akan mengisi daftar snapshot EBS dengan snapshot baru. Anda dapat menemukan snapshot ini di daftar snapshot EBS dengan mencari tanda yang Anda tentukan, atau dengan mencari `AppConsistent`. Jika pelaksanaan perintah gagal, lihat output perintah untuk detail tentang alasan pelaksanaan tersebut gagal.

Jalankan dokumen CreateVssSnapshot perintah AWSEC2 -

Untuk menjalankan dokumen `AWSEC2-CreateVssSnapshot`, ikuti langkah-langkah untuk lingkungan pilihan Anda.

Console

Buat snapshot EBS berbasis VSS dari konsol

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Pilih Jalankan Perintah dari panel navigasi. Ini menunjukkan daftar perintah yang sedang berjalan di akun Anda, jika berlaku.
3. Pilih Jalankan perintah. Ini membuka daftar dokumen perintah yang dapat Anda akses.
4. Pilih `AWSEC2-CreateVssSnapshot` dari daftar dokumen perintah. Untuk merampingkan hasil, Anda dapat memasukkan semua atau sebagian dari nama dokumen. Anda juga dapat memfilter berdasarkan pemilik, berdasarkan jenis platform, atau dengan tanda.

   Saat Anda memilih dokumen perintah, detail terisi di bawah daftar.
5. Pilih `Default version at runtime` dari daftar Versi dokumen.
6. Konfigurasikan Parameter perintah untuk menentukan cara `AWSEC2-CreateVssSnapshot` akan mencadangkan dengan snapshot VSS atau AMI. Untuk detail parameter, lihat Parameter untuk dokumen snapshot VSS Systems Manager.
7. Untuk pemilihan target, tentukan tanda atau pilih instans secara manual untuk mengidentifikasi instans untuk menjalankan operasi ini.

   > **Note**
   >
   > Jika Anda memilih instans secara manual, dan instans yang ingin Anda lihat tidak disertakan dalam daftar, lihat Di Mana Instans Saya? untuk kiat pemecahan masalah.
8. Untuk parameter tambahan guna menentukan perilaku Run Command Systems Manager seperti Kontrol laju, masukkan nilai seperti yang dijelaskan dalam Menjalankan perintah dari konsol.
9. Pilih Jalankan.

   Jika berhasil, perintah tersebut akan mengisi daftar snapshot EBS dengan snapshot baru. Anda dapat menemukan snapshot ini di daftar snapshot EBS dengan mencari tanda yang

Anda tentukan, atau dengan mencari `AppConsistent`. Jika pelaksanaan perintah gagal, lihat output perintah Systems Manager untuk detail tentang alasan pelaksanaan tersebut gagal. Jika perintah berhasil diselesaikan, tetapi pencadangan volume tertentu gagal, Anda dapat memecahkan masalah kegagalan tersebut dalam daftar volume EBS.

AWS CLI

Anda dapat menjalankan perintah berikut di AWS CLI untuk membuat snapshot EBS berbasis VSS.

Buat snapshot EBS berbasis VSS

Jalankan perintah berikut untuk membuat snapshot EBS berbasis VSS. Untuk membuat snapshot, Anda harus mengidentifikasi instans dengan parameter `--instance-ids`. Untuk informasi selengkapnya tentang parameter lain yang dapat Anda gunakan, lihat Parameter untuk dokumen snapshot VSS Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

Jika berhasil, dokumen perintah tersebut mengisi daftar snapshot EBS dengan snapshot baru. Anda dapat menemukan snapshot ini di daftar snapshot EBS dengan mencari tanda yang Anda tentukan, atau dengan mencari `AppConsistent`. Jika pelaksanaan perintah gagal, lihat output perintah untuk detail tentang alasan pelaksanaan tersebut gagal.

PowerShell

Jalankan perintah berikut dengan AWS Tools for Windows PowerShell untuk membuat snapshot EBS berbasis VSS.

Buat snapshot EBS berbasis VSS dengan Tools untuk Windows PowerShell

Jalankan perintah berikut untuk membuat snapshot EBS berbasis VSS. Untuk membuat snapshot, Anda harus mengidentifikasi instans dengan parameter `InstanceId`. Anda dapat menentukan lebih dari satu instans untuk membuat snapshot. Untuk informasi selengkapnya tentang parameter lain yang dapat Anda gunakan, lihat Parameter untuk dokumen snapshot VSS Systems Manager.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value'}
```

Jika berhasil, perintah tersebut akan mengisi daftar snapshot EBS dengan snapshot baru. Anda dapat menemukan snapshot ini di daftar snapshot EBS dengan mencari tanda yang Anda tentukan, atau dengan mencari `AppConsistent`. Jika pelaksanaan perintah gagal, lihat output perintah untuk detail tentang alasan pelaksanaan tersebut gagal. Jika perintah berhasil diselesaikan, tetapi pencadangan volume tertentu gagal, Anda dapat memecahkan masalah kegagalan dalam daftar snapshot EBS.

Jalankan dokumen perintah untuk Klaster Failover Windows dengan penyimpanan EBS bersama

Anda dapat menggunakan salah satu prosedur baris perintah yang dijelaskan di bagian sebelumnya untuk membuat snapshot berbasis VSS. Dokumen perintah (`AWSEC2-VssInstallAndSnapshot` atau `AWSEC2-CreateVssSnapshot`) harus berjalan pada simpul primer di klaster Anda. Dokumen akan gagal pada simpul sekunder karena tidak memiliki akses ke disk bersama. Jika primer dan sekunder Anda berubah secara dinamis, Anda dapat menjalankan dokumen AWS Systems Manager Run Command pada beberapa node dengan harapan bahwa perintah akan berhasil pada node primer dan gagal pada node sekunder.

> **Note**
>
> Untuk mengotomatiskan backup, Anda dapat membuat tugas jendela AWS Systems Manager pemeliharaan yang menggunakan dokumen. `AWSEC2-VssInstallAndSnapshot` Untuk informasi selengkapnya, lihat Bekerja dengan Jendela Pemeliharaan (Konsol) dalam Panduan Pengguna AWS Systems Manager .

Memecahkan masalah snapshot EBS berbasis Windows VSS

Sebelum Anda mencoba langkah pemecahan masalah lainnya, sebaiknya Anda memverifikasi detail berikut.

- Pastikan bahwa Anda telah memenuhi semua Prasyarat untuk membuat snapshot EBS berbasis Windows VSS.

- Verifikasi bahwa Anda menggunakan Dukungan versi Windows OS paket `AwsVssComponents` terbaru untuk sistem operasi Anda. Masalah yang Anda lihat mungkin telah diatasi di versi yang lebih baru.

Topik

- Periksa file log
- Kumpulkan log diagnostik tambahan
- Gunakan VSS pada instance dengan proxy yang dikonfigurasi
- Kesalahan: Koneksi pipa thaw kehabisan waktu, kesalahan pada thaw, batas waktu menunggu VSS Freeze, atau kesalahan batas waktu lainnya
- Kesalahan: Tidak dapat menginvokasi metode. Invokasi metode hanya didukung pada tipe inti dalam mode bahasa ini

Periksa file log

Jika mengalami masalah atau menerima pesan galat saat membuat snapshot EBS berbasis VSS, Anda dapat melihat output perintah di konsol Systems Manager.

Untuk dokumen Systems Manager yang membuat snapshot VSS, Anda dapat mengatur `CollectDiagnosticLogs` parameter ke "`True`" saat runtime. Ketika `CollectDiagnosticLogs` parameter diatur ke "`True`“, VSS mengumpulkan log tambahan untuk membantu dalam debugging. Untuk informasi selengkapnya, lihat Kumpulkan log diagnostik tambahan.

Jika Anda mengumpulkan log diagnostik, dokumen Systems Manager menyimpannya di instans Anda di lokasi berikut: `C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip` Default untuk `CollectDiagnosticLogs` parameter adalah "`False`”.

> **Note**
>
> Untuk bantuan debugging tambahan, Anda dapat mengirim `.zip` file ke Dukungan.

Log tambahan berikut tersedia, apakah Anda mengumpulkan log diagnostik atau tidak:

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

Anda juga dapat membuka aplikasi Event Viewer Windows dan memilih Log Windows, Aplikasi untuk melihat log tambahan. Untuk melihat peristiwa khusus dari Penyedia VSS Windows EC2 dan Layanan Salin Bayangan Volume, filter berdasarkan Sumber pada **`Ec2VssSoftwareProvider`** dan **`VSS`**.

Jika Anda menggunakan Systems Manager dengan titik akhir VPC, dan tindakan API send-command Systems Manager (Jalankan Perintah di konsol) gagal, verifikasi bahwa Anda mengonfigurasi titik akhir berikut dengan benar: com.amazonaws. ***`region`***.ec2.

Tanpa titik akhir Amazon EC2 ditentukan, panggilan untuk menghitung volume EBS terlampir gagal, yang menyebabkan perintah Systems Manager gagal. Untuk informasi selengkapnya tentang pengaturan titik akhir VPC dengan Systems Manager, lihat Buat Titik Akhir Virtual Private Cloud dalam Panduan Pengguna AWS Systems Manager .

Kumpulkan log diagnostik tambahan

Untuk mengumpulkan log diagnostik tambahan saat Anda menggunakan perintah kirim Systems Manager untuk menjalankan dokumen snapshot VSS, atur parameter `CollectDiagnosticLogs` input ke "`True`" saat runtime. Kami menyarankan Anda mengatur parameter ini ke "`True`" saat Anda memecahkan masalah.

Untuk melihat contoh baris perintah, pilih salah satu tab berikut.

AWS CLI

Contoh berikut menjalankan dokumen `AWSEC2-CreateVssSnapshot` Systems Manager di AWS CLI:

```
aws ssm send-command \
    --document-name "AWSEC2-CreateVssSnapshot" \
    --instance-ids "i-1234567890abcdef0" \
    --parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

Contoh berikut menjalankan dokumen `AWSEC2-CreateVssSnapshot` Systems Manager di PowerShell:

```
Send-SSMCommand `
    -DocumentName "AWSEC2-CreateVssSnapshot" `
    -InstanceId "i-1234567890abcdef0" `
    -Parameter @{'description'='Example - create diagnostic logs at
 runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

Gunakan VSS pada instance dengan proxy yang dikonfigurasi

Jika Anda mengalami masalah saat membuat snapshot EBS berbasis VSS pada instans yang menggunakan proxy untuk mencapai titik akhir EC2, verifikasi pengaturan berikut pada instans Anda:

- Verifikasi bahwa proxy dikonfigurasi sehingga titik akhir layanan EC2 di Region dan IMDS instans dapat dijangkau dengan menjalankan sebagai SYSTEM. AWS Tools for Windows PowerShell
- Untuk mendukung penggunaan proxy WinHTTP yang dikonfigurasi sistem, pastikan Anda telah menginstal `AwsVssComponents` versi terbaru pada instance Anda. Untuk informasi selengkapnya tentang mengonfigurasi proksi WinHTTP, lihat Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP) di situs web Microsoft.

Kesalahan: Koneksi pipa thaw kehabisan waktu, kesalahan pada thaw, batas waktu menunggu VSS Freeze, atau kesalahan batas waktu lainnya

Penyedia VSS Windows EC2 mungkin habis karena aktivitas atau layanan pada instance yang mencegah snapshot berbasis VSS berjalan tepat waktu. Windows VSS Framework menyediakan jendela 10 detik yang tidak dapat dikonfigurasi selama komunikasi ke sistem file dijeda. Selama waktu ini, `AWSEC2-CreateVssSnapshot` snapshot volume Anda.

Masalah-masalah berikut dapat menyebabkan EC2 Windows VSS Provider mengalami waktu habis selama snapshot:

- Berlebihan I/O ke volume
- Responsif lambat dari API EC2 pada instans
- Volume terfragmentasi

- Ketidakcocokan dengan beberapa perangkat lunak antivirus
- Masalah dengan penulis aplikasi VSS
- Ketika Module Logging diaktifkan untuk sejumlah besar PowerShell modul, itu dapat menyebabkan PowerShell skrip berjalan lambat

Sebagian besar masalah waktu habis yang terjadi saat Anda menjalankan dokumen perintah `AWSEC2-CreateVssSnapshot` berkaitan dengan beban kerja pada instans yang terlalu tinggi pada saat pencadangan. Tindakan berikut dapat membantu Anda mengambil snapshot dengan sukses:

- Coba lagi perintah `AWSEC2-CreateVssSnapshot` untuk melihat apakah upaya snapshot berhasil. Jika mencoba kembali berhasil dalam beberapa kasus, mengurangi beban instans mungkin membuat snapshot lebih berhasil.
- Tunggu beberapa saat untuk mendapatkan penurunan beban kerja pada instans, dan coba lagi perintah `AWSEC2-CreateVssSnapshot`. Atau, Anda dapat mencoba snapshot ketika instans diketahui berada di bawah tekanan rendah.
- Mencoba snapshot VSS saat perangkat lunak antivirus pada sistem dimatikan. Jika ini menyelesaikan masalah, lihat petunjuk perangkat lunak antivirus dan konfigurasikan untuk memungkinkan Snapshot VSS.
- Jika ada panggilan API Amazon EC2 bervolume tinggi di akun Anda dalam Wilayah yang sama tempat Anda menjalankan snapshot, throttling API mungkin menunda operasi snapshot. Untuk mengurangi dampak pelambatan, gunakan paket terbaru`AwsVssComponents`. Paket ini memanfaatkan tindakan API `CreateSnapshots` EC2 untuk mengurangi jumlah tindakan mutasi seperti pembuatan dan penandaan snapshot per volume.
- Jika Anda memiliki lebih dari satu skrip perintah `AWSEC2-CreateVssSnapshot` yang berjalan secara bersamaan, Anda dapat mengambil langkah berikut untuk mengurangi masalah konkurensi.
  - Pertimbangkan untuk menjadwalkan snapshot selama periode aktivitas API yang lebih rendah.
  - Jika Anda menggunakan Run Command di konsol Systems Manager (atau SendCommand di API) untuk menjalankan skrip perintah, Anda dapat menggunakan kontrol laju Systems Manager guna mengurangi konkurensi.

    Anda juga dapat menggunakan kontrol tingkat Systems Manager untuk mengurangi konkurensi untuk layanan seperti AWS Backup itu menggunakan Systems Manager untuk menjalankan skrip perintah.
- Jalankan perintah `vssadmin list writers` dalam shell dan lihat apakah laporan kesalahan dalam kolom Kesalahan terakhir lapangan untuk setiap penulis pada sistem. Jika ada penulis

melaporkan waktu habis, pertimbangkan untuk mencoba kembali snapshot ketika beban instans sedang rendah.

- Bila Anda menggunakan tipe instance yang lebih kecil *t2 | t3 | t3a* seperti.nano *t2 | t3 | t3a* atau.micro, batas waktu karena memori dan kendala CPU dapat terjadi. Tindakan berikut dapat membantu mengurangi masalah waktu habis.
  - Coba tutup aplikasi intensif memori atau CPU sebelum mengambil snapshot.
  - Coba ambil snapshot selama periode aktivitas instans yang lebih rendah.

Kesalahan: Tidak dapat menginvokasi metode. Invokasi metode hanya didukung pada tipe inti dalam mode bahasa ini

Anda akan mengalami kesalahan ini ketika mode PowerShell bahasa tidak diatur ke`FullLanguage`. Dokumen `AWSEC2-CreateVssSnapshot` SSM harus dikonfigurasi ke `FullLanguage` mode. PowerShell

Untuk memverifikasi mode bahasa, jalankan perintah berikut pada instance di PowerShell konsol:

```
$ExecutionContext.SessionState.LanguageMode
```

Untuk informasi selengkapnya, lihat about_Language_Modes di dokumentasi Microsoft.

Gunakan solusi AWS VSS untuk memulihkan data untuk instans Anda

Anda dapat memulihkan volume EBS untuk instance Windows dari snapshot berbasis VSS yang dibuat oleh solusi VSS. AWS Jika snapshot solusi AWS VSS Anda berisi cadangan database Microsoft SQL Server, Anda dapat memulihkan database menggunakan runbook Otomasi. `AWSEC2-RestoreSqlServerDatabaseWithVss` AWS Systems Manager

Runbook pemulihan database mengotomatiskan seluruh proses pemulihan, termasuk membuat volume dari snapshot dan melampirkannya ke instance. Otomatisasi memanfaatkan teknologi VSS untuk memulihkan database, memungkinkan Anda memulihkan tanpa menghentikan aplikasi SQL Server Anda atau memutuskan koneksi aktif apa pun.

Untuk petunjuk terperinci tentang cara menggunakan runbook database Microsoft SQL Server, lihat Mengembalikan dari snapshot berbasis VSS di Panduan Pengguna Microsoft SQL Server di Amazon EC2.

Kustomisasi skrip untuk memulihkan volume EBS dari snapshot AWS solusi VSS

Anda dapat menggunakan `RestoreVssSnapshotSampleScript.ps1` skrip sebagai model untuk membuat skrip kustom Anda sendiri yang mengembalikan volume EBS dari snapshot solusi AWS VSS. Skrip sampel melakukan tugas-tugas berikut:

- Menghentikan suatu instans
- Hapus semua drive yang ada dari instans (kecuali volume boot, jika dikecualikan)
- Membuat volume baru dari snapshot
- Melampirkan volume ke instans dengan menggunakan tanda ID perangkat di snapshot
- Memulai ulang instans.

> **Important**
>
> Skrip berikut ini memisahkan semua volume yang terlampir ke suatu instans, lalu membuat volume baru dari snapshot. Pastikan bahwa Anda telah mencadangkan instans' dengan benar. Volume lama tidak dihapus. Jika mau, Anda dapat mengedit skrip untuk menghapus volume lama.

Untuk mengembalikan volume dari snapshot EBS berbasis VSS

1. Unduh RestoreVssSnapshotSampleScriptfile.zip dan ekstrak konten file.
2. Buka `RestoreVssSnapshotSampleScript.ps1` di editor teks dan edit panggilan sampel di bagian bawah skrip dengan ID instans EC2 dan ID snapshot EBS yang valid, kemudian jalankan skrip dari PowerShell.

AWS riwayat versi VSS solution

Halaman ini mencakup catatan rilis berdasarkan versi untuk paket komponen AWS VSS, serta persyaratan versi komponen dan skrip untuk setiap versi Windows Server yang didukung.

Topik

- AwsVssComponents versi paket
- Dukungan versi Windows OS

AwsVssComponents versi paket

Tabel berikut menjelaskan versi yang dirilis dari paket komponen AWS VSS.

Versi	Detail	Tanggal rilis	Dapat Diunduh
2.5.1	Memperbaiki kasus di mana restorasi database SQL bisa gagal ketika parameter database target ditentukan.	13 Maret 2025	Ya
2.5.0	• Menambahkan kemampuan untuk membaca file metadata VSS dan mengembalikan database Microsoft SQL Server pada instance. Untuk informasi selengkapnya, lihat Memulihkan dari snapshot berbasis VSS di Panduan Pengguna Microsoft SQL Server di Amazon EC2. • Menambahkan dukungan untuk opsi pembaruan di tempat saat menginstal atau memutakhirkan paket. `AwsVssComponents`	Januari 17, 2025	Ya
2.4.0	Menambahkan kemampuan untuk menyimpan file metadata VSS pada pembuatan snapshot. Untuk mengaktifkan fitur ini, lihat SaveVssMetadata diParameter untuk dokumen snapshot VSS Systems Manager.	Oktober 7, 2024	Ya
2.3.3	Memperbarui agen VSS untuk memastikan bahwa `Ec2VssProvider` digunakan selama pembuatan snapshot.	Juni 25, 2024	Ya
2.3.2	Memperbaiki kasus di mana pendaftaran penyedia VSS tidak dihapus saat penghapusan instalasi.	9 Mei 2024	Ya

Versi	Detail	Tanggal rilis	Dapat Diunduh
2.3.1	Menambahkan tag default baru `AwsVssConfig` untuk mengidentifikasi snapshot dan AMIs dibuat oleh AWS VSS.	7 Maret 2024	Ya
2.2.1	• Menambahkan dukungan untuk menggunakan `DescribeInstanceAttribute` API. • Perbaikan bug dan peningkatan keandalan. • Dukungan usang untuk Windows Server 2012 dan 2012 R2. AWS Komponen VSS versi 2.2.1 instalasi pada Windows Server 2012 dan 2012 R2 akan gagal. AWS Komponen VSS versi 2.1.0 adalah versi terakhir yang mendukung Windows Server 2012 dan 2012 R2.	Januari 18, 2024	Ya
2.1.0	Menambahkan dukungan untuk menggunakan `CreateSnapshots` API.	6 November 2023	Ya
2.0.1	Dukungan tambahan untuk menggunakan pengaturan proksi WinHTTP.	26 Oktober 2023	Tidak
2.0.0	Menambahkan kemampuan ke komponen AWS VSS untuk membuat snapshot dan AMIs, yang memungkinkan kompatibilitas dengan logging PowerShell modul, logging blok skrip, dan fitur transkripsi.	28 April 2023	Tidak
1.3.2.0	Memperbaiki kasus di mana kegagalan instalasi tidak dilaporkan dengan benar.	10 Mei 2022	Tidak

Versi	Detail	Tanggal rilis	Dapat Diunduh
1.3.1.0	• Snapshot tetap gagal di pengendali domain dalam kaitannya dengan kesalahan logging penulis NTDS VSS. • Kesalahan agen VSS tetap saat menghapus pemasangan penyedia VSS versi 1.0.	6 Februari 2020	Ya
1.3.00	• Penebangan yang lebih baik dengan mengurangi kata benda yang tidak diinginkan. • Masalah wilayah diperbaiki selama instalasi. • Memperbaiki kode pengembalian untuk beberapa kondisi kesalahan pendaftaran penyedia. • Memperbaiki berbagai masalah instalasi.	19 Maret 2019	Tidak
1.2.00	• Menambahkan parameter baris perintah `-nw` (tidak-menulis) dan `-copy` (hanya-salinan) kepada agen. • Memperbaiki EventLog kesalahan yang disebabkan oleh panggilan alokasi memori yang tidak tepat.	15 November 2018	Tidak
1.1	Memperbaiki komponen AWS VSS yang digunakan secara tidak benar sebagai penyedia Backup dan Restore Windows default.	12 Desember 2017	Tidak
1.0	Rilis awal.	20 November 2017	Tidak

Dukungan versi Windows OS

Tabel berikut menunjukkan versi solusi AWS VSS mana yang harus Anda jalankan pada setiap versi Windows Server di Amazon EC2.

Versi Windows Server	AwsVssComponents versi	AWSEC2-nama VssInstallAndSnapshot versi	AWSEC2-nama CreateVssSnapshot versi
Windows Server 2025	default	default	default
Windows Server 2022	default	default	default
Windows Server 2019	default	default	default
Windows Server 2016	default	default	default
Windows Server 2012 R2	2.1.0	Tidak didukung	2012R2
Windows Server 2012	2.1.0	Tidak didukung	2012R2
Windows Server 2008 R2	1.3.1.0	Tidak didukung	2008R2

Penyimpanan objek, penyimpanan file, dan caching file di Amazon EC2

Penyimpanan file cloud adalah metode untuk menyimpan data di cloud yang menyediakan akses server dan aplikasi ke data melalui sistem file bersama. Kompatibilitas ini membuat penyimpanan file cloud ideal untuk beban kerja yang mengandalkan sistem file bersama dan menyediakan integrasi sederhana tanpa perubahan kode.

Ada banyak solusi penyimpanan file yang ada, mulai dari server file node tunggal pada instance komputasi menggunakan penyimpanan blok sebagai dasar tanpa skalabilitas atau sedikit redundansi untuk melindungi data, hingga solusi do-it-yourself berkerumun, hingga solusi yang dikelola sepenuhnya. Konten berikut memperkenalkan beberapa layanan penyimpanan yang disediakan oleh AWS untuk digunakan dengan EC2 instans Amazon.

Konten

- Gunakan Amazon S3 dengan instans Amazon EC2
- Menggunakan Amazon EFS dengan instans Amazon EC2 Linux
- Gunakan Amazon FSx dengan EC2 instans Amazon
- Menggunakan Cache File Amazon dengan EC2 instans Amazon

Gunakan Amazon S3 dengan instans Amazon EC2

Amazon Simple Storage Service (Amazon S3) adalah layanan penyimpanan objek yang menawarkan skalabilitas, ketersediaan data, keamanan, dan kinerja terdepan di industri. Anda dapat menggunakan Amazon S3 untuk menyimpan dan mengambil sejumlah data untuk berbagai kasus penggunaan, seperti data lake, situs web, backup, dan analisis data besar, dari EC2 instans Amazon atau dari mana saja melalui internet. Untuk informasi selengkapnya, lihat Apa itu Amazon S3?

Objek adalah entitas dasar yang disimpan di Amazon S3. Setiap objek yang disimpan di Amazon S3 dimuat dalam bucket. Bucket atau GA namespace Amazon S3 di tingkat tertinggi dan identifikasi akun yang bertanggung jawab atas penyimpanan tersebut. Bucket Amazon S3 mirip dengan nama domain internet. Objek yang disimpan di dalam bucket memiliki nilai kunci yang unik dan diambil menggunakan URL. Sebagai contoh, jika sebuah objek dengan nilai kunci `/photos/mygarden.jpg` disimpan di dalam bucket `amzn-s3-demo-bucket1`, objek tersebut dapat dialamatkan menggunakan URL `https://amzn-s3-demo-bucket1.s3.amazonaws.com/photos/mygarden.jpg`. Untuk informasi selengkapnya, lihat Cara kerja Amazon S3.

Contoh penggunaan

Mengingat manfaat Amazon S3 untuk penyimpanan, Anda mungkin memutuskan untuk menggunakan layanan ini untuk menyimpan file dan kumpulan data untuk digunakan dengan EC2 instance. Ada berbagai cara untuk memindahkan data ke dan dari Amazon S3 ke instans Anda. Selain contoh-contoh yang dibahas di bawah ini, ada berbagai alat yang telah ditulis orang yang dapat Anda gunakan untuk mengakses data Anda di Amazon S3 dari komputer atau instans Anda.

Jika Anda memiliki izin, Anda dapat menyalin file ke atau dari Amazon S3 dan instans Anda menggunakan salah satu metode berikut.

wget

> **Note**
>
> Metode ini hanya berfungsi untuk objek publik. Jika objek tidak publik, Anda menerima pesan `ERROR 403: Forbidden`. Jika Anda menerima kesalahan ini, Anda harus menggunakan konsol Amazon S3, AWS API AWS CLI, AWS SDK, atau AWS Tools for Windows PowerShell, dan Anda harus memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk Amazon S3 dan Mengunduh objek di Panduan Pengguna Amazon S3.

Utilitas wget adalah klien HTTP dan FTP yang memungkinkan Anda mengunduh objek publik dari Amazon S3. Utilitas ini diinstal secara default di Amazon Linux dan sebagian besar distribusi lainnya, dan dapat diunduh di Windows. Untuk mengunduh objek Amazon S3, gunakan perintah berikut, dengan mengganti URL objek yang akan diunduh.

```
[ec2-user ~]$ wget https://amzn-s3-demo-bucket.s3.amazonaws.com/path-to-file
```

PowerShell

Anda dapat menggunakan AWS Tools for Windows PowerShelluntuk memindahkan objek ke dan dari Amazon S3.

Gunakan Copy-S3Objectcmdlet untuk menyalin objek Amazon S3 ke instance Windows Anda sebagai berikut.

```
Copy-S3Object `
    -BucketName amzn-s3-demo-bucket `
```

```
    -Key path-to-file `
    -LocalFile my_copied_file.ext
```

Atau, Anda dapat membuka konsol Amazon S3 dengan menggunakan browser web pada instance Windows.

AWS CLI

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk mengunduh item terbatas dari Amazon S3 dan juga untuk mengunggah item. Untuk informasi selengkapnya, seperti cara menginstal dan mengonfigurasi alat, lihat halaman detail AWS Command Line Interface.

Perintah aws s3 cp mirip dengan perintah Unixcp. Anda dapat menyalin file dari Amazon S3 ke instans Anda, menyalin file dari instans ke Amazon S3, dan menyalin file dari satu lokasi Amazon S3 ke lokasi lainnya.

Gunakan perintah berikut untuk menyalin objek dari Amazon S3 ke instans Anda.

```
aws s3 cp s3://amzn-s3-demo-bucket/my_folder/my_file.ext my_copied_file.ext
```

Gunakan perintah berikut untuk menyalin objek dari instans Anda kembali ke Amazon S3.

```
aws s3 cp my_copied_file.ext s3://amzn-s3-demo-bucket/my_folder/my_file.ext
```

Perintah aws s3 sync dapat menyinkronkan seluruh bucket Amazon S3 ke lokasi direktori lokal. Ini dapat membantu untuk mengunduh kumpulan data dan menyimpan salinan lokal up-to-date dengan set jarak jauh. Jika Anda memiliki izin yang tepat pada bucket Amazon S3, Anda dapat mendorong direktori lokal Anda kembali ke cloud setelah selesai dengan membalikkan lokasi sumber dan tujuan dalam perintah.

Gunakan perintah berikut untuk mengunduh seluruh bucket Amazon S3 ke direktori lokal pada instans Anda.

```
aws s3 sync s3://amzn-s3-demo-source-bucket local_directory
```

Amazon S3 API

Jika Anda adalah developer, Anda dapat menggunakan API untuk mengakses data di Amazon S3. Anda dapat menggunakan API ini untuk membantu mengembangkan aplikasi Anda dan

mengintegrasikannya dengan yang lain APIs dan SDKs. Untuk informasi selengkapnya, lihat Contoh kode untuk Amazon S3 yang digunakan AWS SDKs di Referensi API Amazon Simple Storage Service.

Menggunakan Amazon EFS dengan instans Amazon EC2 Linux

> **Note**
>
> Amazon EFS tidak didukung pada instans Windows.

Amazon EFS menyediakan penyimpanan file yang dapat diskalakan untuk digunakan dengan Amazon EC2. Anda dapat menggunakan sistem file EFS sebagai sumber data umum untuk beban kerja dan aplikasi yang berjalan pada beberapa instans. Untuk informasi selengkapnya, silakan lihat halaman produk Amazon Elastic File System.

Tutorial ini menunjukkan cara membuat dan melampirkan sistem file Amazon EFS menggunakan wizard Amazon EFS Quick Create selama peluncuran instance. Untuk tutorial tentang cara membuat sistem file menggunakan konsol Amazon EFS, lihat Memulai Amazon Elastic File System di Panduan Pengguna Amazon Elastic File System.

> **Note**
>
> Ketika Anda membuat sistem file EFS menggunakan Pembuatan Cepat EFS, sistem file dibuat dengan pengaturan layanan yang direkomendasikan berikut ini:
>
> - Pencadangan otomatis diaktifkan.
> - Kelola target pemasangan di VPC yang dipilih.
> - Mode kinerja Tujuan Umum.
> - Mode throughput meledak.
> - Enkripsi data saat istirahat diaktifkan menggunakan kunci default Anda untuk Amazon EFS (`aws/elasticfilesystem`).
> - Manajemen siklus hidup Amazon EFS diaktifkan dengan kebijakan 30 hari.

Tugas

- Membuat sistem file EFS menggunakan Amazon EFS Quick Create
- Menguji sistem file EFS
- Menghapus sistem file EFS

Membuat sistem file EFS menggunakan Amazon EFS Quick Create

Anda dapat membuat sistem file EFS dan memasangnya ke instans saat meluncurkan instans menggunakan fitur Amazon EFS Quick Create dari wizard instans EC2 peluncuran Amazon.

Untuk membuat sistem file EFS menggunakan Amazon EFS Quick Create

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Pilih Luncurkan instans.
3. (Opsional) Di bawah Nama dan tanda, untuk Nama, masukkan nama untuk mengidentifikasi instans Anda.
4. Di bawah Aplikasi dan Gambar OS (Amazon Machine Image), pilih sistem operasi Linux, lalu untuk Amazon Machine Image (AMI), pilih AMI Linux.
5. Di bawah Tipe Instans, untuk Tipe Instans, pilih tipe instans atau pertahankan default.
6. Di bawah Pasangan kunci (login), untuk Nama pasangan kunci, pilih pasangan kunci yang sudah ada atau buat yang baru.
7. Di bawah Pengaturan jaringan, pilih Edit (di kanan), lalu untuk Subnet, pilih subnet.

   > **Note**
   >
   > Anda harus memilih subnet sebelum dapat menambahkan sistem file EFS.

8. Di bawah Konfigurasikan penyimpanan, pilih Edit (di kanan bawah), lalu lakukan hal berikut:

   a. Untuk sistem File, pastikan EFS dipilih, lalu pilih Buat sistem file bersama baru.

   b. Untuk nama sistem File masukkan nama untuk sistem file Amazon EFS, lalu pilih Buat sistem file.

   c. Untuk titik Mount, tentukan titik pemasangan khusus atau pertahankan default.

   d. Untuk mengaktifkan akses ke sistem file, pilih Secara otomatis membuat dan melampirkan grup keamanan. Dengan memilih kotak centang ini, grup keamanan berikut akan secara otomatis dibuat dan dilampirkan ke instance dan target pemasangan sistem file:

- Grup keamanan instans — Termasuk aturan keluar yang memungkinkan lalu lintas melalui port NFS 2049port, tetapi tidak menyertakan aturan masuk.
- Grup keamanan target mount sistem file – Termasuk aturan masuk yang mengizinkan lalu lintas melalui port NFS 2049 dari grup keamanan instans (dijelaskan di atas), dan aturan keluar yang mengizinkan lalu lintas melalui port NFS 2049.

> **Note**
>
> Atau, Anda dapat membuat dan melampirkan grup keamanan secara manual. Jika Anda ingin membuat dan memasang grup keamanan yang Secara otomatis buat dan lampirkan grup keamanan yang diperlukan.

e. Untuk secara otomatis memasang sistem file bersama saat instans diluncurkan, pilih Pasang sistem file bersama secara otomatis dengan melampirkan skrip data pengguna yang diperlukan. Untuk melihat data pengguna yang dibuat secara otomatis, perluas Detail lanjutan, dan gulir ke bawah ke Data pengguna.

> **Note**
>
> Jika Anda menambahkan data pengguna sebelum memilih kotak centang ini, data pengguna asli akan ditimpa oleh data pengguna yang dibuat secara otomatis.

9. Konfigurasikan pengaturan instans lain sesuai kebutuhan.
10. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

Menguji sistem file EFS

Anda dapat terhubung ke instans dan memverifikasi bahwa sistem file terpasang pada direktori yang Anda tentukan (misalnya, /mnt/efs).

Untuk memverifikasi bahwa sistem file terpasang

1. Connect ke instans Anda. Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..

2. Dari jendela terminal untuk instans, jalankan perintah df -T untuk memverifikasi bahwa sistem file EFS sudah terpasang.

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted
 on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

   Perhatikan bahwa nama sistem file, yang ditunjukkan dalam contoh output sebagai*efs-dns*, memiliki bentuk berikut.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Opsional) Buat file di sistem file dari instans, lalu verifikasi bahwa Anda dapat melihat file dari instans lain.

   a. Dari instans, jalankan perintah berikut untuk membuat file.

```
$ sudo touch /mnt/efs/test-file.txt
```

   b. Dari instans lain, jalankan perintah berikut untuk melihat file.

```
$ ls /mnt/efs
test-file.txt
```

Menghapus sistem file EFS

Jika Anda tidak lagi memerlukan sistem file, Anda dapat menghapusnya.

Untuk menghapus sistem file

1. Buka konsol Amazon Elastic File System di https://console.aws.amazon.com/efs/.
2. Pilih sistem file yang akan dihapus.
3. Pilih Tindakan, Hapus sistem file.
4. Saat diminta konfirmasi, masukkan ID sistem file dan pilih Hapus sistem file.

Gunakan Amazon FSx dengan EC2 instans Amazon

Rangkaian layanan Amazon FSx memudahkan peluncuran, menjalankan, dan menskalakan penyimpanan bersama yang didukung oleh sistem file komersial dan sumber terbuka yang populer. Anda dapat menggunakan wizard instans peluncuran baru untuk secara otomatis melampirkan jenis sistem FSx file Amazon berikut ke EC2 instans Amazon Anda saat peluncuran:

- Amazon FSx untuk NetApp ONTAP menyediakan penyimpanan bersama yang dikelola sepenuhnya di AWS Cloud dengan akses data populer dan kemampuan manajemen NetApp ONTAP.
- Amazon FSx untuk OpenZFS menyediakan penyimpanan bersama hemat biaya yang dikelola sepenuhnya didukung oleh sistem file OpenZFS yang populer.

> **Note**
>
> - Fungsi ini tersedia di wizard peluncuran instans baru saja. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol
> - Amazon FSx untuk Windows File Server dan Amazon FSx untuk sistem file Lustre tidak dapat dipasang saat peluncuran. Anda harus memasang sistem file ini secara manual setelah peluncuran.

Anda dapat memilih untuk memasang sistem file yang sudah ada yang Anda buat sebelumnya, atau Anda dapat membuat sistem file baru untuk dipasang ke instans saat peluncuran.

Topik

- Grup keamanan dan skrip data pengguna
- Pasang sistem FSx file Amazon saat diluncurkan

Grup keamanan dan skrip data pengguna

Saat memasang sistem FSx file Amazon ke instans menggunakan wizard instance peluncuran, Anda dapat memilih apakah akan secara otomatis membuat dan melampirkan grup keamanan yang diperlukan untuk mengaktifkan akses ke sistem file, dan apakah akan secara otomatis menyertakan skrip data pengguna yang diperlukan untuk memasang sistem file dan membuatnya tersedia untuk digunakan.

Topik

- Grup keamanan
- Skrip data pengguna

Grup keamanan

Jika Anda memilih untuk secara otomatis membuat grup keamanan yang diperlukan untuk mengaktifkan akses ke sistem file, wizard peluncuran instans membuat dan melampirkan dua grup keamanan - satu grup keamanan dilampirkan ke instans, dan yang lainnya dilampirkan ke sistem file. Untuk informasi selengkapnya tentang persyaratan grup keamanan, lihat FSx kontrol akses sistem file ONTAP dengan Amazon VPC FSx dan untuk kontrol akses sistem file OpenZFS dengan Amazon VPC.

Kami menambahkan tanda `Name=instance-sg-`*`1`* ke grup keamanan yang dibuat dan dilampirkan ke instans. Nilai dalam tag secara otomatis bertambah setiap kali wizard instance peluncuran membuat grup keamanan untuk sistem FSx file Amazon.

Grup keamanan mencakup aturan output berikut ini, tetapi tidak ada aturan masuk.

Aturan-aturan ke luar

Tipe protokol	Nomor port	Destinasi
UDP	111	*file system security group*
UDP	20001 - 20003	*file system security group*
UDP	4049	*file system security group*
UDP	2049	*file system security group*
UDP	635	*file system security group*
UDP	4045 - 4046	*file system security group*
TCP	4049	*file system security group*
TCP	635	*file system security group*
TCP	2049	*file system security group*

Tipe protokol	Nomor port	Destinasi
TCP	111	*file system security group*
TCP	4045 - 4046	*file system security group*
TCP	20001 - 20003	*file system security group*
Semua	Semua	*file system security group*

Grup keamanan yang dibuat dan dilampirkan ke sistem file ditandai dengan `Name=fsx-sg-`*1*. Nilai dalam tag secara otomatis bertambah setiap kali wizard instance peluncuran membuat grup keamanan untuk sistem FSx file Amazon.

Grup keamanan mencakup aturan berikut.

Aturan-aturan ke dalam

Tipe protokol	Nomor port	Sumber
UDP	2049	*instance security group*
UDP	20001 - 20003	*instance security group*
UDP	4049	*instance security group*
UDP	111	*instance security group*
UDP	635	*instance security group*
UDP	4045 - 4046	*instance security group*
TCP	4045 - 4046	*instance security group*
TCP	635	*instance security group*
TCP	2049	*instance security group*
TCP	4049	*instance security group*
TCP	20001 - 20003	*instance security group*

Tipe protokol	Nomor port	Sumber
TCP	111	*instance security group*

Aturan-aturan ke luar

Tipe protokol	Nomor port	Destinasi
Semua	Semua	0.0.0.0/0

Skrip data pengguna

Jika Anda memilih untuk secara otomatis melampirkan skrip data pengguna, wizard peluncuran instans menambahkan data pengguna berikut ke instans. Skrip ini menginstal paket-paket yang diperlukan, memasang sistem file, dan memperbarui pengaturan instans Anda sehingga sistem file akan secara otomatis dipasang ulang setiap kali instans dimulai ulang.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Pasang sistem FSx file Amazon saat diluncurkan

Untuk memasang sistem FSx file Amazon baru atau yang sudah ada saat peluncuran

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans dan kemudian pilih Luncurkan instans untuk membuka wizard peluncuran instans.
3. Di bagian Citra Aplikasi dan OS, pilih AMI yang akan digunakan.
4. Di bagian Tipe instans, pilih tipe instans.
5. Di bagian Pasangan kunci, pilih pasangan kunci yang sudah ada atau buat yang baru.
6. Di bagian Pengaturan jaringan, lakukan hal berikut ini:
   a. Pilih Edit.
   b. Jika Anda ingin memasang sistem file yang ada, untuk Subnet, pilih subnet pilihan sistem file. Sebaiknya luncurkan instans ke Zona Ketersediaan yang sama dengan subnet pilihan sistem file untuk mengoptimalkan performa.

      Jika Anda ingin membuat sistem file baru untuk dipasang ke sebuah instans, untuk Subnet, pilih subnet yang akan digunakan untuk meluncurkan instans.

      > **Important**
      >
      > Anda harus memilih subnet untuk mengaktifkan FSx fungsionalitas Amazon di wizard instance peluncuran baru. Jika Anda tidak memilih subnet, Anda tidak akan dapat memasang sistem file yang ada atau membuat yang baru.

7. Di bagian Penyimpanan, lakukan hal berikut ini:
   a. Konfigurasikan volume sesuai kebutuhan.
   b. Perluas bagian Sistem file dan pilih FSx.
   c. Pilih Tambahkan sistem file bersama.
   d. Untuk Sistem File, pilih sistem file yang akan dipasang.

> **Note**
>
> Daftar ini menampilkan semua Amazon FSx untuk NetApp ONTAP dan Amazon FSx untuk sistem file OpenZFS di akun Anda di Wilayah yang dipilih.

e. Untuk secara otomatis membuat dan melampirkan grup keamanan yang diperlukan untuk mengaktifkan akses ke sistem file, pilih Buat dan lampirkan grup keamanan secara otomatis. Jika Anda lebih suka membuat grup keamanan secara manual, kosongkan kotak centang. Untuk informasi selengkapnya, lihat Grup keamanan.

f. Untuk secara otomatis melampirkan skrip data pengguna yang diperlukan untuk memasang sistem file, pilih Secara otomatis memasang sistem file bersama dengan melampirkan skrip data pengguna yang diperlukan. Jika Anda lebih suka memberikan skrip data pengguna secara manual, kosongkan kotak centang. Untuk informasi selengkapnya, lihat Skrip data pengguna.

8. Di bagian Lanjutan, konfigurasikan pengaturan instans tambahan sesuai kebutuhan.
9. Pilih Luncurkan.

Menggunakan Cache File Amazon dengan EC2 instans Amazon

Amazon File Cache menyediakan cache berkecepatan tinggi yang dikelola sepenuhnya AWS yang membuatnya lebih mudah untuk memproses data file, di mana pun data disimpan. Amazon File Cache berfungsi sebagai lokasi penyimpanan sementara berkinerja tinggi untuk data yang disimpan di sistem file lokal, sistem AWS file, dan bucket Amazon Simple Storage Service (Amazon S3). Anda dapat menggunakan kemampuan ini untuk membuat kumpulan data yang tersebar tersedia untuk aplikasi berbasis file AWS dengan tampilan terpadu, dan pada kecepatan tinggi—latensi sub-milidetik dan throughput tinggi. Untuk informasi selengkapnya, lihat Panduan Pengguna Cache File Amazon.

Amazon File Cache berfungsi dengan Linux paling populer AMIs, dan kompatibel dengan tipe instans berbasis x86 dan tipe instans Graviton. Anda dapat mengakses cache dari EC2 instans Amazon menggunakan klien Lustre open-source. Anda dapat me-mount cache Anda dan kemudian bekerja dengan file dan direktori di cache Anda menggunakan perintah Linux standar. EC2 Instans Amazon dapat mengakses cache Anda dari Availability Zone lain dalam virtual private cloud (VPC) yang sama, asalkan konfigurasi jaringan Anda memungkinkan akses di seluruh subnet dalam VPC. Anda juga dapat membuat cache di VPC bersama.

Untuk memulai, lihat Memulai Cache File Amazon di Panduan Pengguna Cache File Amazon.

Kelola sumber daya Amazon EC2 Anda

Sumber daya adalah entitas yang dapat Anda gunakan. Amazon EC2 menciptakan sumber daya saat Anda menggunakan fitur layanan. Misalnya, sumber daya Amazon EC2 mencakup gambar, instans, armada, pasangan kunci, dan grup keamanan. Semua jenis sumber daya Amazon EC2 menyertakan atribut yang menjelaskan sumber daya. Misalnya, nama, deskripsi, pengidentifikasi sumber daya, dan Nama Sumber Daya Amazon (ARN).

Sumber daya Amazon EC2 khusus untuk AWS Wilayah atau zona tempat mereka tinggal. Misalnya, Amazon Machine Image (AMI) khusus untuk AWS Wilayah, tetapi instance yang Anda luncurkan dari AMI khusus untuk zona tempat Anda meluncurkannya. Anda dapat menentukan sumber daya Amazon EC2 dalam kebijakan izin menggunakan ARN.

Anda Akun AWS memiliki kuota default untuk Amazon EC2. Kuota ini menentukan jumlah maksimum sumber daya yang dapat Anda buat. Misalnya, ada kuota untuk jumlah maksimum v CPUs di seluruh instance yang sedang berjalan. Jika meluncurkan instance atau memulai instans yang dihentikan akan menyebabkan Anda melebihi kuota, operasi gagal.

Anda dapat mencari sumber daya tertentu di Akun AWS menurut Wilayah Anda, menggunakan ID atau tag sumber daya. Untuk mencari sumber daya atau jenis sumber daya tertentu di beberapa Wilayah, gunakan Tampilan Global Amazon EC2.

Daftar Isi

- Pilih Wilayah untuk sumber daya Amazon EC2
- Temukan sumber daya Amazon EC2 Anda
- Melihat sumber daya di seluruh Wilayah menggunakan Tampilan AWS Global
- Tandai sumber daya Amazon EC2 Anda
- Kuota EC2 layanan Amazon

Pilih Wilayah untuk sumber daya Amazon EC2

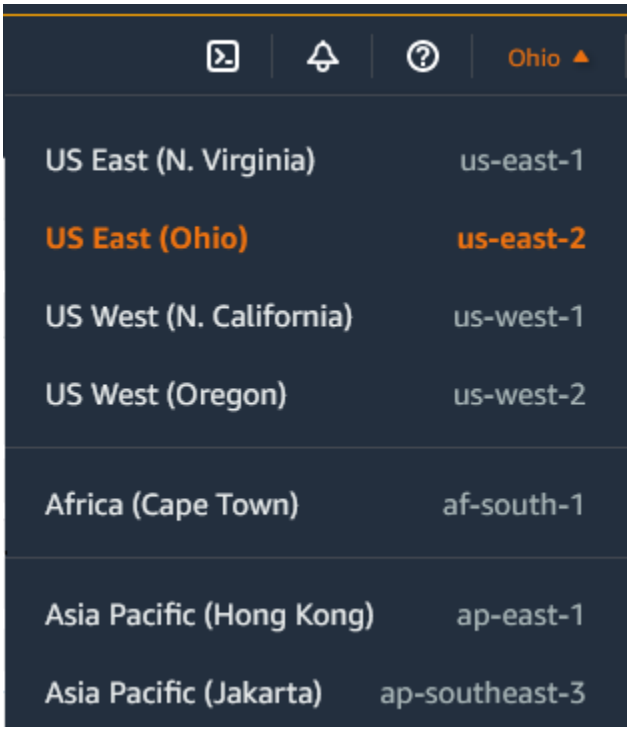
Sumber daya Amazon EC2 khusus untuk AWS Wilayah atau zona tempat mereka tinggal. Saat Anda membuat sumber daya Amazon EC2, Anda memilih Wilayah untuk sumber daya.

Pertimbangan-pertimbangan

- Beberapa AWS sumber daya mungkin tidak tersedia di semua Wilayah. Pastikan Anda dapat membuat semua AWS sumber daya yang Anda butuhkan di Wilayah sebelum Anda mulai membuat sumber daya di Wilayah.
- Beberapa Wilayah dinonaktifkan secara default. Anda harus mengaktifkan Wilayah ini sebelum dapat menggunakannya. Untuk informasi selengkapnya, lihat AWS Wilayah.

Untuk memilih Wilayah untuk sumber daya menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari bilah navigasi, pilih pemilih Wilayah, kemudian pilih Wilayah.



3. Pemilih Wilayah mencakup semua sumber daya yang tersedia untuk digunakan di Anda Akun AWS. Pilih teks yang digarisbawahi di dekat bagian bawah daftar untuk melihat Wilayah yang tidak diaktifkan untuk akun Anda.

Untuk memilih Wilayah untuk sumber daya menggunakan AWS CLI

Anda dapat mengkonfigurasi AWS CLI untuk menggunakan Wilayah default. Jika Anda tidak menentukan Region dalam perintah, Region default digunakan. Untuk menggunakan Region yang berbeda untuk perintah tertentu, tambahkan opsi berikut.

```
--region us-east-1
```

Untuk memilih Wilayah untuk sumber daya menggunakan Alat untuk PowerShell

Anda dapat mengonfigurasi Alat untuk Windows PowerShell untuk menggunakan Wilayah default. Jika Anda tidak menentukan Region dalam perintah, Region default akan digunakan. Untuk menggunakan Region yang berbeda untuk perintah tertentu, tambahkan parameter berikut.

```
-Region us-east-1
```

Temukan sumber daya Amazon EC2 Anda

Anda dapat memperoleh daftar beberapa tipe sumber daya menggunakan konsol Amazon EC2. Anda dapat memperoleh daftar setiap tipe sumber daya menggunakan perintah atau tindakan API yang sesuai. Jika memiliki banyak sumber daya, Anda dapat memfilter hasilnya agar hanya menyertakan atau mengecualikan sumber daya yang cocok dengan kriteria tertentu.

Daftar Isi

- Membuat daftar dan memfilter sumber daya menggunakan konsol
- Daftar dan filter menggunakan baris perintah
- Melihat sumber daya di seluruh Wilayah menggunakan Amazon EC2 Global View

Membuat daftar dan memfilter sumber daya menggunakan konsol

Daftar Isi

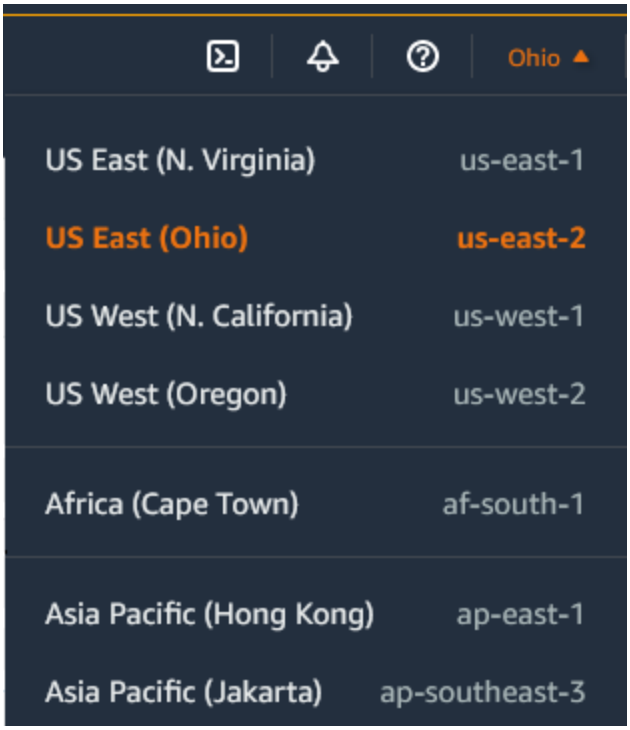
- Membuat daftar sumber daya menggunakan konsol
- Memfilter sumber daya menggunakan konsol
  - Filter yang didukung
- Simpan set filter menggunakan konsol
  - Fitur utama
  - Buat set filter
  - Ubah set filter
  - Hapus satu set filter

Membuat daftar sumber daya menggunakan konsol

Anda dapat melihat tipe sumber daya Amazon EC2 yang paling umum menggunakan konsol. Untuk melihat sumber daya tambahan, gunakan antarmuka baris perintah atau tindakan API.

Untuk membuat daftar sumber daya EC2 menggunakan konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Sumber daya Amazon EC2 khusus untuk file. AWS Region Dari bilah navigasi, pilih Region dari pemilih Regions.



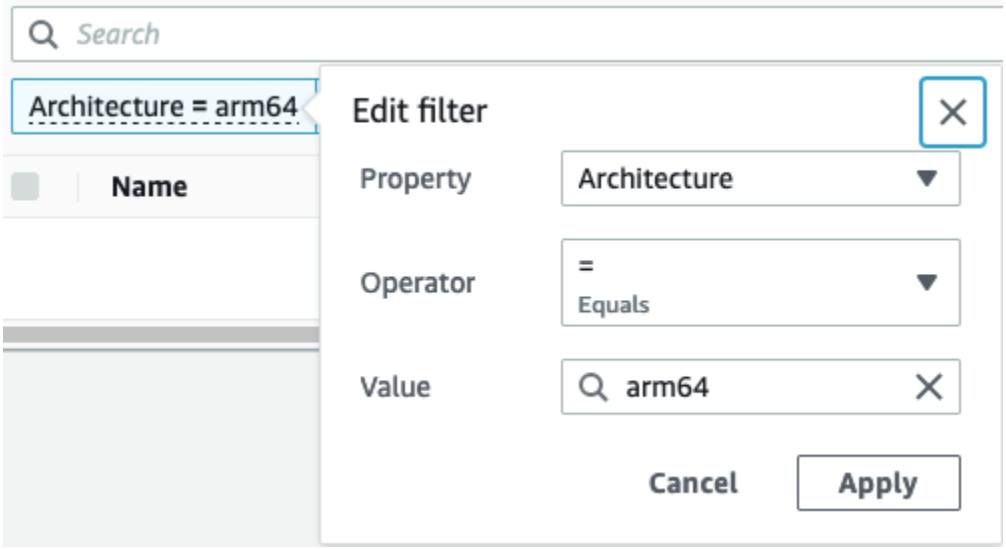
3. Di panel navigasi, pilih opsi yang sesuai dengan tipe sumber daya tersebut. Misalnya, untuk mencantumkan semua instans Anda, pilih Instans.

Memfilter sumber daya menggunakan konsol

Untuk memfilter daftar sumber daya

1. Di panel navigasi, pilih tipe sumber daya (misalnya, Instans).
2. Pilih bidang pencarian.
3. Pilih filter dari dalam daftar.

4. Pilih operator, misalnya, = (Sama dengan). Beberapa atribut memiliki berbagai operator yang tersedia untuk dipilih. Perhatikan bahwa tidak semua layar mendukung pemilihan operator.
5. Pilih nilai filter.
6. Untuk mengedit filter yang dipilih, pilih token filter (kotak biru), lakukan pengeditan yang diperlukan, lalu pilih Terapkan. Perhatikan bahwa tidak semua layar mendukung pengeditan filter yang dipilih.



7. Setelah selesai, hapus filter.

Filter yang didukung

Konsol Amazon EC2 mendukung dua jenis penyaringan.

- Pemfilteran API terjadi pada sisi server. Pemfilteran diterapkan pada panggilan API, mengurangi jumlah sumber daya yang dikembalikan oleh server. Tindakan ini memungkinkan pemfilteran cepat di sejumlah set sumber daya dan tindakan ini akan dapat menghemat waktu transfer data serta biaya antara server dan peramban. Pemfilteran API mendukung operator = (sama dengan) dan : (berisi) dan selalu peka huruf besar/kecil.
- Pemfilteran klien terjadi pada sisi klien. Tindakan ini memungkinkan Anda untuk memfilter data yang sudah tersedia dalam peramban (dengan kata lain, data yang telah dikembalikan oleh API). Pemfilteran klien berfungsi baik dalam kaitannya dengan filter API untuk memfilter set data yang lebih kecil dalam peramban. Selain operator = (sama dengan) dan: (berisi), pemfilteran klien juga dapat mendukung berbagai operator, seperti >= (lebih besar dari atau sama dengan), dan operator negasi (terbalik), seperti!= (tidak sama dengan).

Konsol Amazon EC2 mendukung jenis pencarian berikut:

Pencarian berdasarkan kata kunci

Pencarian berdasarkan kata kunci adalah pencarian teks bebas yang memungkinkan Anda mencari nilai di semua atribut atau tanda sumber daya, tanpa menentukan atribut atau kunci tanda untuk pencarian.

> **Note**
>
> Semua pencarian kata kunci menggunakan pemfilteran klien.

Untuk mencari berdasarkan kata kunci, masukkan atau tempelkan apa yang Anda cari dalam bidang pencarian, lalu pilih Enter. Misalnya, pencarian 123 cocok dengan semua instans yang memiliki 123 dalam atributnya, seperti alamat IP, ID instans, ID VPC, atau ID AMI, atau dalam tandanya, seperti Nama. Jika pencarian teks bebas Anda menampilkan kecocokan yang tidak terduga, terapkan filter tambahan.

Cari berdasarkan atribut

Pencarian berdasarkan atribut memungkinkan Anda untuk mencari atribut tertentu pada semua sumber daya.

> **Note**
>
> Pencarian atribut menggunakan pemfilteran API atau pemfilteran klien, bergantung pada atribut yang dipilih. Saat melakukan pencarian atribut, atribut akan dikelompokkan.

Misalnya, Anda dapat mencari atribut Status Instans untuk semua instans agar hanya menampilkan instans yang berada dalam status `stopped`. Untuk melakukannya:

1. Di bidang pencarian pada layar Instans, mulai masukkan `Instance state`. Saat Anda memasukkan karakter, kedua tipe filter muncul untuk Status Instans: Filter API dan Filter Klien.
2. Untuk mencari pada sisi server, pilih Status instans di bawah Filter API. Untuk mencari pada sisi klien, pilih Status instans (klien) di bawah Filter klien.

   Daftar operator yang mungkin untuk atribut yang dipilih akan muncul.
3. Pilih operator = (Sama dengan).

Daftar dari nilai yang mungkin untuk atribut dan operator yang dipilih akan muncul.

4. Pilih dihentikan dari daftar.

Cari berdasarkan tanda

Pencarian berdasarkan tanda memungkinkan Anda memfilter sumber daya dalam tabel yang ditampilkan saat ini berdasarkan kunci tanda atau nilai tanda.

Pencarian tanda menggunakan pemfilteran API atau pemfilteran klien, tergantung pengaturan di jendela Preferensi.

Guna memastikan pemfilteran API untuk tanda

1. Buka jendela Preferensi.
2. Kosongkan kotak centang Gunakan pencocokan ekspresi reguler. Jika kotak centang ini dipilih, pemfilteran klien dilakukan.
3. Pilih kotak centang Use case sensitive matching. Jika kotak centang ini dihapus, pemfilteran klien dilakukan.
4. Pilih Konfirmasi.

Saat mencari berdasarkan tanda, Anda dapat menggunakan nilai berikut:

- (kosong) – Menemukan semua sumber daya dengan kunci tanda yang ditentukan, tetapi tidak boleh ada nilai tanda.
- Semua nilai – Menemukan semua sumber daya dengan kunci tanda yang ditentukan dan nilai tanda apa pun.
- Tidak ditandai – Menemukan semua sumber daya yang tidak memiliki kunci tanda tertentu.
- Nilai yang ditampilkan - Menemukan semua sumber daya dengan kunci tanda tertentu dan nilai tanda tertentu.

Anda dapat menggunakan teknik berikut untuk meningkatkan atau menyempurnakan pencarian:

Pencarian terbalik

Pencarian terbalik memungkinkan Anda mencari sumber daya yang tidak cocok dengan nilai yang ditentukan. Di Instans dan AMIslayar, pencarian terbalik dilakukan dengan memilih! = (Tidak sama) atau! : (Tidak mengandung) operator dan kemudian memilih nilai. Di layar lainnya,

pencarian terbalik dilakukan dengan menambahkan prefiks pada kata kunci pencarian dengan karakter tanda seru (!).

> **Note**
>
> Pencarian terbalik didukung dengan pencarian kata kunci dan pencarian atribut hanya pada filter klien. Pencarian ini tidak didukung dengan pencarian atribut pada filter API.

Misalnya, Anda dapat mencari atribut Status instans untuk semua instans guna mengecualikan semua instans yang berada dalam status `terminated`. Untuk melakukannya:

1. Di bidang pencarian pada layar Instans, mulai masukkan `Instance state`. Saat Anda memasukkan karakter, kedua tipe filter muncul untuk Status Instans: Filter API dan Filter Klien.
2. Di bawah Filter klien, pilih Status instans (klien). Pencarian terbalik hanya didukung pada filter klien.

   Daftar operator yang mungkin untuk atribut yang dipilih akan muncul.
3. Pilih != (Tidak sama dengan), lalu pilih diakhiri.

Untuk memfilter instans berdasarkan atribut status instans, Anda juga dapat menggunakan ikon pencarian (

) di kolom Status instans. Ikon pencarian dengan tanda plus (+) menampilkan semua instans yang cocok dengan atribut tersebut. Ikon pencarian dengan tanda minus (-) mengecualikan semua instans yang cocok dengan atribut tersebut.

Berikut ini contoh lainnya dalam menggunakan pencarian terbalik: Untuk membuat daftar semua instans yang tidak diberikan grup keamanan `launch-wizard-1`, di Filter klien, cari berdasarkan atribut Nama grup keamanan, pilih !=, dan di bilah pencarian, masukkan `launch-wizard-1`.

Pencarian parsial

Dengan pencarian parsial, Anda dapat mencari nilai string parsial. Untuk melakukan pencarian parsial, hanya masukkan sebagian kata kunci yang ingin Anda cari. Pada Instans dan AMIslayar, pencarian sebagian hanya dapat dilakukan dengan operator: (Berisi). Di layar lainnya, Anda dapat memilih atribut filter klien dan segera memasukkan sebagian kata kunci yang ingin Anda cari saja. Misalnya, pada layar Tipe instans, untuk mencari semua instans `t2.micro`, `t2.small`, dan `t2.medium`, cari berdasarkan atribut Tipe Instans, dan untuk kata kunci, masukkan `t2`.

Pencarian ekspresi reguler

Untuk menggunakan pencarian ekspresi reguler, Anda harus memilih kotak centang Gunakan pencocokan ekspresi reguler di jendela Preferensi.

Ekspresi reguler berguna saat Anda harus mencocokkan nilai dalam sebuah bidang dengan pola tertentu. Misalnya, untuk mencari nilai yang dimulai dengan `s`, cari `^s`. Untuk mencari nilai yang berakhir dengan `xyz`, cari `xyz$`. Atau, untuk mencari nilai yang dimulai dengan angka yang diikuti oleh satu karakter atau lebih, cari `[0-9]+.*`.

> **Note**
>
> Pencarian ekspresi reguler didukung dengan pencarian kata kunci dan pencarian atribut pada filter klien saja. Pencarian ini tidak didukung dengan pencarian atribut pada filter API.

Pencarian peka huruf besar/kecil

Untuk menggunakan penelusuran peka huruf besar/kecil, Anda harus memilih kotak centang Use case sensitive matching di jendela Preferensi. Preferensi peka huruf besar/kecil hanya berlaku untuk filter klien dan tanda.

> **Note**
>
> Filter API selalu peka huruf besar/kecil.

Pencarian wildcard

Gunakan wildcard `*` untuk mencocokkan nol atau berbagai karakter. Gunakan wildcard `?` untuk mencocokkan nol atau satu karakter. Misalnya, jika Anda memiliki set data dengan nilai `prod`, `prods`, dan `production`, pencarian `prod*` mencocokkan dengan semua nilai, sedangkan `prod?` hanya mencocokkan `prod` dan `prods`. Untuk menggunakan nilai literal, hindari dengan garis miring terbalik (\). Misalnya, "`prod\*`" akan cocok dengan `prod*`.

> **Note**
>
> Pencarian wildcard didukung dengan pencarian atribut dan tanda pada filter API saja. Pencarian ini tidak didukung dengan pencarian kata kunci, dan dengan pencarian atribut dan tanda pada filter klien.

Pencarian gabungan

Secara umum, banyak filter dengan atribut yang sama secara otomatis digabungkan dengan OR. Misalnya, pencarian `Instance State : Running` dan `Instance State : Stopped` menampilkan semua instans baik yang berjalan ATAU berhenti. Untuk pencarian gabungan dengan AND, cari di berbagai atribut. Misalnya, pencarian `Instance State : Running` dan `Instance Type : c4.large` hanya menampilkan instans dengan tipe `c4.large` DAN yang berada dalam status berjalan.

Simpan set filter menggunakan konsol

Kumpulan filter tersimpan adalah grup filter khusus yang dapat Anda buat dan gunakan kembali untuk melihat sumber daya Amazon EC2 Anda secara efisien. Fitur ini membantu merampingkan alur kerja Anda, memungkinkan akses cepat ke tampilan sumber daya tertentu.

Set filter tersimpan hanya didukung di konsol Amazon EC2 dan saat ini hanya tersedia untuk halaman Volume.

Fitur utama

- Kustomisasi: Buat set filter yang disesuaikan dengan kebutuhan Anda. Misalnya, Anda dapat membuat set filter untuk hanya menampilkan `gp3` volume yang dibuat setelah tanggal yang ditentukan.
- Filter default: Tetapkan set filter default untuk halaman, dan filter default diterapkan secara otomatis saat Anda menavigasi ke halaman. Jika tidak ada default yang disetel, tidak ada filter yang diterapkan.
- Aplikasi mudah: Pilih set filter yang disimpan untuk menerapkannya secara instan. Amazon EC2 kemudian menampilkan sumber daya yang relevan, dengan filter aktif yang ditunjukkan oleh token biru.
- Fleksibilitas: Buat, modifikasi, dan hapus set filter sesuai kebutuhan.

Buat set filter

Untuk membuat set filter baru

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Volume.

> **Note**
>
> Set filter tersimpan saat ini hanya tersedia untuk Volume.

3. Di bidang pencarian, pilih filter untuk set filter Anda.
4. Pilih panah di sebelah tombol Hapus filter, dan pilih Simpan set filter baru.
5. Di jendela Simpan set filter, lakukan hal berikut:
   a. Untuk nama set Filter, masukkan nama untuk set filter.
   b. (Opsional) Untuk deskripsi set Filter, masukkan deskripsi untuk set filter.
   c. (Opsional) Untuk mengatur set filter sebagai filter default, pilih kotak centang Set as default.

   > **Note**
   >
   > Filter default diterapkan secara otomatis setiap kali Anda membuka halaman konsol.

   d. Pilih Simpan.

Ubah set filter

Untuk memodifikasi set filter

1. Dari daftar Set filter tersimpan, pilih filter yang akan dimodifikasi.
2. Untuk menambahkan filter, di bidang pencarian, pilih filter untuk ditambahkan ke set filter Anda. Untuk menghapus filter di set, pilih X pada token filter.
3. Pilih panah di sebelah tombol Hapus filter, dan pilih Ubah set filter.
4. Di jendela Modify filter set, lakukan hal berikut:
   a. (Opsional) Untuk mengatur set filter sebagai filter default, pilih kotak centang Set as default.

> **Note**
>
> Filter default diterapkan secara otomatis setiap kali Anda membuka halaman konsol.

b. Pilih Ubah.

Hapus satu set filter

Untuk menghapus set filter

1. Dari daftar Set filter tersimpan, pilih filter yang akan dihapus.
2. Pilih panah di sebelah tombol Hapus filter, dan pilih Hapus set filter.
3. Di jendela Hapus set filter, tinjau filter untuk mengonfirmasi bahwa ini adalah filter yang ingin Anda hapus, lalu pilih Hapus.

Daftar dan filter menggunakan baris perintah

Setiap jenis sumber daya memiliki tindakan API terkait yang Anda gunakan untuk mendeskripsikan, membuat daftar, atau mendapatkan sumber daya dari jenis tersebut. Daftar sumber daya yang dihasilkan dapat sangat panjang, sehingga lebih cepat dan lebih berguna untuk memfilter hasil guna menyertakan sumber daya yang cocok dengan kriteria tertentu saja.

Pertimbangan pemfilteran

- Anda dapat menentukan hingga 50 filter dan hingga 200 nilai per filter dalam satu permintaan.
- String filter dapat mencapai 255 karakter panjangnya.
- Anda dapat menggunakan wildcard dengan nilai filter. Tanda bintang (*) cocok dengan nol karakter atau lebih, dan tanda tanya (?) cocok dengan nol atau satu karakter.
- Nilai filter peka huruf besar/kecil.
- Pencarian dapat menyertakan nilai literal dari karakter wildcard; Anda hanya perlu menghindarinya dengan garis miring terbalik sebelum karakter. Misalnya, nilai `\*amazon\?\\` akan mencari string literal `*amazon?\`.
- Anda tidak dapat menentukan nilai filter darinull. Sebagai gantinya, gunakan pemfilteran sisi klien. Misalnya, perintah berikut menggunakan --query opsi dan mengembalikan IDs instance yang diluncurkan tanpa key pair.

```
aws ec2 describe-instances \
    --query 'Reservations[*].Instances[?!not_null(KeyName)].InstanceId' \
    --output text
```

AWS CLI

Example Contoh: Tentukan satu filter

Anda dapat membuat daftar instans Amazon EC2 menggunakan describe-instances. Tanpa filter, respons akan berisi informasi untuk semua sumber daya Anda. Anda dapat menggunakan opsi berikut untuk menyertakan hanya instance yang berjalan dalam output.

```
--filters Name=instance-state-name,Values=running
```

Untuk hanya mencantumkan instance IDs untuk instance yang sedang berjalan, tambahkan `--query` opsi sebagai berikut.

```
--query "Reservations[*].Instances[*].InstanceId"
```

Example Contoh: Tentukan banyak filter atau nilai filter

Jika Anda menentukan beberapa filter atau beberapa nilai filter, sumber daya harus cocok dengan semua filter untuk disertakan dalam output.

Anda dapat menggunakan opsi berikut untuk mencantumkan semua contoh yang tipenya adalah salah satu `m5.large` ataum`5d.large`.

```
--filters Name=instance-type,Values=m5.large,m5d.large
```

Anda dapat menggunakan opsi berikut untuk mencantumkan semua instance yang dihentikan yang tipenya. `t2.micro`

```
--filters Name=instance-state-name,Values=stopped Name=instance-type,Values=t2.micro
```

Example Contoh: Gunakan wildcard dalam nilai filter

Anda dapat menggunakan opsi berikut dengan deskripsi-snapshot untuk mengembalikan hanya snapshot yang deskripsinya adalah “database”.

```
--filters Name=description,Values=database
```

Wildcard * cocok dengan nol karakter atau lebih. Anda dapat menggunakan opsi berikut untuk mengembalikan hanya snapshot yang deskripsinya menyertakan katadatabase.

```
--filters Name=description,Values=*database*
```

Wildcard ? cocok dengan 1 karakter saja. Anda dapat menggunakan opsi berikut untuk mengembalikan hanya snapshot yang deskripsinya "" atau database "database" diikuti oleh satu karakter.

```
--filters Name=description,Values=database?
```

Anda dapat menggunakan opsi berikut untuk mengembalikan hanya snapshot yang deskripsinya adalah “database” diikuti hingga empat karakter. Ini tidak termasuk deskripsi dengan “database” diikuti oleh lima atau lebih karakter.

```
--filters Name=description,Values=database????
```

Example Contoh: Filter berdasarkan tanggal

Dengan AWS CLI, Anda dapat menggunakan JMESPath untuk memfilter hasil menggunakan ekspresi. Misalnya, describe-snapshotsperintah berikut menampilkan semua snapshot IDs yang dibuat oleh yang ditentukan Akun AWS sebelum tanggal yang ditentukan. Jika Anda tidak menentukan pemiliknya, hasilnya akan menyertakan semua snapshot publik.

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime<='2024-03-31')].[SnapshotId]" \
    --output text
```

Contoh berikut menampilkan semua snapshot IDs yang dibuat dalam rentang tanggal yang ditentukan.

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime>='2024-01-01') && (StartTime<='2024-12-31')].
[SnapshotId]" \
```

```
    --output text
```

Contoh: Filter berdasarkan tag

Untuk contoh tentang cara memfilter daftar sumber daya menurut tandanya, lihat Filter sumber daya Amazon EC2 berdasarkan tag.

PowerShell

Example Contoh: Tentukan satu filter

Anda dapat membuat daftar instans Amazon EC2 menggunakan Get-EC2Instance. Tanpa filter, respons akan berisi informasi untuk semua sumber daya Anda. Anda dapat menggunakan parameter berikut untuk menyertakan hanya instance yang berjalan dalam output.

```
-Filter @{Name="instance-state-name"; Values="running"}
```

Contoh berikut hanya mencantumkan instance IDs untuk instance yang sedang berjalan.

```
(Get-EC2Instance -Filter @{Name="instance-state-name"; Values="stopped"}).Instances
 | Select InstanceId
```

Example Contoh: Tentukan banyak filter atau nilai filter

Jika Anda menentukan banyak filter atau banyak nilai filter, sumber daya harus cocok dengan semua filter yang disertakan dalam hasil.

Anda dapat menggunakan opsi berikut untuk mencantumkan semua contoh yang tipenya adalah salah satu `m5.large` atau`m5d.large`.

```
-Filter @{Name="instance-type"; Values="m5.large", "m5d.large"}
```

Anda dapat menggunakan opsi berikut untuk mencantumkan semua instance yang dihentikan yang tipenya. `t2.micro`

```
-Filter @{Name="instance-state-name"; Values="stopped"}, @{Name="instance-type";
 Values="t2.micro"}
```

Melihat sumber daya di seluruh Wilayah menggunakan Amazon EC2 Global View

Amazon EC2 Global View memungkinkan Anda melihat dan mencari sumber daya Amazon EC2 dan Amazon VPC dalam satu Wilayah, atau di AWS beberapa Wilayah secara bersamaan dalam satu konsol. Lihat informasi yang lebih lengkap di Melihat sumber daya di seluruh Wilayah menggunakan Tampilan AWS Global.

Melihat sumber daya di seluruh Wilayah menggunakan Tampilan AWS Global

AWS Global View memungkinkan Anda untuk melihat beberapa sumber daya Amazon EC2 dan Amazon VPC Anda di satu AWS Wilayah, atau di beberapa Wilayah dalam satu konsol. AWS Global View juga menyediakan fungsionalitas penelusuran global yang memungkinkan Anda mencari sumber daya tertentu atau jenis sumber daya tertentu di beberapa Wilayah secara bersamaan.

AWS Tampilan Global tidak memungkinkan Anda memodifikasi sumber daya dengan cara apa pun.

Sumber daya yang didukung

Menggunakan Tampilan AWS Global, Anda dapat melihat ringkasan global sumber daya berikut di semua Wilayah tempat Anda Akun AWS diaktifkan.

- Grup Auto Scaling
- Zona Ketersediaan
- Reservasi Kapasitas dan Blok Kapasitas
- Klaster DB
- Instans DB
- Pengaturan opsi DHCP
- Gateway internet khusus egress
- Elastis IPs
- Layanan titik akhir
- Instans
- Gateway internet

- Daftar prefiks terkelola
- Gateway NAT
- Jaringan ACLs
- Antarmuka jaringan
- Outposts
- Tabel rute
- Bucket S3
- Grup keamanan
- Subnet
- volume
- VPCs
- Titik akhir VPC
- Koneksi peering VPC

Izin yang diperlukan

Pengguna harus memiliki izin berikut untuk menggunakan AWS Global View.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "autoscaling:DescribeAutoScalingGroups",
      "ec2:DescribeRegions",
      "ec2:DescribeCapacityReservations",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeEgressOnlyInternetGateways",
      "ec2:DescribeAddresses",
      "ec2:DescribeVpcEndpointServices",
      "ec2:DescribeInstances",
      "ec2:DescribeInternetGateways",
      "ec2:DescribePrefixLists",
      "ec2:DescribeNatGateways",
```

```
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeManagedPrefixLists",
        "outposts:ListOutposts",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
    }]
}
```

Untuk menggunakan Tampilan AWS Global

Masuk ke konsol Tampilan AWS Global.

> **Important**
>
> Anda tidak dapat menggunakan jendela pribadi di Firefox untuk mengakses Tampilan AWS Global.

Konsol tersebut terdiri dari hal-hal berikut:

- Region explorer - Halaman ini mencakup bagian-bagian berikut:
  - Ringkasan — Memberikan ikhtisar tingkat tinggi tentang sumber daya Anda di semua Wilayah.

    Perluas Tampilkan semua ringkasan sumber daya menunjukkan jumlah Wilayah tempat Anda Akun AWS diaktifkan. Bidang yang tersisa menunjukkan jumlah sumber daya yang saat ini Anda miliki di Wilayah tersebut. Pilih salah satu tautan untuk melihat sumber daya tipe tersebut di semua Wilayah. Misalnya, jika tautan di bawah label Instans 29 di 10 Wilayah, hal ini

menunjukkan bahwa saat ini Anda memiliki 29 instans di 10 Wilayah. Pilih tautan untuk melihat daftar 29 instans.

- Region explorer — Daftar semua Wilayah AWS (termasuk yang akun Anda tidak diaktifkan) dan menyediakan total untuk setiap jenis sumber daya untuk setiap Wilayah.

  Pilih nama Wilayah untuk melihat semua sumber daya dari semua tipe untuk Wilayah tertentu. Misalnya, pilih Afrika (Cape Town) af-south-1 untuk melihat VPCs semua, subnet, instans, grup keamanan, volume, dan grup Auto Scaling di Wilayah tersebut. Atau, pilih Wilayah dan pilih Lihat sumber daya untuk Wilayah yang dipilih.

  Pilih nilai untuk tipe sumber daya tertentu di Wilayah tertentu untuk hanya melihat sumber daya dari tipe tersebut di Wilayah tersebut. Misalnya, pilih nilai untuk Instans Afrika (Cape Town) af-south-1 untuk hanya melihat instans di Wilayah tersebut.

- Pencarian global — Halaman ini memungkinkan Anda untuk mencari sumber daya tertentu atau jenis sumber daya tertentu di satu Wilayah atau di beberapa Wilayah. Tab tersebut juga memungkinkan Anda melihat detail sumber daya tertentu.

  Untuk mencari sumber daya, masukkan kriteria pencarian di bidang sebelum grid. Anda dapat mencari berdasarkan Wilayah, berdasarkan tipe sumber daya, dan berdasarkan tanda yang ditetapkan ke sumber daya.

  Untuk melihat detail sumber daya tertentu, pilih sumber daya tersebut di grid. Anda juga dapat memilih ID sumber daya dari sebuah sumber daya untuk membukanya di konsol masing-masing. Misalnya, pilih ID instans untuk membuka instans di konsol Amazon EC2, atau pilih ID subnet untuk membuka subnet di konsol Amazon VPC.

- Wilayah dan Zona - Halaman ini memungkinkan Anda untuk melihat dan mengelola semua Wilayah, Availability Zone, Local Zones, dan Wavelength Zone yang tersedia.

  Dari tab Wilayah, Anda dapat melihat semua AWS Wilayah. Kolom Status menampilkan Wilayah yang diaktifkan untuk Anda Akun AWS. Dari halaman ini, Anda dapat memilih Wilayah untuk:

  - Lihat detail Wilayah seperti kode Wilayah, Geografi, dan jumlah setiap jenis Zona.

    Anda juga dapat melihat daftar Availability Zones, Local Zones, dan Wavelength Zones dan daftar sumber daya Anda di Wilayah.

  - Aktifkan atau nonaktifkan Wilayah.

  Dari setiap tab zona, Anda dapat melihat daftar jenis zona tersebut. Dari tab Local Zones, Anda dapat memilih masuk ke Local Zone.

> **Tip**
>
> Jika Anda hanya menggunakan Wilayah atau jenis sumber daya tertentu, Anda dapat menyesuaikan Tampilan AWS Global untuk hanya menampilkan Wilayah dan jenis sumber daya tersebut. Untuk menyesuaikan Wilayah dan jenis sumber daya yang ditampilkan, di panel navigasi, pilih Pengaturan, lalu pada tab Sumber Daya dan Wilayah, pilih Wilayah dan jenis sumber daya yang tidak ingin ditampilkan di Tampilan AWS Global.

Tandai sumber daya Amazon EC2 Anda

Untuk membantu mengelola instans, citra, dan sumber daya Amazon EC2 lainnya, Anda dapat menetapkan metadata Anda sendiri ke setiap sumber daya dalam bentuk tanda. Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Hal ini berguna ketika Anda memiliki banyak sumber daya dengan jenis yang sama—Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang telah Anda tetapkan. Topik ini menjelaskan tanda dan menunjukkan cara membuatnya.

> **Warning**
>
> Kunci tanda dan nilainya akan ditampilkan oleh berbagai panggilan API. Menolak akses ke `DescribeTags` tidak secara otomatis menolak akses ke tag yang dikembalikan oleh yang lain APIs. Sebagai praktik terbaik, sebaiknya Anda tidak menyertakan data sensitif ke dalam tanda.

Daftar Isi

- Dasar-dasar tag
- Tandai sumber daya Anda
- Pembatasan tanda
- Manajemen tanda dan akses
- Menandai sumber daya Anda untuk penagihan
- Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan
- Menambahkan dan menghapus tag untuk sumber daya Amazon EC2

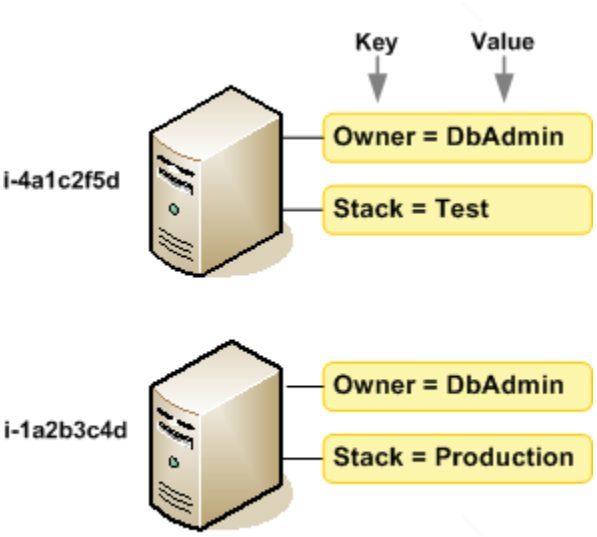
- Filter sumber daya Amazon EC2 berdasarkan tag
- Lihat tag untuk instans EC2 Anda menggunakan metadata instans

Dasar-dasar tag

Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag terdiri atas sebuah kunci dan sebuah nilai opsional, dan Anda menentukan sendiri keduanya.

Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menentukan satu set tanda untuk instans Amazon EC2 dari akun Anda yang dapat membantu melacak setiap pemilik dan tingkat tumpukan instans.

Diagram berikut menggambarkan cara kerja penandaan. Dalam contoh ini, Anda telah menetapkan dua tanda pada setiap instans—satu tanda dengan kunci `Owner` dan tanda lain dengan kunci `Stack`. Setiap tanda juga memiliki nilai yang terkait.



Sebaiknya Anda merancang set kunci tanda yang memenuhi kebutuhan setiap tipe sumber daya. Penggunaan set kunci tag yang konsisten akan memudahkan manajemen sumber daya Anda. Anda dapat mencari dan memfilter sumber daya berdasarkan tag yang Anda tambahkan. Untuk informasi selengkapnya tentang cara menerapkan strategi penandaan sumber daya yang efektif, lihat Whitepaper Praktik AWS Terbaik Tagging.

Tanda tidak memiliki makna semantik untuk Amazon EC2 dan diinterpretasikan sebagai string karakter. Selain itu, tanda tidak secara otomatis ditetapkan ke sumber daya Anda. Anda dapat

mengedit kunci dan nilai tanda, dan dapat menghapus tanda dari sumber daya kapan saja. Anda dapat mengatur nilai tanda ke string kosong, tetapi tidak dapat mengatur nilai tanda ke null. Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang telah ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama. Jika Anda menghapus sumber daya, tanda apa pun untuk sumber daya tersebut juga dihapus.

> **Note**
>
> Setelah Anda menghapus sumber daya, tanda sumber daya tersebut mungkin tetap terlihat di konsol, API, dan output CLI untuk waktu yang singkat. Tanda ini akan secara bertahap dipisahkan dari sumber daya dan dihapus secara permanen.

Tandai sumber daya Anda

Saat menggunakan konsol Amazon EC2, Anda dapat menerapkan tag ke sumber daya menggunakan tab Tag di layar sumber daya yang relevan, atau Anda dapat menggunakan Editor Tag di AWS Resource Groups konsol. Beberapa layar sumber daya memungkinkan Anda menentukan tanda untuk sebuah sumber daya saat sumber daya tersebut dibuat; misalnya, tanda dengan kunci `Name` dan nilai yang Anda tentukan. Dalam kebanyakan kasus, konsol menerapkan tanda segera setelah sumber daya dibuat (alih-alih selama pembuatan sumber daya). Konsol dapat mengatur sumber daya sesuai dengan tanda `Name`, tetapi tanda ini tidak memiliki makna semantik untuk layanan Amazon EC2.

Jika Anda menggunakan Amazon EC2 API, the, atau AWS SDK AWS CLI, Anda dapat menggunakan tindakan `CreateTags` EC2 API untuk menerapkan tag ke sumber daya yang ada. Selain itu, beberapa tindakan pembuatan sumber daya memungkinkan Anda menentukan tag untuk sumber daya saat sumber daya tersebut dibuat. Jika tag tidak dapat diterapkan selama pembuatan sumber daya, kami akan mengembalikan proses pembuatan sumber daya. Hal ini untuk memastikan bahwa sumber daya dibuat dengan tag atau tidak akan dibuat sama sekali, dan tidak akan ada sumber daya yang dibiarkan tidak bertanda. Dengan menandai sumber daya saat pembuatan, Anda dapat menghilangkan kebutuhan untuk menjalankan skrip penandaan kustom setelah pembuatan sumber daya. Untuk informasi selengkapnya tentang memungkinkan pengguna menandai sumber daya saat pembuatan, lihat Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan.

Anda dapat menerapkan izin tingkat sumber daya berbasis tanda dalam kebijakan IAM untuk tindakan API Amazon EC2 yang mendukung penandaan saat pembuatan guna

mengimplementasikan kontrol terperinci atas pengguna dan grup yang dapat menandai sumber daya saat pembuatan. Sumber daya Anda diamankan secara tepat sejak pembuatan—tanda segera diterapkan pada sumber daya Anda, oleh karena itu, izin tingkat sumber daya berbasis tanda yang mengontrol penggunaan sumber daya langsung berlaku. Sumber daya Anda dapat dilacak dan dilaporkan dengan lebih akurat. Anda dapat menerapkan penggunaan penandaan pada sumber daya baru serta mengontrol kunci dan nilai tanda mana yang ditetapkan pada sumber daya Anda.

Anda juga dapat menerapkan izin tingkat sumber daya untuk tindakan API Amazon EC2 `CreateTags` dan `DeleteTags` dalam kebijakan IAM Anda untuk mengontrol kunci dan nilai tanda mana yang ditetapkan pada sumber daya yang ada. Untuk informasi selengkapnya, lihat Contoh: Memberi tanda pada sumber daya.

Untuk informasi selengkapnya tentang penandaan sumber daya untuk penagihan, lihat Menggunakan tanda alokasi biaya dalam Buku Panduan AWS Billing .

Pembatasan tanda

Batasan dasar berikut berlaku untuk tag:

- Jumlah maksimum tag per sumber daya – 50
- Untuk setiap sumber daya, setiap kunci tag harus unik, dan setiap kunci tag hanya dapat memuat satu nilai.
- Panjang kunci maksimum – 128 karakter Unicode dalam UTF-8
- Panjang nilai maksimum – 256 karakter Unicode dalam UTF-8
- Karakter yang diizinkan
  - Meskipun EC2 memungkinkan karakter apa pun dalam tagnya, AWS layanan lain lebih ketat. Karakter yang diizinkan di semua AWS layanan adalah: huruf (`a-z`,`A-Z`), angka (`0-9`), dan spasi yang dapat direpresentasikan dalam UTF-8, dan karakter berikut:. `+ - = . _ : / @`
  - Jika Anda mengaktifkan tanda instans dalam metadata instans, kunci tanda instans hanya dapat menggunakan huruf (`a-z`, `A-Z`), angka (`0-9`), dan karakter berikut: `+ - = . , _ : @`. Kunci tanda instans tidak dapat memuat spasi atau `/`, dan tidak dapat terdiri dari `.` (satu titik), `..` (dua titik), atau `_index` saja. Untuk informasi selengkapnya, lihat Lihat tag untuk instans EC2 Anda menggunakan metadata instans.
- Kunci dan nilai tanda peka huruf besar/kecil.
- `aws:`Awalan dicadangkan untuk AWS digunakan. Jika tag memiliki kunci tag dengan awalan ini, Anda tidak dapat mengedit atau menghapus kunci atau nilai tag tersebut. Tag dengan awalan `aws:` tidak dihitung terhadap tag per batas sumber daya.

Anda tidak dapat mengakhiri, menghentikan, atau menghapus sumber daya berdasarkan tandanya saja; Anda harus menentukan pengidentifikasi sumber daya tersebut. Misalnya, untuk menghapus snapshot yang Anda beri tag dengan tag kunci yang disebut `DeleteMe`, Anda harus menggunakan tindakan `DeleteSnapshots` dengan pengidentifikasi sumber daya snapshot tersebut, seperti `snap-1234567890abcdef0`.

Saat Anda menandai sumber daya publik atau bersama, tag yang Anda tetapkan hanya tersedia untuk AWS akun Anda; tidak ada AWS akun lain yang memiliki akses ke tag tersebut. Untuk kontrol akses berbasis tag ke sumber daya bersama, setiap AWS akun harus menetapkan set tag sendiri untuk mengontrol akses ke sumber daya.

Manajemen tanda dan akses

Jika Anda menggunakan AWS Identity and Access Management (IAM), Anda dapat mengontrol pengguna mana di AWS akun Anda yang memiliki izin untuk membuat, mengedit, atau menghapus tag. Untuk informasi selengkapnya, lihat Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan.

Anda dapat menggunakan tanda sumber daya untuk mengimplementasikan kontrol berbasis atribut (ABAC). Anda dapat membuat kebijakan IAM yang memungkinkan operasi berdasarkan tanda untuk sumber daya. Untuk informasi selengkapnya, lihat Kontrol akses menggunakan akses berbasis atribut.

Menandai sumber daya Anda untuk penagihan

Anda dapat menggunakan tag untuk mengatur AWS tagihan Anda untuk mencerminkan struktur biaya Anda sendiri. Untuk melakukan ini, daftar untuk mendapatkan tagihan AWS akun Anda dengan nilai kunci tag yang disertakan. Untuk informasi selengkapnya tentang pengaturan laporan alokasi biaya dengan tanda, lihat Laporan alokasi biaya bulanan di Panduan Pengguna AWS Billing . Untuk melihat biaya sumber daya gabungan, Anda dapat mengatur informasi penagihan berdasarkan sumber daya yang memiliki nilai kunci tanda yang sama. Misalnya, Anda dapat menandai beberapa sumber daya dengan nama aplikasi tertentu, kemudian mengatur informasi penagihan untuk melihat biaya total aplikasi tersebut pada beberapa layanan. Untuk informasi selengkapnya, lihat Menggunakan tanda alokasi biaya dalam Panduan Pengguna AWS Billing .

> **Note**
>
> Jika Anda baru saja mengaktifkan pelaporan, data untuk bulan yang berjalan dapat dilihat setelah 24 jam.

Tanda alokasi biaya dapat mengindikasikan sumber daya mana yang memengaruhi biaya, tetapi penghapusan atau penonaktifkan sumber daya tidak selalu mengurangi biaya. Misalnya, data snapshot yang direferensikan oleh snapshot lain disimpan, bahkan jika snapshot yang berisi data asli dihapus. Untuk informasi selengkapnya, lihat Snapshot dan volume Amazon Elastic Block Store di Panduan Pengguna AWS Billing .

> **Note**
>
> Alamat IP Elastis yang diberikan tanda tidak akan muncul pada laporan alokasi biaya Anda.

Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan

Beberapa tindakan API Amazon EC2 yang digunakan untuk membuat sumber daya memungkinkan Anda menentukan tanda saat Anda membuat sumber daya. Anda dapat menggunakan tanda sumber daya untuk menerapkan pengendalian berbasis atribut (ABAC). Untuk informasi selengkapnya, lihat Tandai sumber daya Anda dan Kontrol akses menggunakan akses berbasis atribut.

Untuk memungkinkan para pengguna memberikan tanda pada sumber daya pada saat pembuatan, para pengguna tersebut harus memiliki izin untuk menggunakan tindakan-tindakan yang membuat sumber daya, seperti `ec2:RunInstances` atau `ec2:CreateVolume`. Jika tanda-tanda ditentukan dalam tindakan yang digunakan untuk membuat sumber daya, maka Amazon akan melakukan otorisasi tambahan pada tindakan `ec2:CreateTags` untuk melakukan verifikasi apakah pengguna memiliki izin untuk membuat tanda. Oleh karena itu, para pengguna juga harus memiliki izin eksplisit untuk menggunakan tindakan `ec2:CreateTags`.

Di dalam definisi kebijakan IAM untuk tindakan `ec2:CreateTags`, gunakan elemen `Condition` dengan kunci syarat `ec2:CreateAction` untuk memberikan izin pemberian tanda pada tindakan yang membuat sumber daya.

Contoh berikut ini mendemonstrasikan kebijakan yang memungkinkan para pengguna untuk meluncurkan instans dan menerapkan tanda apa pun pada instans dan volume saat dilakukan

peluncuran. Pengguna tidak diizinkan untuk menandai sumber daya yang sudah ada (mereka tidak dapat memanggil tindakan `ec2:CreateTags` secara langsung).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Demikian pula, kebijakan berikut memungkinkan para pengguna untuk membuat volume dan menerapkan tanda apa pun pada volume saat volume dibuat. Para pengguna tidak diizinkan untuk memberi tanda pada sumber daya yang sudah ada (mereka tidak dapat memerintahkan tindakan `ec2:CreateTags` secara langsung).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
          }
       }
    }
  ]
}
```

Tindakan `ec2:CreateTags` akan dievaluasi hanya jika tanda diterapkan selama tindakan pembuatan sumber daya. Oleh karena itu, seorang pengguna yang memiliki izin untuk membuat sumber daya (dengan asumsi tidak ada syarat untuk pemberian tanda) tidak memerlukan izin untuk menggunakan tindakan `ec2:CreateTags` jika tidak ada tanda yang ditentukan dalam permintaan. Akan tetapi, jika pengguna tersebut mencoba untuk membuat sumber daya dengan tanda, maka permintaan akan gagal jika pengguna tidak memiliki izin untuk menggunakan tindakan `ec2:CreateTags`.

Tindakan `ec2:CreateTags` juga akan dievaluasi jika tanda disediakan dalam templat peluncuran. Untuk melihat contoh kebijakan IAM, lihat Tanda di templat peluncuran.

Mengendalikan akses ke tanda-tanda tertentu

Anda dapat menggunakan syarat tambahan dalam elemen `Condition` dari kebijakan IAM Anda untuk mengontrol kunci tanda dan nilai tanda yang dapat diterapkan ke sumber daya.

Kunci syarat berikut dapat digunakan dengan contoh-contoh pada bagian sebelumnya:

- `aws:RequestTag`: Untuk mengindikasikan bahwa kunci tanda tertentu atau kunci dan nilai tanda tertentu harus ada di permintaan. Tanda-tanda yang lain juga dapat ditentukan dalam permintaan.
  - Gunakan bersama dengan operator syarat `StringEquals` untuk memberlakukan kombinasi kunci dan nilai tanda tertentu, misalnya, untuk memberlakukan tanda `cost-center=cc123`:

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

  - Gunakan bersama dengan operator syarat `StringLike` untuk memberlakukan kunci tanda tertentu dalam permintaan, misalnya, untuk memberlakukan kunci tanda `purpose`:

```
"StringLike": { "aws:RequestTag/purpose": "*" }
```

- `aws:TagKeys`: Untuk memberlakukan kunci tanda yang digunakan dalam permintaan.
  - Gunakan bersama dengan pemodifikasi `ForAllValues` untuk menerapkan kunci tanda tertentu jika disediakan dalam permintaan (jika tanda ditentukan dalam permintaan, hanya kunci tanda tertentu saja yang diperbolehkan; tidak ada tanda lain yang diperbolehkan). Sebagai contoh, kunci tanda `environment` atau `cost-center` diperbolehkan:

    ```
    "ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
    ```

  - Gunakan pemodifikasi `ForAnyValue` untuk memaksakan keberadaan setidaknya salah satu kunci tanda tertentu dalam permintaan. Sebagai contoh, setidaknya salah satu kunci tanda `environment` atau `webserver` harus ada dalam permintaan:

    ```
    "ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
    ```

Kunci syarat ini dapat diterapkan untuk tindakan-tindakan yang digunakan untuk membuat sumber daya yang mendukung pemberian tanda, serta tindakan `ec2:CreateTags` dan `ec2:DeleteTags`. Untuk mempelajari apakah tindakan API Amazon EC2 mendukung pemberian tanda, lihat Tindakan, sumber daya, dan kunci syarat untuk Amazon EC2.

Untuk memaksa para pengguna menentukan tanda pada saat mereka membuat sumber daya, Anda harus menggunakan kunci syarat `aws:RequestTag` atau kunci syarat `aws:TagKeys` dengan pemodifikasi `ForAnyValue` pada tindakan yang digunakan untuk membuat sumber daya. Tindakan `ec2:CreateTags` tidak akan dievaluasi jika pengguna tidak menentukan tanda untuk tindakan yang digunakan untuk pembuatan sumber daya.

Untuk syarat, kunci syarat tidak bersifat peka terhadap huruf besar dan kecil dan nilai syarat bersifat peka huruf besar dan kecil. Oleh karena itu, untuk memaksakan sifat peka terhadap huruf besar atau kecil dari kunci tanda, gunakan kunci syarat `aws:TagKeys`, di mana kunci tanda ditetapkan sebagai nilai dalam syarat tersebut.

Untuk contoh kebijakan IAM, lihat Contoh kebijakan untuk mengontrol akses API Amazon EC2. Untuk informasi selengkapnya, lihat Ketentuan dengan beberapa kunci konteks atau nilai dalam Panduan Pengguna IAM.

Menambahkan dan menghapus tag untuk sumber daya Amazon EC2

Saat membuat sumber daya Amazon EC2, seperti instans Amazon EC2, Anda dapat menentukan tag yang akan ditambahkan ke sumber daya. Anda juga dapat menggunakan konsol Amazon EC2 untuk menampilkan tag untuk sumber daya Amazon EC2 tertentu. Anda juga dapat menambahkan atau menghapus tag dari sumber daya Amazon EC2 yang ada.

Anda dapat menggunakan Editor Tag di AWS Resource Groups konsol untuk melihat, menambah, atau menghapus tag di semua sumber AWS daya Anda di semua Wilayah. Anda dapat menerapkan atau menghapus tag dari berbagai jenis sumber daya secara bersamaan. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Sumber Daya Penandaan.

Tugas

- Tambahkan tag menggunakan konsol
- Tambahkan tag menggunakan AWS CLI
- Tambahkan tag menggunakan PowerShell
- Tambahkan tag menggunakan CloudFormation

Tambahkan tag menggunakan konsol

Anda dapat menambahkan tag ke sumber daya yang ada langsung dari halaman untuk sumber daya.

Untuk menambahkan tag ke sumber daya yang ada

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dari bilah navigasi, pilih Wilayah tempat sumber daya berada.
3. Di panel navigasi, pilih tipe sumber daya (misalnya, Instans).
4. Pilih sumber daya dari daftar.
5. Dari tab Tag, pilih Kelola tag.
6. Pilih Tambahkan tag baru dan masukkan kunci dan nilai untuk tag.
7. Pilih Simpan.

Tambahkan tag menggunakan AWS CLI

Anda dapat menambahkan tag saat membuat sumber daya atau sumber daya yang ada.

Untuk menambahkan tag pada pembuatan sumber daya

Gunakan `-tag-specifications` opsi untuk menandai sumber daya pada pembuatan. Spesifikasi tag memerlukan jenis sumber daya yang akan diberi tag, kunci tag, dan nilai tag. Contoh berikut membuat tag dan menambahkannya ke spesifikasi tag.

```
--tag-specifications 'ResourceType=instance,Tags=[{Key=stack,Value=production}]'
```

Untuk menambahkan tag ke sumber daya yang ada

Contoh berikut menunjukkan cara menambahkan tag ke sumber daya yang ada menggunakan perintah create-tags.

Example Contoh: Menambahkan tanda ke sumber daya

Perintah berikut menambahkan tanda **`Stack=production`** ke citra tertentu, atau menimpa tanda yang sudah ada untuk AMI di mana kunci tandanya adalah stack. Jika perintah berhasil, tidak ada output yang akan ditampilkan.

```
aws ec2 create-tags \
    --resources ami-0abcdef1234567890 \
    --tags Key=stack,Value=production
```

Example Contoh: Menambahkan tanda ke banyak sumber daya

Contoh ini menambahkan (atau menimpa) dua tanda untuk AMI dan instans. Salah satu tanda hanya berisi kunci (webserver), dan tanpa nilai (kami mengatur nilai ke string kosong). Tanda lainnya terdiri dari kunci (stack) dan nilai (**`Production`**). Jika perintah berhasil, tidak ada output yang akan ditampilkan.

```
aws ec2 create-tags \
    --resources ami-0abcdef1234567890 i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Contoh: Menambahkan tanda dengan karakter khusus

Contoh ini menambahkan tanda [Group]=test ke instans. Tanda kurung siku ([dan]) adalah karakter khusus, yang harus dihindari.

Jika Anda menggunakan Linux atau OS X, untuk mengecualikan karakter khusus, sertakan elemen dengan karakter khusus dengan petik ganda ("), lalu sertakan seluruh kunci dan struktur nilai dengan tanda petik tunggal (').

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Jika Anda menggunakan Windows, untuk mengecualikan karakter khusus, sertakan elemen yang memiliki karakter khusus dengan petik ganda (“), lalu di depan setiap karakter bertanda petik ganda, tambahkan garis miring terbalik (****) sebagai berikut:

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

Jika Anda menggunakan Windows PowerShell, untuk melarikan diri dari karakter khusus, lampirkan nilai yang memiliki karakter khusus dengan tanda kutip ganda (**"**), mendahului setiap karakter kutipan ganda dengan garis miring terbalik (****), dan kemudian lampirkan seluruh kunci dan struktur nilai dengan tanda kutip tunggal () sebagai berikut: **'**

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Tambahkan tag menggunakan PowerShell

Anda dapat menambahkan tag saat membuat sumber daya atau sumber daya yang ada.

Untuk menambahkan tag pada pembuatan sumber daya

Gunakan `-TagSpecification` parameter untuk menandai sumber daya pada pembuatan. Spesifikasi tag memerlukan jenis sumber daya yang akan diberi tag, kunci tag, dan nilai tag. Contoh berikut membuat tag dan menambahkannya ke spesifikasi tag.

```
$tag = @{Key="stack"; Value="production"}
$tagspec = new-object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance"
$tagspec.Tags.Add($tag)
```

Contoh berikut menentukan tag ini dalam `-TagSpecification` parameter.

```
-TagSpecification $tagspec
```

Untuk menambahkan tag ke sumber daya yang ada

Gunakan New-EC2Tagcmdlet. Anda harus menentukan sumber daya, kunci tag, dan nilai tag.

```
New-EC2Tag `
    -Resource i-1234567890abcdef0 `
    -Tag @{Key="purpose"; Value="production"}
```

Tambahkan tag menggunakan CloudFormation

Dengan tipe sumber daya Amazon EC2, Anda menentukan tanda menggunakan `Tags` atau properti `TagSpecifications`.

Contoh berikut menambahkan tag **`Stack=Production`** untuk AWS::EC2::Instancemenggunakan `Tags` propertinya.

Example Contoh: Tanda dalam YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Contoh: Tanda dalam JSON

```
"Tags": [
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

Contoh berikut menambahkan tag **`Stack=Production`** untuk AWS::EC2::LaunchTemplate LaunchTemplateDatamenggunakan `TagSpecifications` propertinya.

Example Contoh: TagSpecifications di YAMAL

```
TagSpecifications:
  - ResourceType: "instance"
```

```
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example Contoh: TagSpecifications di JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

Filter sumber daya Amazon EC2 berdasarkan tag

Setelah menambahkan tag, Anda dapat memfilter kunci tag dan nilai tag berbasis sumber daya Amazon EC2.

Console

Untuk memfilter sumber daya berdasarkan tag

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih tipe sumber daya (misalnya, Instans).
3. Pilih bidang pencarian.
4. Dalam daftar, di bawah Tanda, pilih kunci tanda.
5. Pilih nilai tanda yang sesuai dari daftar.
6. Setelah selesai, hapus filter.

Untuk informasi selengkapnya tentang penggunaan filter di konsol Amazon EC2, lihat Temukan sumber daya Amazon EC2 Anda.

AWS CLI

Untuk mendeskripsikan sumber daya dari satu jenis dengan kunci tag yang ditentukan

Tambahkan filter berikut ke `describe` perintah untuk menjelaskan sumber daya dari jenis itu dengan Stack tag, terlepas dari nilai tag.

```
--filters Name=tag-key,Values=Stack
```

Untuk mendeskripsikan sumber daya dari satu jenis dengan tag yang ditentukan

Tambahkan filter berikut ke `describe` perintah untuk menjelaskan sumber daya jenis itu dengan tagStack=production.

```
--filters Name=tag:Stack,Values=production
```

Untuk mendeskripsikan sumber daya dari satu jenis dengan nilai tag yang ditentukan

Tambahkan filter berikut ke `describe` perintah untuk menjelaskan sumber daya dari jenis itu dengan tag dengan nilaiproduction, terlepas dari kunci tag.

```
--filters Name=tag-value,Values=production
```

Untuk mendeskripsikan semua sumber daya EC2 dengan tag yang ditentukan

Tambahkan filter berikut ke perintah deskripsi-tag untuk mendeskripsikan semua sumber daya EC2 dengan tag. Stack=test

```
--filters Name=key,Values=Stack Name=value,Values=test
```

PowerShell

Untuk memfilter sumber daya dari satu jenis dengan kunci tag

Tambahkan filter berikut ke `Get` cmdlet untuk menjelaskan sumber daya jenis itu dengan Stack tag, terlepas dari nilai tag.

```
-Filter @{Name="tag-key"; Values="Stack"}
```

Untuk memfilter sumber daya dari satu jenis dengan tag

Tambahkan filter berikut ke `Get` cmdlet untuk menjelaskan sumber daya jenis itu dengan tag. Stack=production

```
-Filter @{Name="tag:Stack"; Values="production"}
```

Untuk memfilter sumber daya dari satu jenis dengan nilai tag

Tambahkan filter berikut ke `Get` cmdlet untuk menjelaskan sumber daya dari jenis itu dengan tag dengan nilaiproduction, terlepas dari nilai kunci tag.

```
-Filter @{Name="tag-value"; Values="production"}
```

Untuk memfilter semua sumber daya EC2 berdasarkan tag

Tambahkan filter berikut ke Get-EC2Tagcmdlet untuk menjelaskan semua sumber daya EC2 dengan tag. Stack=test

```
-Filter @{Name="tag:Stack"; Values="test"}
```

Lihat tag untuk instans EC2 Anda menggunakan metadata instans

Anda dapat mengakses tanda instans dari metadata instans. Dengan mengakses tanda dari metadata instans, Anda tidak perlu lagi menggunakan panggilan API `DescribeInstances` atau `DescribeTags` untuk mengambil informasi tanda, yang mengurangi transaksi API per detik, dan memungkinkan pengambilan tanda diskalakan dengan jumlah instans yang Anda kontrol. Selain itu, proses lokal yang berjalan pada sebuah instans dapat melihat informasi tanda instans secara langsung dari metadata instans.

Secara default, tanda tidak tersedia dari metadata instans; Anda harus secara eksplisit mengizinkan akses. Anda dapat mengizinkan akses saat peluncuran instans, atau setelah peluncuran pada instans yang sedang berjalan atau dihentikan. Anda juga dapat mengizinkan akses ke tanda dengan menentukannya dalam templat peluncuran. Instans yang diluncurkan menggunakan templat mengizinkan akses ke tanda dalam metadata instans.

Jika Anda menambahkan atau menghapus tanda instans, metadata instans diperbarui saat instans sedang berjalan, tanpa perlu berhenti dan kemudian memulai instans.

Tugas

- Aktifkan akses ke tag dalam metadata contoh
- Mengambil tanda dari metadata instans
- Nonaktifkan akses ke tag dalam metadata contoh

Aktifkan akses ke tag dalam metadata contoh

Secara default, tidak ada akses ke tanda instans dalam metadata instans. Untuk setiap contoh, Anda harus secara eksplisit mengaktifkan akses.

> **Note**
>
> Jika Anda mengizinkan akses ke tag dalam metadata instance, kunci tag instance tunduk pada batasan tertentu. Ketidakpatuhan akan mengakibatkan peluncuran yang gagal untuk instance baru atau kesalahan untuk instance yang ada. Batasannya adalah:
>
> - Hanya dapat menyertakan huruf (`a-z`,`A-Z`), angka (`0-9`), dan karakter berikut:`+ - = . , _ : @`.
> - Tidak dapat berisi spasi atau`/`.
> - Tidak dapat hanya terdiri dari `.` (satu periode), `..` (dua periode), atau`_index`.
>
> Untuk informasi selengkapnya, lihat Pembatasan tanda.

Console

Untuk mengaktifkan akses ke tag dalam metadata instance selama peluncuran instance

1. Ikuti prosedur untuk meluncurkan instans.
2. Perluas Detail lanjutan, dan untuk Izinkan tag dalam metadata, pilih Aktifkan.
3. Di panel Summary, tinjau konfigurasi instans Anda, lalu pilih Launch instans. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.

Untuk mengaktifkan akses ke tag dalam metadata instance setelah peluncuran instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans Anda, lalu pilih Tindakan, Pengaturan instans, Izinkan tag dalam metadata instance.
4. Untuk mengizinkan akses ke tag dalam metadata instance, pilih kotak centang Izinkan.

5. Pilih Simpan.

AWS CLI

Untuk mengaktifkan akses ke tag dalam metadata instance selama peluncuran instance

Gunakan perintah run-instance dan tambahkan opsi berikut. `--metadata-options`

```
--metadata-options "InstanceMetadataTags=enabled"
```

Untuk mengaktifkan akses ke tag dalam metadata instance setelah peluncuran instance

Gunakan perintah berikut modify-instance-metadata-options.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --instance-metadata-tags enabled
```

Untuk memverifikasi bahwa akses ke tag dalam metadata instance diaktifkan

Gunakan perintah describe-instance dan periksa nilai. `InstanceMetadataTags`

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[].MetadataOptions[].InstanceMetadataTags"
```

Berikut ini adalah output contoh. Nilainya adalah `enabled` atau `disabled`.

```
[
    "enabled"
]
```

PowerShell

Untuk mengaktifkan akses ke tag dalam metadata instance selama peluncuran instance

Gunakan New-EC2Instancecmdlet dan tambahkan parameter berikut-`MetadataOptions_InstanceMetadataTags`.

```
-MetadataOptions_InstanceMetadataTags enabled
```

Untuk mengaktifkan akses ke tag dalam metadata instance setelah peluncuran instance

Gunakan Edit-EC2InstanceMetadataOptioncmdlet.

```
Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -InstanceMetadataTags enabled
```

Untuk memverifikasi bahwa akses ke tag dalam metadata instance diaktifkan

Gunakan Get-EC2Instancecmdlet dan periksa nilai. `InstanceMetadataTags`

```
(Get-EC2Instance `
    -
InstanceId i-1234567890abcdef0).Instances.MetadataOptions.InstanceMetadataTags.Value
```

Berikut ini adalah output contoh. Nilainya adalah `enabled` atau `disabled`.

```
enabled
```

Mengambil tanda dari metadata instans

Setelah mengizinkan akses ke tag instance dalam metadata instance, Anda dapat mengakses `tags/instance` kategori dari metadata instance. Untuk informasi selengkapnya, lihat Akses metadata instans untuk instans EC2.

IMDSv2

Linux

Jalankan perintah berikut dari instance Linux Anda untuk mencantumkan semua kunci tag untuk instance tersebut.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/tags/instance
```

Contoh ini mendapatkan nilai kunci yang diperoleh pada contoh sebelumnya. IMDSv2 Permintaan menggunakan token tersimpan yang dibuat menggunakan perintah pada contoh sebelumnya. Token tidak boleh kedaluwarsa.

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
tags/instance/tag-key
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda untuk mencantumkan semua kunci tag untuk instance tersebut.

```
$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
```

Contoh ini mendapatkan nilai kunci yang diperoleh pada contoh sebelumnya. IMDSv2 Permintaan menggunakan token tersimpan yang dibuat menggunakan perintah pada contoh sebelumnya. Token tidak boleh kedaluwarsa.

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

IMDSv1

Linux

Jalankan perintah berikut dari instance Linux Anda untuk mencantumkan semua kunci tag untuk instance tersebut.

```
curl http://169.254.169.254/latest/meta-data/tags/instance
```

Contoh ini mendapatkan nilai kunci yang diperoleh pada contoh sebelumnya.

```
curl http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Windows

Jalankan cmdlet berikut dari instance Windows Anda untuk mencantumkan semua kunci tag untuk instance tersebut.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/tags/instance
```

Contoh ini mendapatkan nilai kunci yang diperoleh pada contoh sebelumnya.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Nonaktifkan akses ke tag dalam metadata contoh

Anda dapat menonaktifkan akses ke tag instance dalam metadata instance. Anda tidak perlu menonaktifkan akses ke tag instance pada metadata instance saat peluncuran karena dimatikan secara default.

Console

Untuk menonaktifkan akses ke tag dalam metadata contoh

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih sebuah instans, lalu pilih Tindakan, Pengaturan instans, Izinkan tanda dalam metadata instans.
4. Untuk menonaktifkan akses ke tag dalam metadata instance, kosongkan kotak centang Izinkan.
5. Pilih Simpan.

AWS CLI

Untuk menonaktifkan akses ke tag dalam metadata contoh

Gunakan perintah berikut modify-instance-metadata-options.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --instance-metadata-tags disabled
```

PowerShell

Untuk menonaktifkan akses ke tag dalam metadata contoh

Gunakan Edit-EC2InstanceMetadataOptioncmdlet.

```
Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -InstanceMetadataTag disabled
```

Kuota EC2 layanan Amazon

Saat Anda membuat Akun AWS, kami menetapkan kuota default (juga disebut sebagai batas) pada AWS sumber daya Anda per wilayah. Jika Anda mencoba melebihi kuota sumber daya, permintaan gagal. Misalnya, ada jumlah maksimum Amazon EC2 v CPUs yang dapat Anda berikan untuk Instans Sesuai Permintaan di Wilayah. Jika Anda mencoba meluncurkan instans di Wilayah dan permintaan ini akan menyebabkan penggunaan Anda melebihi kuota ini, permintaan gagal. Jika ini terjadi, Anda dapat mengurangi penggunaan sumber daya atau meminta peningkatan kuota.

Konsol Service Quotas adalah lokasi pusat tempat Anda dapat melihat dan mengelola kuota untuk AWS layanan, dan meminta peningkatan kuota untuk banyak sumber daya yang Anda gunakan. Gunakan kuota yang kami sediakan untuk mengelola AWS infrastruktur Anda. Rencanakan permintaan peningkatan kuota sebelum Anda membutuhkannya.

Dokumentasi kuota terkait

- EC2 Titik akhir dan kuota Amazon
- Kuota jenis EC2 instans Amazon
- Kuota untuk Amazon EBS
- Kuota Amazon VPC

Melihat kuota Anda saat ini

Anda dapat melihat kuota untuk setiap Wilayah menggunakan konsol EC2 Amazon Service .

Untuk melihat kuota saat ini menggunakan konsol Kuota Layanan

1. Buka konsol Service Quotas di https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Dari bilah navigasi (di bagian atas layar), pilih Wilayah.
3. Pada panel Kelola kuota, pilih layanan; misalnya, Amazon Elastic Compute Cloud (Amazon). EC2 Pilih Lihat kuota.
4. Gunakan bidang filter untuk memfilter daftar berdasarkan nama sumber daya. Misalnya, masukkan **`On-Demand`** guna menemukan kuota untuk Instans Sesuai Permintaan.
5. Untuk melihat informasi selengkapnya, pilih nama kuota untuk membuka halaman detail kuota.

Meminta peningkatan

Anda dapat meminta peningkatan kuota untuk setiap Wilayah.

Untuk meminta peningkatan menggunakan konsol Kuota Layanan

1. Buka konsol Service Quotas di https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Dari bilah navigasi (di bagian atas layar), pilih Wilayah.
3. Gunakan bidang filter untuk memfilter daftar berdasarkan nama sumber daya. Misalnya, masukkan **`On-Demand`** guna menemukan kuota untuk Instans Sesuai Permintaan.
4. Jika kuota dapat disesuaikan, pilih kuota lalu pilih Minta peningkatan kuota.
5. Untuk Ubah nilai kuota, masukkan nilai kuota baru.
6. Pilih Minta.
7. Untuk melihat permintaan yang tertunda atau baru diselesaikan di konsol, pilih Dasbor dari panel navigasi. Untuk permintaan yang tertunda, pilih status permintaan untuk membuka penerimaan permintaan. Status awal dari permintaan adalah Tertunda. Setelah status berubah menjadi Kuota yang diminta, Anda akan melihat nomor kasus dengan Dukungan. Pilih nomor kasus untuk membuka tiket untuk permintaan Anda.

Untuk informasi selengkapnya, termasuk cara menggunakan AWS CLI atau SDKs meminta peningkatan kuota, lihat Meminta peningkatan kuota dalam Panduan Pengguna Service Quotas.

Pembatasan pada email yang dikirim menggunakan port 25

Secara default, Amazon EC2 mengizinkan lalu lintas keluar melalui port 25 hanya ke IPv4 alamat pribadi. Lalu lintas di atas port 25 diblokir ke IPv4 alamat dan IPv6 alamat publik.

Anda dapat meminta penghapusan pembatasan ini. Untuk informasi selengkapnya, lihat Bagaimana cara menghapus pembatasan pada port 25 dari EC2 instans Amazon atau fungsi Lambda saya?

Pembatasan ini tidak berlaku untuk lalu lintas keluar melalui port 25 yang ditujukan untuk:

- Alamat IP di blok CIDR utama VPC di mana antarmuka jaringan asal berada.
- Alamat IP dalam CIDRs didefinisikan dalam RFC 1918, RFC6598, dan RFC 4193.

Pantau sumber daya Amazon EC2

Pemantauan merupakan bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja instans Amazon EC2 dan solusi Anda. AWS Anda harus mengumpulkan data pemantauan dari semua bagian dalam AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi.

AWS menyediakan berbagai alat yang dapat Anda gunakan untuk memantau Amazon EC2. Dasbor Amazon EC2 dan CloudWatch konsol memberikan at-a-glance tampilan status lingkungan Amazon EC2 Anda. Selain itu, kami menyediakan yang berikut:

- Pemeriksaan status sistem — Pantau AWS sistem yang diperlukan untuk menggunakan instans Anda untuk memastikan bahwa mereka berfungsi dengan baik. Pemeriksaan ini mendeteksi masalah dengan instans Anda yang memerlukan AWS keterlibatan untuk memperbaiki. Jika pemeriksaan status sistem gagal, Anda dapat memilih untuk menunggu AWS memperbaiki masalah tersebut atau Anda dapat memecahkannya sendiri (misalnya, dengan menghentikan dan memulai ulang atau mengakhiri dan mengganti instans). Contoh masalah yang menyebabkan kegagalan pemeriksaan status sistem meliputi:
  - Kehilangan konektivitas jaringan
  - Kehilangan daya sistem
  - Masalah perangkat lunak pada host fisik
  - Masalah perangkat keras pada host fisik yang memengaruhi jangkauan jaringan

  Untuk informasi selengkapnya, lihat Pemeriksaan status untuk instans Amazon EC2.
- Pemeriksaan status instans — Pantau konfigurasi perangkat lunak dan jaringan instans individual Anda. Pemeriksaan ini mendeteksi masalah yang memerlukan keterlibatan Anda untuk memperbaikinya. Jika pemeriksaan status instans gagal, biasanya Anda perlu menangani sendiri masalah tersebut (misalnya, dengan melakukan boot ulang instans tersebut atau membuat modifikasi dalam sistem operasi Anda). Contoh masalah yang mungkin menyebabkan kegagalan pemeriksaan status instans meliputi:
  - Pemeriksaan status sistem gagal
  - Konfigurasi jaringan atau pemulaian salah
  - Memori habis
  - Sistem file rusak
  - Kernel tidak kompatibel

Untuk informasi selengkapnya, lihat Pemeriksaan status untuk instans Amazon EC2.

- CloudWatch Alarm Amazon — Tonton satu metrik selama periode waktu yang Anda tentukan, dan lakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. Tindakan ini adalah pengiriman notifikasi ke topik Amazon Simple Notification Service (Amazon SNS) atau kebijakan Amazon EC2 Auto Scaling. Alarm memanggil tindakan untuk perubahan status berkelanjutan saja. CloudWatch alarm tidak akan memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Untuk informasi selengkapnya, lihat Pantau instans Anda menggunakan CloudWatch.
- EventBridge Acara Amazon — Otomatiskan AWS layanan Anda dan tanggapi peristiwa sistem secara otomatis. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu dekat, dan Anda dapat menentukan tindakan otomatis yang akan diambil saat acara cocok dengan aturan yang Anda tulis. Untuk informasi selengkapnya, lihat the section called “Otomatisasi menggunakan EventBridge”.
- AWS CloudTrail log - Tangkap informasi terperinci tentang panggilan yang dilakukan ke Amazon EC2 API dan menyimpannya sebagai file log di Amazon S3. Anda dapat menggunakan CloudTrail log untuk menentukan panggilan mana yang dilakukan, alamat IP sumber untuk panggilan, siapa yang melakukan panggilan, dan kapan panggilan dilakukan. Untuk informasi selengkapnya, lihat the section called “Log panggilan API menggunakan CloudTrail”.
- CloudWatch agen — Kumpulkan log dan metrik tingkat sistem dari host dan tamu di instans EC2 dan server lokal Anda. Untuk informasi selengkapnya, lihat Mengumpulkan Metrik dan Log dari Instans Amazon EC2 dan Server Lokal dengan CloudWatch Agen di Panduan Pengguna Amazon. CloudWatch

Pantau status instans Amazon EC2 Anda

Anda dapat memantau status instans dengan melihat pemeriksaan status dan peristiwa terjadwal untuk instans Anda.

Pemeriksaan status memberi Anda informasi yang dihasilkan dari pemeriksaan otomatis yang dilakukan oleh Amazon EC2. Pemeriksaan otomatis ini mendeteksi apakah masalah tertentu memengaruhi instans Anda. Informasi pemeriksaan status, bersama dengan data yang disediakan oleh Amazon CloudWatch, memberi Anda visibilitas operasional terperinci ke setiap instans Anda.

Anda juga dapat melihat status acara tertentu yang dijadwalkan untuk instans Anda. Status peristiwa memberikan informasi tentang aktivitas mendatang yang direncanakan untuk instans Anda, seperti

boot ulang atau pemensiunan. Status tersebut juga memberikan informasi waktu mulai dan selesai terjadwal untuk setiap peristiwa.

Daftar Isi

- Pemeriksaan status untuk instans Amazon EC2
- Peristiwa perubahan status untuk instans Amazon EC2
- Acara terjadwal untuk instans Amazon EC2

Pemeriksaan status untuk instans Amazon EC2

Dengan pemantauan status instans, Anda dapat dengan cepat menentukan apakah Amazon EC2 telah mendeteksi masalah yang mungkin mencegah instans Anda dari menjalankan aplikasi. Amazon EC2 melakukan pemeriksaan otomatis pada setiap instans EC2 yang berjalan untuk mengidentifikasi masalah perangkat keras dan perangkat lunak. Anda dapat melihat hasil dari pemeriksaan status ini untuk mengidentifikasi masalah spesifik yang dapat dideteksi. Data status peristiwa menambah informasi yang telah disediakan Amazon EC2 tentang status setiap instans (`pending`sepert`i`running`,`stopping`,) dan metrik pemanfaatan yang dipantau CloudWatch Amazon (pemanfaatan CPU, lalu lintas jaringan, dan aktivitas disk).

Pemeriksaan status dilakukan setiap menit dan menghasilkan status lulus atau gagal. Jika semua pemeriksaan lulus, status keseluruhan instans adalah OK. Jika satu atau beberapa pemeriksaan gagal, status keseluruhannya adalah terganggu. Pemeriksaan status dibangun di Amazon EC2 sehingga pemeriksaan tidak dapat dinonaktifkan atau dihapus.

Ketika pemeriksaan status gagal, CloudWatch metrik yang sesuai untuk pemeriksaan status bertambah. Untuk informasi selengkapnya, lihat Metrik pemeriksaan status. Anda dapat menggunakan metrik ini untuk membuat alarm CloudWatch yang dipicu berdasarkan hasil pemeriksaan status. Misalnya, Anda dapat membuat alarm untuk memperingatkan Anda jika pemeriksaan status gagal pada instans tertentu. Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm untuk instans Amazon EC2 yang gagal memeriksa status.

Anda juga dapat membuat CloudWatch alarm Amazon yang memantau instans Amazon EC2 dan memulihkan instans secara otomatis jika menjadi rusak karena masalah mendasar. Untuk informasi selengkapnya, lihat Pemulihan instans otomatis.

Daftar Isi

- Tipe pemeriksaan status

- Lihat pemeriksaan status untuk instans Amazon EC2
- Membuat CloudWatch alarm untuk instans Amazon EC2 yang gagal memeriksa status

Tipe pemeriksaan status

Ada tiga jenis pemeriksaan status.

- Pemeriksaan status sistem
- Pemeriksaan status instans
- Pemeriksaan status EBS terlampir

Pemeriksaan status sistem

Pemeriksaan status sistem memantau AWS sistem tempat instance Anda berjalan. Pemeriksaan ini mendeteksi masalah yang mendasari instans, yang memerlukan keterlibatan AWS untuk diperbaiki. Ketika pemeriksaan status sistem gagal, Anda dapat memilih untuk menunggu AWS untuk memperbaiki masalah, atau Anda dapat menyelesaikannya sendiri. Untuk instans yang didukung oleh Amazon EBS, Anda dapat menghentikan dan memulai instans sendiri, yang pada sebagian besar kasus akan membuat instans dimigrasikan ke host baru. Untuk instance yang didukung oleh penyimpanan instans (hanya didukung untuk instance Linux), Anda dapat menghentikan dan mengganti instance. Perhatikan bahwa volume penyimpanan instans bersifat sementara dan semua data akan hilang saat instans dihentikan.

Berikut adalah contoh masalah yang dapat menyebabkan kegagalan pemeriksaan status sistem:

- Hilangnya konektivitas jaringan
- Kehilangan daya sistem
- Masalah perangkat lunak pada host fisik
- Masalah perangkat keras pada hosting fisik yang memengaruhi jangkauan jaringan

Jika pemeriksaan status sistem gagal, kami menambah metrik StatusCheckFailed_System.

Instans bare metal

Jika Anda memulai ulang dari sistem operasi pada instans bare metal, pemeriksaan status sistem tersebut mungkin kembali ke status gagal untuk sementara. Ketika instans tersedia, pemeriksaan status sistem seharusnya kembali ke status lulus.

Pemeriksaan status instans

Pemeriksaan status instans memantau perangkat lunak dan konektivitas jaringan dari instans individual Anda. Amazon EC2 memeriksa kondisi instans dengan mengirimkan permintaan protokol resolusi alamat (ARP) ke antarmuka jaringan (NIC). Pemeriksaan ini mendeteksi masalah yang memerlukan keterlibatan Anda untuk memperbaikinya. Jika pemeriksaan status instans gagal, Anda biasanya harus mengatasi sendiri masalah tersebut (misalnya, dengan melakukan boot ulang instans atau membuat perubahan konfigurasi instans).

> **Note**
>
> Distribusi Linux terbaru yang digunakan `systemd-networkd` untuk konfigurasi jaringan mungkin melaporkan pemeriksaan kesehatan secara berbeda dari distribusi sebelumnya. Selama proses boot, jenis jaringan ini dapat dimulai lebih awal dan berpotensi selesai sebelum tugas startup lainnya yang juga dapat mempengaruhi kesehatan instance. Pemeriksaan status yang bergantung pada ketersediaan jaringan dapat melaporkan status yang sehat sebelum tugas lain selesai.

Berikut adalah contoh masalah yang dapat menyebabkan kegagalan pemeriksaan status instans:

- Pemeriksaan status sistem gagal
- Konfigurasi jaringan atau pemulaian salah
- Memori habis
- Sistem file rusak
- Kernel tidak kompatibel
- Selama reboot, pemeriksaan status instance melaporkan kegagalan hingga instance tersedia kembali.

Jika pemeriksaan status instance gagal, kami menambah metrik StatusCheckFailed_Instance.

Instans bare metal

Jika Anda memulai ulang dari sistem operasi pada instans bare metal, pemeriksaan status instans tersebut mungkin akan kembali ke status gagal untuk sementara. Ketika instans tersedia, pemeriksaan status instans seharusnya kembali ke status lulus.

Pemeriksaan status EBS terlampir

Pemeriksaan status EBS terlampir memantau apakah volume Amazon EBS yang dilampirkan ke instans dapat dijangkau dan dapat menyelesaikan operasi. I/O `StatusCheckFailed_AttachedEBS`Metrik adalah nilai biner yang menunjukkan penurunan jika satu atau lebih volume EBS yang melekat pada instance tidak dapat menyelesaikan I/O operasi. Pemeriksaan status ini mendeteksi masalah yang mendasari komputasi atau infrastruktur Amazon EBS. Jika metrik pemeriksaan status EBS terlampir gagal, Anda dapat menunggu AWS untuk menyelesaikan masalah, atau Anda dapat mengambil tindakan, seperti mengganti volume yang terpengaruh atau menghentikan dan memulai ulang instance.

Berikut adalah contoh masalah yang dapat menyebabkan kegagalan pemeriksaan status EBS terlampir:

- Masalah perangkat keras atau perangkat lunak pada subsistem penyimpanan yang mendasari volume EBS
- Masalah perangkat keras pada host fisik yang memengaruhi jangkauan volume EBS
- Masalah konektivitas antara instans dan volume EBS

Anda dapat menggunakan metrik `StatusCheckFailed_AttachedEBS` untuk membantu meningkatkan ketahanan beban kerja Anda. Anda dapat menggunakan metrik ini untuk membuat CloudWatch alarm Amazon yang dipicu berdasarkan hasil pemeriksaan status. Misalnya, Anda dapat melakukan failover ke instans sekunder atau Zona Ketersediaan saat mendeteksi adanya dampak yang berkepanjangan. Atau, Anda dapat memantau volume EBS apa pun yang dilampirkan ke instans Anda, dan pemeriksaan status EBS menunjukkan penurunan, Anda dapat menghentikan dan memulai instans untuk memindahkannya ke host baru. I/O performance of each attached volume using EBS CloudWatch metrics to detect and replace the impaired volume. If your workload is not driving I/O Ini dapat menyelesaikan masalah host mendasar yang memengaruhi jangkauan volume EBS. Untuk informasi selengkapnya, lihat CloudWatch Metrik Amazon untuk Amazon EBS.

Anda juga dapat mengonfigurasi grup Penskalaan Otomatis Amazon EC2 untuk mendeteksi kegagalan pemeriksaan status EBS terlampir, lalu mengganti instans yang terpengaruh dengan yang baru. Untuk informasi selengkapnya, lihat Memantau dan mengganti instans Auto Scaling dengan volume Amazon EBS yang terganggu di Panduan Pengguna Amazon EC2 Auto Scaling.

> **Note**
>
> Metrik pemeriksaan status EBS yang terlampir hanya tersedia untuk instans Nitro.

Lihat pemeriksaan status untuk instans Amazon EC2

Jika instans Anda memiliki pemeriksaan status yang gagal, Anda biasanya harus mengatasi sendiri masalah tersebut (misalnya, dengan melakukan boot ulang instans atau membuat perubahan konfigurasi instans). Untuk memecahkan sendiri masalah kegagalan pemeriksaan status sistem atau instans, lihat Memecahkan masalah instans Amazon EC2 Linux dengan pemeriksaan status yang gagal.

Console

Untuk melihat pemeriksaan status

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pada halaman Instans, kolom Pemeriksaan status menampilkan status operasional setiap instans.
4. Untuk melihat status instans tertentu, pilih instans, lalu pilih tab Status dan alarm.
5. Untuk meninjau CloudWatch metrik untuk pemeriksaan status, pada tab Status dan alarm, perluas Metrik untuk melihat grafik untuk metrik berikut:

   - Pemeriksaan status sistem gagal
   - Pemeriksaan status instans gagal
   - Pemeriksaan status gagal untuk EBS terlampir

   Untuk informasi selengkapnya, lihat the section called “Metrik pemeriksaan status”.

AWS CLI

Untuk melihat pemeriksaan status

Gunakan perintah describe-instance-status.

Contoh: Dapatkan status semua instance yang sedang berjalan

```
aws ec2 describe-instance-status
```

Contoh: Dapatkan status semua instance

```
aws ec2 describe-instance-status --include-all-instances
```

Contoh: Dapatkan status dari satu instance yang sedang berjalan

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

Contoh: Dapatkan semua instance dengan status `impaired`

```
aws ec2 describe-instance-status \
--filters Name=instance-status.status,Values=impaired
```

PowerShell

Untuk melihat pemeriksaan status

Gunakan perintah Get-EC2InstanceStatus.

Contoh: Dapatkan status semua instance yang sedang berjalan

```
Get-EC2InstanceStatus
```

Contoh: Dapatkan status semua instance

```
Get-EC2InstanceStatus -IncludeAllInstance $true
```

Contoh: Dapatkan status dari satu instance yang sedang berjalan

```
Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0
```

Contoh: Dapatkan semua instance dengan status `impaired`

```
Get-EC2InstanceStatus \
-Filter @{Name="instance-status.status"; Values="impaired"}
```

Membuat CloudWatch alarm untuk instans Amazon EC2 yang gagal memeriksa status

Anda dapat menggunakan metrik pemeriksaan status untuk membuat CloudWatch alarm untuk memberi tahu Anda ketika sebuah instans memiliki pemeriksaan status yang gagal.

Pemeriksaan status dan alarm pemeriksaan status untuk sementara dapat memasukkan status data yang tidak mencukupi jika ada titik data metrik yang hilang. Meskipun jarang, ini bisa terjadi ketika ada gangguan dalam sistem pelaporan metrik, bahkan ketika sebuah instance sehat. Kami menyarankan agar Anda memperlakukan status ini sebagai data yang hilang, bukan kegagalan pemeriksaan status atau pelanggaran alarm. Hal ini sangat penting ketika mengambil stop, terminate, reboot, atau memulihkan tindakan pada instance sebagai tanggapan.

Console

Contoh ini mengonfigurasi alarm yang mengirimkan pemberitahuan saat instance gagal memeriksa status. Anda dapat menghentikan, menghentikan, atau memulihkan instance secara opsional.

Untuk membuat alarm pemeriksaan status

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans, pilih tab Pemeriksaan Status, dan pilih Tindakan, Buat alarm pemeriksaan status.
4. Pada halaman Kelola CloudWatch alarm, di bawah Tambah atau edit alarm, pilih Buat alarm.
5. Untuk Notifikasi alarm, aktifkan sakelar guna mengonfigurasi notifikasi Amazon Simple Notification Service (Amazon SNS). Pilih topik Amazon SNS yang ada atau masukkan nama untuk membuat topik baru.

   Jika Anda menambahkan alamat email ke daftar penerima atau membuat topik baru, Amazon SNS mengirimkan email konfirmasi ke setiap alamat baru. Setiap penerima harus memilih tautan konfirmasi di email. Hanya alamat yang dikonfirmasi yang menerima pemberitahuan peringatan.
6. Untuk Tindakan alarm, aktifkan tombol untuk menentukan tindakan yang perlu dilakukan saat alarm dipicu. Pilih tindakan.
7. Untuk Ambang batas alarm, pilih metrik dan kriteria alarm.

Anda dapat membiarkan pengaturan tetap default untuk Kelompokkan sampel berdasarkan (Rata-rata) dan Tipe data untuk sampel (Pemeriksaan status failed:either), atau Anda dapat mengubah pengaturan tersebut sesuai dengan kebutuhan.

Untuk Periode berturut-turut, atur jumlah periode yang ingin Anda evaluasi dan, pada Periode, masukkan durasi periode evaluasi sebelum memicu alarm dan mengirimkan email.

8. (Opsional) Untuk Data metrik sampel, pilih Tambahkan ke dasbor.
9. Pilih Buat.

Jika Anda perlu mengubah alarm status instance, Anda dapat mengeditnya.

Untuk mengedit alarm pemeriksaan status

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans dan pilih Tindakan, Pemantauan, Kelola CloudWatch alarm.
4. Pada halaman Kelola CloudWatch alarm, di bawah Tambah atau edit alarm, pilih Edit alarm.
5. Untuk Cari alarm, pilih alarm.
6. Setelah Anda selesai membuat perubahan, pilih Perbarui.

AWS CLI

Dalam contoh berikut, alarm menerbitkan notifikasi ke topik SNS saat instans gagal baik pemeriksaan instans atau pemeriksaan status sistem untuk setidaknya dua periode berturut-turut. CloudWatch Metrik yang digunakan adalah`StatusCheckFailed`.

Untuk membuat alarm pemeriksaan status

1. Pilih topik SNS yang ada atau buat baru. Untuk informasi selengkapnya, lihat Mengakses Amazon SNS AWS CLI di Panduan Pengguna AWS Command Line Interface .
2. Gunakan perintah list-metrics berikut untuk melihat metrik Amazon CloudWatch yang tersedia untuk Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Gunakan put-metric-alarmperintah berikut untuk membuat alarm.

```
aws cloudwatch put-metric-alarm \
    --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
    --metric-name StatusCheckFailed \
    --namespace AWS/EC2 \
    --statistic Maximum \
    --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
    --unit Count \
    --period 300 \
    --evaluation-periods 2 \
    --threshold 1 \
    --comparison-operator GreaterThanOrEqualToThreshold \
    --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

Periode adalah kerangka waktu, dalam detik, saat metrik Amazon CloudWatch dikumpulkan. Contoh ini menggunakan 300, yaitu 60 detik dikalikan 5 menit. Periode evaluasi adalah jumlah periode berturut-turut yang nilai metriknya harus dibandingkan dengan ambang batas. Contoh ini menggunakan 2. Tindakan alarm adalah tindakan yang harus dilakukan saat alarm ini dipicu.

PowerShell

Untuk membuat alarm pemeriksaan status

Gunakan cmdlet Write- CWMetric Alarm sebagai berikut untuk mempublikasikan notifikasi ke topik SNS saat instans gagal memeriksa status setidaknya selama dua periode berturut-turut.

```
Write-CWMetricAlarm `
    -AlarmName "StatusCheckFailed-Alarm-for-i-1234567890abcdef0" `
    -MetricName "StatusCheckFailed" `
    -Namespace "AWS/EC2" `
    -Statistic "Maximum" `
    -Dimension @{Name="InstanceId"; Values="i-1234567890abcdef0"} `
    -Unit "Count" `
    -Period 300 `
    -EvaluationPeriod 2 `
    -Threshold 1 `
    -ComparisonOperator "GreaterThanOrEqualToThreshold" `
    -AlarmAction "arn:aws:sns:us-west-2:111122223333:my-sns-topic"
```

Periode adalah kerangka waktu, dalam detik, saat metrik Amazon CloudWatch dikumpulkan. Contoh ini menggunakan 300, yaitu 60 detik dikalikan 5 menit. Periode evaluasi adalah jumlah periode berturut-turut yang nilai metriknya harus dibandingkan dengan ambang batas. Contoh ini menggunakan 2. Tindakan alarm adalah tindakan yang harus dilakukan saat alarm ini dipicu.

Peristiwa perubahan status untuk instans Amazon EC2

Amazon EC2 mengirimkan `EC2 Instance State-change Notification` peristiwa ke Amazon EventBridge saat status instans berubah.

Berikut adalah data contoh untuk peristiwa ini. Dalam contoh ini, instans memasuki status `pending`.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
   ],
   "detail":{
      "instance-id":"i-1234567890abcdef0",
      "state":"pending"
   }
}
```

Nilai yang mungkin untuk `state` adalah:

- `pending`
- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Saat Anda meluncurkan atau memulai sebuah instans, instans tersebut akan memasuki status `pending`, lalu status `running`. Saat Anda menghentikan sebuah instans, instans tersebut akan memasuki status `stopping`, lalu status `stopped`. Saat Anda mengakhiri sebuah instans, instans tersebut akan memasuki status `shutting-down`, lalu status `terminated`. Untuk informasi selengkapnya, lihat Perubahan status EC2 instans Amazon.

Buat alarm yang mengirim email saat instans Amazon EC2 mengubah status

Untuk menerima pemberitahuan email saat instans Anda mengubah status, buat topik Amazon SNS, lalu buat EventBridge aturan untuk acara tersebut`EC2 Instance State-change Notification`.

Cara membuat sebuah topik SNS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di panel navigasi, pilih Pengguna.
3. Pilih Buat topik.
4. Untuk Tipe, pilih Standar.
5. Untuk Nama, masukkan nama untuk topik Anda.
6. Pilih Buat topik.
7. Pilih Buat langganan.
8. Untuk Protokol, pilih Email.
9. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima pemberitahuan.
10. Pilih Buat langganan.
11. Anda akan menerima pesan email dengan baris subjek berikut: AWS Notification - Subscription Confirmation. Ikuti petunjuk untuk mengonfirmasi langganan Anda.

Untuk membuat EventBridge aturan

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Pilih Buat aturan.
3. Untuk Nama, masukkan nama untuk topik Anda.
4. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
5. Pilih Berikutnya.
6. Untuk Pola peristiwa, lakukan hal berikut:

a. Untuk Sumber peristiwa, pilih Layanan AWS.
b. Untuk Layanan AWS, pilih EC2.
c. Untuk Tipe peristiwa, pilih Notifikasi State-change Instans EC2.
d. Secara default, kami mengirim notifikasi untuk perubahan status apa pun pada instans apa pun. Anda dapat memilih status tertentu atau instans tertentu jika menginginkannya.

7. Pilih Berikutnya.
8. Tentukan target sebagai berikut:

a. Untuk Tipe target, pilih Layanan AWS.
b. Untuk Pilih target, pilih topik SNS.
c. Untuk Topik, pilih topik SNS yang Anda buat pada prosedur sebelumnya.

9. Pilih Berikutnya.
10. (Opsional) Tambahkan tanda ke aturan Anda.
11. Pilih Berikutnya.
12. Pilih Buat aturan.
13. Untuk menguji aturan Anda, lakukan perubahan status. Misalnya, mulai instans yang berhenti, hentikan instans yang sedang berjalan, atau luncurkan instans. Anda akan menerima pesan email dengan baris subjek berikut: AWS Notification Message. Badan email berisi data peristiwa.

Acara terjadwal untuk instans Amazon EC2

Untuk memastikan keandalan dan kinerja infrastruktur, AWS dapat menjadwalkan acara untuk reboot, menghentikan, dan menghentikan instans Anda. Peristiwa ini tidak sering terjadi.

Jika salah satu instans Anda akan terpengaruh oleh acara yang dijadwalkan, AWS beri tahu Anda terlebih dahulu melalui email, menggunakan alamat email yang terkait dengan akun Anda AWS . Email tersebut memberikan rincian tentang acara tersebut, seperti tanggal mulai dan berakhir. Tergantung pada jenis acara, Anda mungkin dapat mengambil tindakan untuk mengontrol waktu acara. AWS juga mengirimkan AWS Health acara, yang dapat Anda pantau dan kelola dengan menggunakan Amazon EventBridge. Untuk informasi selengkapnya, lihat Memantau peristiwa AWS Health dengan Amazon EventBridge.

Acara terjadwal dikelola oleh AWS. Anda tidak dapat menjadwalkan acara untuk instans Anda. Namun, Anda dapat:

- Lihat acara terjadwal untuk instans Anda.
- Sesuaikan pemberitahuan acara terjadwal untuk menyertakan atau menghapus tag dari pemberitahuan email.
- Jadwalkan ulang acara terjadwal tertentu.
- Buat jendela acara khusus untuk acara terjadwal.
- Ambil tindakan ketika sebuah instance dijadwalkan untuk reboot, berhenti, atau pensiun.

Untuk memastikan bahwa Anda menerima pemberitahuan acara terjadwal, verifikasi informasi kontak Anda di halaman Akun.

> **Note**
>
> Saat sebuah instans terpengaruh oleh peristiwa terjadwal, dan peristiwa tersebut merupakan bagian dari grup Auto Scaling, Amazon EC2 Auto Scaling pada akhirnya akan menggantikan peristiwa tersebut sebagai bagian dari pemeriksaan kondisinya, tanpa perlu tindakan lebih lanjut dari Anda. Untuk informasi selengkapnya tentang pemeriksaan kesehatan yang dilakukan oleh Amazon EC2 Auto Scaling, lihat Pemeriksaan kesehatan untuk instans dalam grup Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling.

Tipe peristiwa terjadwal

Amazon EC2 dapat membuat jenis acara terjadwal berikut untuk instans Anda, di mana acara terjadi pada waktu yang dijadwalkan:

Tipe peristiwa	Kode acara	Aksi acara
Penghentian instans	`instance-stop`	Pada waktu yang dijadwalkan, instans dihentikan. Saat Anda memulainya lagi, instans dimigrasikan ke host baru. Hanya berlaku untuk instance dengan volume root Amazon EBS.
Pensiun instans	`instance-retirement`	Pada waktu yang dijadwalkan, instance dihentikan

Tipe peristiwa	Kode acara	Aksi acara
		jika memiliki volume root Amazon EBS, atau dihentikan jika memiliki volume root penyimpanan instance.
Mulai ulang instans	`instance-reboot`	Pada waktu yang dijadwalkan, instans diboot ulang. Instance tetap berada di host, dan selama reboot, host mengalami pemeliharaan. Ini dikenal sebagai reboot di tempat.
Boot ulang sistem	`system-reboot`	Pada waktu yang dijadwalkan, instance di-boot ulang dan dimigrasikan ke host baru. Ini dikenal sebagai migrasi reboot.
Pemeliharaan sistem	`system-maintenance`	Pada waktu yang dijadwalkan, instans mungkin terpengaruh untuk sementara oleh pemeliharaan jaringan atau pemeliharaan daya.

Tentukan jenis acara

Anda dapat memeriksa jenis acara apa yang dijadwalkan untuk instans Anda.

Console

Untuk menentukan jenis acara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Dalam tabel, kode acara muncul di kolom Jenis acara.

4. Untuk memfilter tabel agar hanya menampilkan peristiwa untuk instance, di bidang pencarian pilih Jenis sumber: instance dari daftar filter.

AWS CLI

Untuk menentukan jenis acara untuk sebuah instance

Gunakan perintah describe-instance-status. Jika instance memiliki acara terjadwal terkait, output memberikan informasi tentang acara yang dijadwalkan.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query InstanceStatuses[].Events
```

Berikut ini adalah output contoh. Kode acara yang dijadwalkan adalah`system-reboot`.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2020-03-14T22:00:00.000Z",
            "NotBefore": "2020-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2020-04-05T11:00:00.000Z"
        }
    ]
]
```

PowerShell

Untuk menentukan jenis acara untuk sebuah instance

Gunakan Get-EC2InstanceStatuscmdlet. Jika instance memiliki acara terjadwal terkait, output memberikan informasi tentang acara yang dijadwalkan.

```
(Get-EC2InstanceStatus `
    -InstanceId i-1234567890abcdef0).Events
```

Berikut ini adalah output contoh. Kode acara yang dijadwalkan adalah`system-reboot`.

```
Code              : system-reboot
Description       : The instance is scheduled for a reboot
InstanceEventId   : instance-event-0d59937288b749b32
NotAfter          : 2020-03-14T22:00:00.000Z
NotBefore         : 2020-03-14T20:00:00.000Z
NotBeforeDeadline : 2020-04-05T11:00:00.000Z
```

Daftar Isi

- Mengelola instans Amazon EC2 yang dijadwalkan untuk berhenti atau pensiun
- Kelola instans Amazon EC2 yang dijadwalkan untuk reboot
- Mengelola instans Amazon EC2 yang dijadwalkan untuk pemeliharaan
- Melihat peristiwa terjadwal yang memengaruhi instans Amazon EC2 Anda
- Sesuaikan pemberitahuan acara terjadwal untuk instans EC2 Anda
- Menjadwalkan ulang acara terjadwal untuk instans EC2
- Buat jendela acara khusus untuk acara terjadwal yang memengaruhi instans Amazon EC2 Anda

Mengelola instans Amazon EC2 yang dijadwalkan untuk berhenti atau pensiun

Saat AWS mendeteksi kegagalan host yang mendasari yang tidak dapat diperbaiki untuk instans Anda, instans akan menjadwalkan untuk berhenti atau mengakhiri, tergantung pada jenis volume root instance.

- Jika instans memiliki volume root Amazon EBS, instance dijadwalkan untuk berhenti.
- Jika instance memiliki volume root penyimpanan instance, instance dijadwalkan untuk dihentikan.

Untuk informasi selengkapnya, lihat Pensiun instans.

> **Important**
>
> Semua data yang disimpan pada volume penyimpanan instans hilang saat instans dihentikan, dihibernasi, atau diakhiri. Ini termasuk volume penyimpanan instance yang dilampirkan ke instance yang memiliki volume root EBS. Pastikan untuk menyimpan data dari volume penyimpanan instans yang mungkin Anda perlukan nanti sebelum instans dihentikan, dihibernasi, atau diakhiri.

Tindakan yang dapat Anda ambil

Tindakan yang dapat Anda ambil untuk instance dengan volume root EBS

Saat menerima pemberitahuan `instance-stop` acara terjadwal, Anda dapat melakukan salah satu tindakan berikut:

- Tunggu pemberhentian terjadwal: Anda dapat menunggu instans berhenti dalam jendela pemeliharaan terjadwal.
- Lakukan stop dan start manual: Anda dapat menghentikan dan memulai instance sendiri pada waktu yang sesuai dengan Anda, yang memigrasikannya ke host baru. Ini tidak sama dengan me-reboot instance. Untuk informasi selengkapnya, lihat Hentikan dan mulai instans Amazon EC2.
- Otomatiskan berhenti dan mulai: Anda dapat mengotomatiskan penghentian langsung dan memulai sebagai respons terhadap acara yang dijadwalkan`instance-stop`. Untuk informasi selengkapnya, lihat Menjalankan operasi pada instans EC2 secara otomatis sebagai respons terhadap peristiwa AWS Health di AWS Health Panduan Pengguna.

Tindakan yang dapat Anda ambil untuk instance dengan volume root penyimpanan instance

Ketika Anda menerima pemberitahuan `system-retirement` acara terjadwal, dan Anda ingin menyimpan data Anda, Anda dapat mengambil tindakan berikut:

1. Luncurkan instance pengganti dari AMI terbaru Anda.
2. Migrasikan semua data yang diperlukan ke instance pengganti sebelum instance dijadwalkan untuk dihentikan.
3. Hentikan instance asli, atau tunggu sampai berakhir sesuai jadwal.

Untuk informasi lebih lanjut tentang tindakan yang dapat Anda lakukan, lihatPensiun instans.

Kelola instans Amazon EC2 yang dijadwalkan untuk reboot

Ketika AWS harus melakukan tugas-tugas seperti menginstal pembaruan atau memelihara host yang mendasarinya, itu dapat menjadwalkan reboot instance. Selama reboot terjadwal, instance tetap berada di host yang sama, atau bermigrasi ke host yang berbeda, tergantung pada acara, sebagai berikut:

- Kejadian `instance-reboot`

  - Selama reboot, instance tetap ada di host. Ini dikenal sebagai reboot di tempat.
  - Tuan rumah saat ini menjalani pemeliharaan.
  - Biasanya selesai dalam hitungan detik.
- Kejadian `system-reboot`
  - Selama reboot, instance dimigrasikan ke host baru. Ini dikenal sebagai migrasi reboot.
  - Biasanya selesai dalam hitungan menit.

Untuk memeriksa jenis acara apa yang dijadwalkan untuk instans Anda, lihatTentukan jenis acara.

Tindakan yang dapat Anda ambil

Ketika Anda menerima pemberitahuan terjadwal `instance-reboot` atau `system-reboot` acara, Anda dapat mengambil salah satu tindakan berikut:

- Tunggu reboot terjadwal: Anda dapat menunggu reboot instance terjadi dalam jendela pemeliharaan terjadwal.
- Jadwalkan ulang reboot: Anda dapat menjadwal ulang instance reboot ke tanggal dan waktu yang cocok untuk Anda.
- Lakukan reboot yang dimulai pengguna: Anda dapat me-reboot instance secara manual sendiri pada waktu yang sesuai dengan Anda. Namun, hasilnya tergantung pada acara:
  - `instance-reboot`event — Instance Anda tetap berada di perangkat keras saat ini (reboot di tempat), tidak ada pemeliharaan host yang terjadi, dan acara tetap terbuka.
  - Kejadian `system-reboot`
    - Jika migrasi reboot diaktifkan pada instans Anda, reboot yang dimulai pengguna mencoba memigrasikan instance Anda ke perangkat keras baru. Jika berhasil, acara dihapus. Jika tidak berhasil, reboot di tempat terjadi dan acara tetap dijadwalkan.
    - Jika migrasi reboot dinonaktifkan pada instance Anda, reboot yang dimulai pengguna menyimpan instance pada perangkat keras yang sama (reboot di tempat), tidak ada pemeliharaan host yang terjadi, dan acara tetap dijadwalkan. Ketika acara terjadwal akhirnya berlangsung, AWS akan memindahkan instance Anda ke perangkat keras baru (reboot migrasi).

Setelah AWS me-reboot instance Anda

Hal berikut ini berlaku setelah AWS me-reboot instance Anda:

- Acara yang dijadwalkan dihapus.
- Deskripsi acara diperbarui.
- Untuk sebuah `instance-reboot` acara:
  - Pemeliharaan host yang mendasarinya selesai.
- Untuk sebuah `system-reboot` acara:
  - Instance pindah ke host baru.
  - Instance mempertahankan alamat IP dan nama DNS.
  - Setiap data pada volume penyimpanan instans lokal dipertahankan.
- Anda dapat menggunakan instance Anda setelah booting sepenuhnya.

Opsi alternatif

Jika Anda tidak dapat menjadwal ulang acara reboot atau mengaktifkan migrasi reboot untuk reboot yang dimulai pengguna, tetapi ingin mempertahankan operasi normal selama jendela pemeliharaan terjadwal, Anda dapat melakukan hal berikut:

- Misalnya dengan volume root EBS
  - Hentikan dan mulai instance secara manual untuk memigrasikannya ke host baru. Ini tidak sama dengan me-reboot instance secara manual, di mana instance tetap berada di host yang sama.
  - Secara opsional, otomatiskan penghentian instan dan mulai sebagai respons terhadap peristiwa reboot terjadwal. Untuk informasi selengkapnya, lihat Menjalankan operasi pada instans EC2 secara otomatis sebagai respons terhadap peristiwa AWS Health di AWS Health Panduan Pengguna.

> **Important**
>
> Data pada volume penyimpanan instance hilang saat instance dihentikan. Untuk informasi selengkapnya, lihat Hentikan dan mulai instans Amazon EC2.

- Untuk contoh dengan volume root penyimpanan instance
  1. Luncurkan instance pengganti dari AMI terbaru Anda.
  2. Migrasikan semua data yang diperlukan ke instance pengganti sebelum jendela pemeliharaan terjadwal.
  3. Mengakhiri instance asli.

Mengaktifkan atau menonaktifkan migrasi reboot

Ketika sebuah instance dijadwalkan untuk suatu `system-reboot` acara, Anda dapat me-reboot sebelum acara. Hasil reboot yang dimulai pengguna bergantung pada setelan migrasi reboot instans:

- Diaktifkan - Reboot yang dimulai pengguna mencoba memigrasikan instance Anda ke perangkat keras baru (migrasi reboot). Jika berhasil, acara dihapus. Jika tidak berhasil, reboot di tempat terjadi dan acara tetap dijadwalkan. Perhatikan bahwa meskipun diaktifkan, migrasi reboot hanya dapat terjadi jika instance Anda memenuhi persyaratan migrasi reboot.
- Dinonaktifkan - Reboot yang dimulai pengguna menyimpan instance pada perangkat keras yang sama (reboot di tempat), tidak ada pemeliharaan host yang terjadi, dan acara tetap dijadwalkan. Ketika acara terjadwal akhirnya berlangsung, AWS akan memindahkan instance Anda ke perangkat keras baru (reboot migrasi).

Reboot dengan migrasi membutuhkan waktu lebih lama daripada reboot di tempat:

- Reboot di tempat: Sekitar 30 detik
- Reboot dengan migrasi: Beberapa menit

> **Note**
>
> Instance yang menerima pemberitahuan `system-reboot` peristiwa diaktifkan untuk migrasi reboot yang dimulai pengguna secara default.

Persyaratan untuk mengaktifkan migrasi reboot

Migrasi reboot dapat diaktifkan pada instance yang memenuhi kriteria berikut:

Tipe instans

Tidak semua tipe instance mendukung pengaktifan migrasi reboot. Anda dapat melihat jenis instance yang mendukung pengaktifan migrasi reboot.

Console

Untuk melihat jenis instance yang mendukung pengaktifan migrasi reboot

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/

2. Di panel navigasi kiri, pilih Tipe Instans.
3. Di bilah filter, masukkan Reboot Migration support: supported. Saat Anda memasukkan karakter dan nama filter muncul, Anda dapat memilihnya.

   Tabel tipe Instance menampilkan semua tipe instance yang mendukung pengaktifan migrasi reboot.

AWS CLI

Untuk melihat jenis instance yang mendukung pengaktifan migrasi reboot

Gunakan describe-instance-typesperintah dengan `reboot-migration-support` filter.

```
aws ec2 describe-instance-types \
    --filters Name=reboot-migration-support,Values=supported \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Untuk melihat jenis instance yang mendukung pengaktifan migrasi reboot

Gunakan Get-EC2InstanceTypecmdlet dengan filter. `reboot-migration-support`

```
Get-EC2InstanceType `
    -Filter @{Name="reboot-migration-support";Values="true"} | `
    Select InstanceType | Sort-Object InstanceType
```

Penghunian

- Bersama
- Instans Khusus

Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.

Batasan

Migrasi reboot tidak didukung untuk instance dengan karakteristik berikut:

- Platform: Instans berjalan secara native di hypervisor Xen

- Ukuran instans: `metal` contoh
- Penyewaan: Tuan Rumah Khusus. Untuk Host Khusus, gunakan Pemulihan Otomatis Host Khusus sebagai gantinya.
- Penyimpanan: Instans dengan volume penyimpanan instans
- Jaringan: Contoh menggunakan Adaptor Kain Elastis
- Auto Scaling: Instans yang merupakan bagian dari grup Auto Scaling

Langkah-langkah untuk mengaktifkan atau menonaktifkan migrasi reboot

Ketika sebuah instance menerima `system-reboot` acara, itu diaktifkan untuk migrasi reboot secara default. Anda dapat menonaktifkan migrasi reboot sehingga selama reboot yang dimulai pengguna, instance tetap pada perangkat keras yang sama (reboot di tempat).

`default`Konfigurasi tidak mengaktifkan migrasi reboot untuk instance yang tidak didukung. Untuk informasi selengkapnya, lihat Persyaratan untuk mengaktifkan migrasi reboot.

Anda dapat menonaktifkan atau mengaktifkan migrasi reboot pada instance yang sedang berjalan atau dihentikan.

AWS CLI

Untuk menonaktifkan migrasi reboot

Gunakan modify-instance-maintenance-optionsperintah dan atur `--reboot-migration` parameter ke`disabled`.

```
aws ec2 modify-instance-maintenance-options \

    --instance-id i-0abcdef1234567890 \

    --reboot-migration disabled
```

Untuk mengaktifkan migrasi reboot

Gunakan modify-instance-maintenance-optionsperintah dan atur `--reboot-migration` parameter ke`default`.

```
aws ec2 modify-instance-maintenance-options \
```

```
    --instance-id i-0abcdef1234567890 \

    --reboot-migration default
```

PowerShell

Untuk menonaktifkan migrasi reboot

Gunakan Edit-EC2InstanceMaintenanceOptioncmdlet.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId  `
    -RebootMigration Disabled
```

Untuk mengaktifkan migrasi reboot

Gunakan Edit-EC2InstanceMaintenanceOptioncmdlet.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -RebootMigration Enabled
```

Mengelola instans Amazon EC2 yang dijadwalkan untuk pemeliharaan

Ketika AWS harus memelihara host yang mendasarinya untuk sebuah instance, itu menjadwalkan instance untuk pemeliharaan. Terdapat dua tipe peristiwa pemeliharaan: pemeliharaan jaringan dan pemeliharaan daya.

- Selama pemeliharaan jaringan, instans terjadwal kehilangan konektivitas jaringan dalam jangka waktu singkat. Konektivitas jaringan normal ke instans Anda akan dipulihkan setelah pemeliharaan selesai.
- Selama pemeliharaan daya, instans terjadwal akan offline dalam jangka waktu singkat, lalu di-boot ulang. Saat boot ulang dilakukan, semua pengaturan konfigurasi instans Anda dipertahankan.

Setelah instans di-boot ulang (biasanya membutuhkan waktu beberapa menit), verifikasi bahwa aplikasi Anda berfungsi seperti yang diharapkan. Pada tahap ini, instans Anda seharusnya tidak lagi memiliki peristiwa terjadwal yang terkait dengannya, atau jika masih ada, deskripsi peristiwa terjadwal

dimulai dengan [Completed]. Terkadang, diperlukan waktu hingga 1 jam untuk menyegarkan deskripsi status instans. Peristiwa pemeliharaan yang sudah selesai akan ditampilkan di dasbor konsol Amazon EC2 hingga seminggu.

Tindakan yang dapat Anda ambil

Tindakan yang dapat Anda ambil untuk instance dengan volume root EBS

Ketika Anda menerima pemberitahuan `system-maintenance` acara, Anda dapat mengambil salah satu tindakan berikut:

- Tunggu pemeliharaan terjadwal: Anda dapat menunggu pemeliharaan terjadi sesuai jadwal.
- Lakukan stop dan stop manual: Anda dapat menghentikan dan memulai instance, yang memigrasikannya ke host baru. Ini tidak sama dengan me-reboot instance. Untuk informasi selengkapnya, lihat Hentikan dan mulai instans Amazon EC2.
- Mengotomatiskan berhenti dan mulai: Anda dapat mengotomatiskan penghentian langsung dan memulai sebagai respons terhadap acara pemeliharaan terjadwal. Untuk informasi selengkapnya, lihat Menjalankan operasi pada instans EC2 secara otomatis sebagai respons terhadap peristiwa AWS Health di AWS Health Panduan Pengguna.

Tindakan yang dapat Anda ambil untuk instance dengan volume root penyimpanan instance

Ketika Anda menerima pemberitahuan `system-maintenance` acara, Anda dapat mengambil salah satu tindakan berikut:

- Tunggu pemeliharaan terjadwal: Anda dapat menunggu pemeliharaan terjadi sesuai jadwal.
- Luncurkan instance pengganti: Jika Anda ingin mempertahankan operasi normal selama jendela pemeliharaan terjadwal:
  1. Luncurkan instance pengganti dari AMI terbaru Anda.
  2. Migrasikan semua data yang diperlukan ke instance pengganti sebelum jendela pemeliharaan terjadwal.
  3. Mengakhiri instance asli.

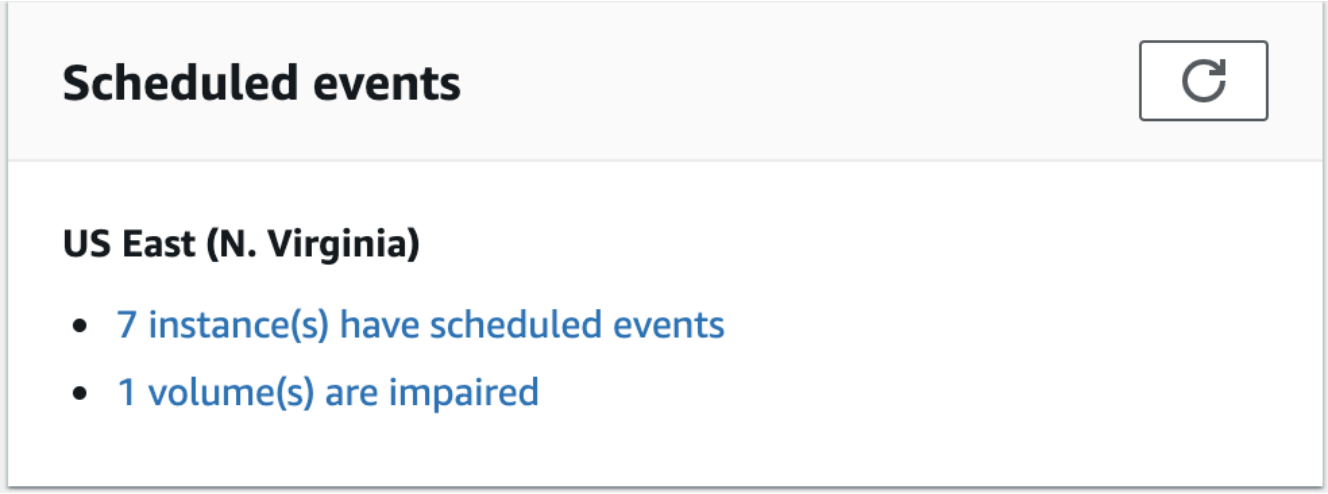
Melihat peristiwa terjadwal yang memengaruhi instans Amazon EC2 Anda

Selain menerima pemberitahuan acara terjadwal di email, Anda dapat memeriksa acara yang dijadwalkan.

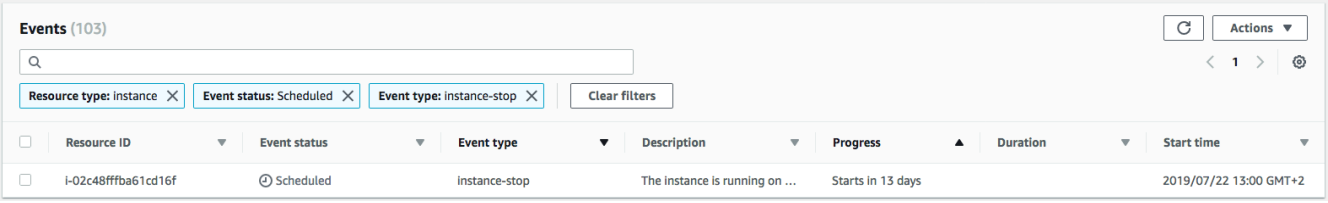
Console

Untuk melihat peristiwa terjadwal instans Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Dasbor menampilkan semua sumber daya dengan peristiwa terkait di bagian Peristiwa terjadwal.



3. Untuk detail selengkapnya, pilih Peristiwa pada panel navigasi. Semua sumber daya dengan peristiwa terkait akan ditampilkan. Anda dapat memfilter berdasarkan karakteristik, seperti tipe peristiwa, tipe sumber daya, dan Zona Ketersediaan.



AWS CLI

Untuk melihat peristiwa terjadwal instans Anda

Gunakan perintah describe-instance-status.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

Contoh output berikut menunjukkan peristiwa boot ulang.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

Output contoh berikut menunjukkan peristiwa retirement instans.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
        }
    ]
]
```

PowerShell

Untuk melihat peristiwa terjadwal instans Anda

Gunakan perintah berikut Get-EC2InstanceStatus.

```
(Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

Contoh output berikut menunjukkan peristiwa pemensiunan instans.

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

Untuk melihat peristiwa terjadwal pada instans Anda menggunakan metadata instans

Anda dapat mengambil informasi tentang peristiwa pemeliharaan yang aktif pada instans dari metadata instans menggunakan Layanan Metadata Instans Versi 2 atau Layanan Metadata Instans Versi 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

Berikut adalah contoh output dengan informasi tentang peristiwa boot ulang sistem terjadwal, dalam format JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

Untuk melihat riwayat terkait peristiwa yang selesai atau dibatalkan pada instans Anda menggunakan metadata instans

Anda dapat mengambil informasi tentang peristiwa yang selesai atau dibatalkan pada instans dari metadata instans menggunakan Layanan Metadata Instans Versi 2 atau Layanan Metadata Instans Versi 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

Berikut adalah contoh output dengan informasi tentang peristiwa boot ulang sistem yang dibatalkan, dan peristiwa boot ulang sistem yang selesai, dalam format JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

Anda dapat menggunakan Dasbor AWS Health untuk mempelajari tentang peristiwa yang dapat memengaruhi instans Anda. Ini Dasbor Health mengatur masalah dalam tiga kelompok: masalah terbuka, perubahan terjadwal, dan pemberitahuan lainnya. Grup perubahan terjadwal berisi item yang sedang berlangsung atau yang akan datang.

Untuk informasi selengkapnya, lihat Memulai dengan Anda Dasbor AWS Health di Panduan AWS Health Pengguna.

Sesuaikan pemberitahuan acara terjadwal untuk instans EC2 Anda

Anda dapat menyesuaikan notifikasi peristiwa terjadwal untuk menyertakan tanda dalam notifikasi email. Hal ini memudahkan untuk mengidentifikasi sumber daya yang terpengaruh (instans atau Host Khusus) dan memprioritaskan tindakan untuk peristiwa mendatang.

Saat menyesuaikan notifikasi peristiwa untuk menyertakan tanda, Anda dapat memilih untuk menyertakan:

- Semua tanda yang terkait dengan sumber daya yang terpengaruh
- Hanya tanda tertentu yang terkait dengan sumber daya yang terpengaruh

Misalnya, Anda menetapkan tanda `application`, `costcenter`, `project`, dan `owner` ke semua instans. Anda dapat memilih untuk menyertakan semua tanda tersebut dalam notifikasi peristiwa. Atau, jika Anda hanya ingin melihat tanda `owner` dan `project` dalam notifikasi peristiwa, Anda dapat memilih untuk hanya menyertakan tanda tersebut.

Setelah Anda memilih tanda yang akan disertakan, notifikasi peristiwa akan menyertakan ID sumber daya (ID instans atau ID Host Khusus) serta kunci tanda dan pasangan nilai yang terkait dengan sumber daya yang terpengaruh.

Tugas

- Menyertakan tanda dalam notifikasi peristiwa
- Menghapus tanda dari notifikasi peristiwa
- Melihat tanda yang akan disertakan dalam notifikasi peristiwa

Menyertakan tanda dalam notifikasi peristiwa

Tanda yang Anda pilih untuk disertakan berlaku pada semua sumber daya (instans dan Host Khusus) di Wilayah yang dipilih. Untuk menyesuaikan notifikasi peristiwa di Wilayah lain, pilih terlebih dahulu Wilayah yang diperlukan, lalu lakukan langkah-langkah berikut.

Console

Untuk menyertakan tanda dalam notifikasi peristiwa

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.

3. Pilih Tindakan, Kelola notifikasi peristiwa.
4. Aktifkan Sertakan tanda dalam notifikasi peristiwa.
5. Lakukan salah satu hal berikut, tergantung pada tanda yang ingin Anda sertakan dalam notifikasi peristiwa:
   - Untuk menyertakan semua tanda yang terkait dengan instans atau Host Khusus yang terpengaruh, pilih Sertakan semua tanda.
   - Untuk memilih tanda yang akan disertakan, klik Pilih tanda yang akan disertakan, lalu pilih atau masukkan kunci tanda.
6. Pilih Simpan.

AWS CLI

Untuk menyertakan semua tanda dalam notifikasi peristiwa

Gunakan perintah register-instance-event-notification-attributes dan atur `IncludeAllTagsOfInstance` parameternya `ketrue`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

Untuk menyertakan tanda tertentu dalam notifikasi peristiwa

Gunakan perintah register-instance-event-notification-attributes dan tentukan tag yang akan disertakan dengan menggunakan `InstanceTagKeys` parameter.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

PowerShell

Untuk menyertakan semua tanda dalam notifikasi peristiwa

Gunakan Register-EC2InstanceEventNotificationAttributecmdlet.

```
Register-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_IncludeAllTagsOfInstance $true
```

Untuk menyertakan tanda tertentu dalam notifikasi peristiwa

Gunakan Register-EC2InstanceEventNotificationAttributecmdlet.

```
Register-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_InstanceTagKey tag_key_1, tag_key_2, tag_key_3
```

Menghapus tanda dari notifikasi peristiwa

Anda dapat menghapus tag dari pemberitahuan acara.

Console

Untuk menghapus tanda dari notifikasi peristiwa

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Pilih Tindakan, Kelola notifikasi peristiwa.
4. Untuk menghapus semua tanda dari notifikasi peristiwa, nonaktifkan Sertakan tanda dalam notifikasi peristiwa.
5. Untuk menghapus tanda tertentu dari notifikasi peristiwa, pilih X) pada kunci tanda yang sesuai.
6. Pilih Simpan.

AWS CLI

Untuk menghapus semua tanda dari notifikasi peristiwa

Gunakan perintah deregister-instance-event-notification-attributes dan atur `IncludeAllTagsOfInstance` parameternya ke`false`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

Untuk menghapus tag dari pemberitahuan acara

Gunakan perintah deregister-instance-event-notification-attributes dan tentukan tag yang akan dihapus dengan menggunakan `InstanceTagKeys` parameter.

```
aws ec2 deregister-instance-event-notification-attributes \
```

```
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_3"]'
```

PowerShell

Untuk menghapus semua tanda dari notifikasi peristiwa

Gunakan Unregister-EC2InstanceEventNotificationAttributecmdlet.

```
Unregister-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_IncludeAllTagsOfInstance $false
```

Untuk menghapus tag dari pemberitahuan acara

Gunakan Unregister-EC2InstanceEventNotificationAttributecmdlet.

```
Unregister-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_InstanceTagKey tag_key_3
```

Melihat tanda yang akan disertakan dalam notifikasi peristiwa

Anda dapat melihat tag yang akan disertakan dalam pemberitahuan acara.

Console

Untuk melihat tanda yang akan disertakan dalam notifikasi peristiwa

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Pilih Tindakan, Kelola notifikasi peristiwa.

AWS CLI

Untuk melihat tag yang akan disertakan dalam pemberitahuan acara

Gunakan perintah describe-instance-event-notification-attributes.

```
aws ec2 describe-instance-event-notification-attributes
```

PowerShell

Untuk melihat tag yang akan disertakan dalam pemberitahuan acara

Gunakan Get-EC2InstanceEventNotificationAttributecmdlet.

```
Get-EC2InstanceEventNotificationAttribute
```

Menjadwalkan ulang acara terjadwal untuk instans EC2

Anda dapat menjadwalkan ulang peristiwa agar terjadi pada tanggal dan waktu tertentu yang sesuai untuk Anda. Setelah Anda menjadwal ulang acara, mungkin diperlukan satu atau dua menit sebelum tanggal yang diperbarui ditampilkan.

Batasan

- Hanya peristiwa dengan tanggal batas waktu yang dapat dijadwalkan ulang. Peristiwa dapat dijadwalkan ulang hingga tanggal batas waktu. Tanggal tenggat waktu acara ditunjukkan di kolom Batas waktu (konsol) dan `NotBeforeDeadline` bidang (AWS CLI).
- Hanya peristiwa yang belum dimulai yang dapat dijadwalkan ulang. Waktu mulai ditunjukkan di kolom Waktu mulai (konsol) dan `NotBefore` bidang (AWS CLI). Acara yang dijadwalkan akan dimulai dalam 5 menit ke depan tidak dapat dijadwal ulang.
- Waktu mulai peristiwa yang baru harus setidaknya 60 menit dari waktu saat ini.
- Jika Anda menjadwalkan ulang banyak peristiwa menggunakan konsol, tanggal batas waktu peristiwa tersebut ditentukan oleh peristiwa dengan tanggal batas waktu paling awal.

Console

Untuk menjadwalkan ulang peristiwa

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Pilih Tipe sumber daya: instans dari daftar filter.
4. Pilih satu atau beberapa instans, lalu pilih Tindakan, Jadwalkan peristiwa.

   Hanya peristiwa dengan tanggal batas waktu, yang ditunjukkan dengan nilai untuk Batas waktu, yang dapat dijadwalkan ulang. Jika salah satu peristiwa yang dipilih tidak memiliki tanggal batas waktu, Tindakan, Jadwalkan peristiwa dinonaktifkan.
5. Untuk Waktu mulai baru, masukkan tanggal dan waktu baru untuk peristiwa tersebut. Tanggal dan waktu baru harus terjadi sebelum Batas waktu peristiwa.

6. Pilih Simpan.

   Mungkin diperlukan waktu satu atau dua menit untuk menampilkan waktu mulai peristiwa yang terbaru di konsol.

AWS CLI

Untuk menjadwalkan ulang peristiwa

Gunakan perintah modify-instance-event-start-time.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2020-03-25T10:00:00.000
```

PowerShell

Untuk menjadwalkan ulang peristiwa

Gunakan Edit-EC2InstanceEventStartTimecmdlet.

```
Edit-EC2InstanceEventStartTime `
    -InstanceId i-1234567890abcdef0 `
    -InstanceEventId instance-event-0d59937288b749b32 `
    -NotBefore 2020-03-25T10:00:00.000
```

Buat jendela acara khusus untuk acara terjadwal yang memengaruhi instans Amazon EC2 Anda

Anda dapat menentukan jendela peristiwa kustom yang berulang setiap minggu untuk peristiwa terjadwal yang melakukan boot ulang, menghentikan, atau mengakhiri instans Amazon EC2 Anda. Anda dapat mengaitkan satu atau beberapa instans dengan jendela peristiwa. Jika peristiwa terjadwal untuk instans tersebut direncanakan, AWS akan menjadwalkan peristiwa dalam jendela peristiwa terkait.

Anda dapat menggunakan jendela peristiwa untuk memaksimalkan ketersediaan beban kerja dengan menentukan jendela peristiwa yang terjadi selama periode di luar jam sibuk untuk beban kerja Anda. Anda juga dapat menyelaraskan jendela peristiwa dengan jadwal pemeliharaan internal Anda.

Tetapkan jendela peristiwa dengan menentukan serangkaian rentang waktu. Rentang waktu minimum adalah 2 jam. Rentang waktu gabungan setidaknya harus mencapai total 4 jam.

Anda dapat mengaitkan satu atau beberapa instance dengan jendela acara dengan menggunakan tag instance IDs atau instance. Anda juga dapat mengaitkan Host Khusus dengan jendela peristiwa menggunakan ID host.

> **Warning**
>
> Jendela peristiwa hanya berlaku untuk peristiwa terjadwal yang menghentikan, melakukan boot ulang, atau mengakhiri instans.
> Jendela peristiwa tidak berlaku untuk:
>
> - Peristiwa terjadwal yang dipercepat dan peristiwa pemeliharaan jaringan.
> - Pemeliharaan tidak terjadwal seperti pemulihan instans otomatis dan reboot yang tidak direncanakan.

Bekerja dengan jendela peristiwa

- Pertimbangan-pertimbangan
- Membuat jendela peristiwa
- Mengaitkan target dengan jendela peristiwa
- Putuskan hubungan target dari jendela acara
- Memodifikasi jendela acara
- Hapus jendela acara

Pertimbangan-pertimbangan

- Format waktu semua jendela peristiwa adalah UTC.
- Jendela acara dapat berisi beberapa rentang waktu. Sementara setiap rentang individu harus minimal 2 jam, total durasi di semua rentang harus minimal 4 jam.
- Hanya satu tipe target (ID instans, ID Host Khusus, atau tanda instans) yang dapat dikaitkan dengan suatu jendela peristiwa.
- Target (ID instans, ID Host Khusus, atau tanda instans) hanya dapat dikaitkan dengan satu jendela peristiwa.

- Maksimal 100 instance IDs, atau 50 Dedicated Host IDs, atau 50 tag instans dapat dikaitkan dengan jendela acara. Tanda instans dapat dikaitkan dengan sejumlah instans.
- Maksimal 200 jendela acara dapat dibuat per AWS Wilayah.
- Banyak instans yang terkait dengan jendela peristiwa berpotensi memiliki peristiwa terjadwal yang terjadi pada saat bersamaan.
- Jika AWS telah menjadwalkan acara, memodifikasi jendela acara tidak akan mengubah waktu acara yang dijadwalkan. Jika peristiwa memiliki tanggal batas waktu, Anda dapat menjadwalkan ulang peristiwa.
- Anda dapat menghentikan dan memulai instance sebelum acara yang dijadwalkan. Ini memigrasikan instance ke host baru dan menghapus acara.

Membuat jendela peristiwa

Anda dapat membuat satu atau beberapa jendela peristiwa. Untuk setiap jendela peristiwa, Anda menentukan satu atau beberapa blok waktu. Misalnya, Anda dapat membuat jendela peristiwa dengan blok waktu yang terjadi setiap hari pada pukul 04.00 selama 2 jam. Atau, Anda dapat membuat jendela peristiwa dengan blok waktu yang terjadi pada hari Minggu mulai pukul 02.00 hingga 04.00 dan pada hari Rabu mulai pukul 03.00 hingga 05.00.

Jendela peristiwa berulang setiap pekan sampai Anda menghapusnya.

Console

Untuk membuat jendela peristiwa

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Pilih Tindakan, Kelola jendela peristiwa.
4. Pilih Buat jendela peristiwa instans.
5. Untuk Nama jendela peristiwa, masukkan nama deskriptif untuk jendela peristiwa tersebut.
6. Untuk Jadwal jendela peristiwa, pilih untuk menentukan blok waktu pada jendela peristiwa menggunakan pembuat jadwal cron atau dengan menentukan rentang waktu.
   - Jika Anda memilih Pembuat jadwal cron, tentukan hal berikut:
     1. Untuk Hari (UTC), tentukan hari dalam satu pekan sebagai waktu jendela peristiwa terjadi.

2. Untuk Waktu mulai (UTC), tentukan waktu mulai jendela peristiwa.
3. Untuk Durasi, tentukan durasi blok waktu dalam jendela peristiwa. Durasi minimum per blok waktu adalah 2 jam. Durasi minimum jendela peristiwa secara total harus sama dengan atau lebih dari 4 jam. Format waktunya adalah UTC.

- Jika Anda memilih Rentang waktu, pilih Tambahkan rentang waktu baru, lalu tentukan hari dan waktu mulai serta hari dan waktu selesai. Ulangi untuk setiap rentang waktu. Durasi minimum per rentang waktu adalah 2 jam. Durasi minimum untuk semua rentang waktu yang digabungkan secara total harus sama dengan atau lebih dari 4 jam.

7. (Opsional) Untuk detail Target, kaitkan satu atau beberapa instance dengan jendela acara. Gunakan contoh IDs atau tag instance untuk mengaitkan instance. Gunakan host IDs untuk mengaitkan Host Khusus. Ketika target ini dijadwalkan untuk pemeliharaan, acara akan terjadi selama jendela acara ini.

   Perhatikan bahwa Anda dapat membuat jendela peristiwa tanpa mengaitkan target dengan jendela tersebut. Kemudian, Anda dapat memodifikasi jendela untuk mengaitkan satu atau beberapa target.
8. (Opsional) Untuk Tanda jendela peristiwa, pilih Tambahkan tanda, lalu masukkan kunci dan nilai untuk tanda tersebut. Ulangi hal itu untuk setiap tanda.
9. Pilih Buat jendela peristiwa.

AWS CLI

Untuk membuat jendela peristiwa dengan rentang waktu

Gunakan perintah create-instance-event-window.

```
aws ec2 create-instance-event-window \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
```

```
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Untuk membuat jendela peristiwa dengan ekspresi cron

Gunakan perintah create-instance-event-window.

```
aws ec2 create-instance-event-window \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
```

```
}
```

PowerShell

Untuk membuat jendela peristiwa dengan rentang waktu

Gunakan New-EC2InstanceEventWindowcmdlet.

```
$timeRange = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange.StartWeekDay = "monday"
$timeRange.EndWeekDay = "wednesday"
$timeRange.StartHour = 2
$timeRange.EndHour = 8
$tag = @{Key="key1"; Value="value1"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance-event-window"
$tagspec.Tags.Add($tag)
New-EC2InstanceEventWindow `
    -Name my-event-window `
    -TagSpecification $tagspec `
    -TimeRange @($timeRange)
```

Berikut ini adalah output contoh.

```
AssociationTarget     :
CronExpression        :
InstanceEventWindowId : iew-0abcdef1234567890
Name                  : my-event-window
State                 : creating
Tags                  : {key1}
TimeRanges            : {Amazon.EC2.Model.InstanceEventWindowTimeRange}
```

Untuk membuat jendela peristiwa dengan ekspresi cron

Gunakan New-EC2InstanceEventWindowcmdlet.

```
$tag = @{Key="key1"; Value="value1"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance-event-window"
$tagspec.Tags.Add($tag)
New-EC2InstanceEventWindow `
    -Name my-event-window `
```

```
    -TagSpecification $tagspec`
    -CronExpression "* 21-23 * * 2,3"
```

Berikut ini adalah output contoh.

```
AssociationTarget     :
CronExpression        : * 21-23 * * 2,3
InstanceEventWindowId : iew-0abcdef1234567890
Name                  : my-event-window
State                 : creating
Tags                  : {key1}
TimeRanges            : {}
```

Mengaitkan target dengan jendela peristiwa

Setelah Anda membuat jendela acara, Anda dapat mengaitkan target dengan jendela acara. Anda dapat mengaitkan hanya satu jenis target dengan jendela acara. Anda dapat menentukan instance IDs, Dedicated Host IDs, atau tag instance.

Console

Untuk mengaitkan target dengan jendela acara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Pilih jendela acara untuk memodifikasi.
4. Pilih Actions, Modify instance event window.

AWS CLI

Untuk mengaitkan tanda instans dengan jendela peristiwa

Gunakan perintah associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Untuk mengaitkan instance IDs dengan jendela acara

Gunakan perintah associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
```

```
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Untuk mengaitkan Host Khusus dengan jendela peristiwa

Gunakan perintah associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

PowerShell

Untuk mengaitkan tanda instans dengan jendela peristiwa

Gunakan Register-EC2InstanceEventWindowcmdlet.

```
$tag1 = @{Key="key1"; Value="value1"}
$tag2 = @{Key="key2"; Value="value2"}
```

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceTag @($tag1,$tag2)
```

Untuk mengaitkan instance IDs dengan jendela acara

Gunakan Register-EC2InstanceEventWindowcmdlet.

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceId i-1234567890abcdef0, i-0598c7d356eba48d7
```

Untuk mengaitkan Host Khusus dengan jendela peristiwa

Gunakan Register-EC2InstanceEventWindowcmdlet.

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_DedicatedHostId h-029fa35a02b99801d
```

Putuskan hubungan target dari jendela acara

Console

Untuk memisahkan target dengan jendela acara

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Pilih jendela acara untuk memodifikasi.
4. Pilih Actions, Modify instance event window.

AWS CLI

Untuk memisahkan tanda instans dari jendela peristiwa

Gunakan perintah disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
```

```
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Untuk memisahkan instance IDs dari jendela acara

Gunakan perintah disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Untuk memisahkan Host Khusus dari jendela peristiwa

Gunakan perintah disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

PowerShell

Untuk memisahkan tanda instans dari jendela peristiwa

Gunakan Unregister-EC2InstanceEventWindowcmdlet.

```
$tag1 = @{Key="key1"; Value="value1"}
$tag2 = @{Key="key2"; Value="value2"}
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceTag @($tag1, $tag2)
```

Untuk memisahkan instance IDs dari jendela acara

Gunakan Unregister-EC2InstanceEventWindowcmdlet.

```
Unregister-EC2InstanceEventWindow `
```

```
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceId i-1234567890abcdef0, i-0598c7d356eba48d7
```

Untuk memisahkan Host Khusus dari jendela peristiwa

Gunakan Unregister-EC2InstanceEventWindowcmdlet.

```
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_DedicatedHostId h-029fa35a02b99801d
```

Memodifikasi jendela acara

Anda dapat memodifikasi semua bidang jendela peristiwa kecuali ID-nya. Misalnya, saat musim panas dimulai, Anda mungkin ingin mengubah jadwal jendela peristiwa. Untuk jendela peristiwa yang ada, Anda mungkin ingin menambahkan atau menghapus target.

Anda dapat memodifikasi rentang waktu atau ekspresi cron saat memodifikasi jendela peristiwa, tetapi tidak keduanya.

Console

Untuk memodifikasi jendela peristiwa

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Pilih Tindakan, Kelola jendela peristiwa.
4. Pilih jendela peristiwa yang akan dimodifikasi, lalu pilih Tindakan, Modifikasi jendela peristiwa instans.
5. Modifikasi bidang pada jendela peristiwa, lalu pilih Modifikasi jendela peristiwa.

AWS CLI

Untuk memodifikasi rentang waktu jendela peristiwa

Gunakan perintah modify-instance-event-window.

```
aws ec2 modify-instance-event-window
```

```
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Untuk memodifikasi serangkaian rentang waktu pada jendela peristiwa

Gunakan perintah modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
```

```
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Untuk memodifikasi ekspresi cron jendela peristiwa

Gunakan perintah modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Berikut ini adalah output contoh.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

PowerShell

Untuk memodifikasi rentang waktu jendela peristiwa

Gunakan Edit-EC2InstanceEventWindowcmdlet.

```
$timeRange1 = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange1.StartWeekDay = "monday"
$timeRange1.EndWeekDay = "wednesday"
$timeRange1.StartHour = 2
$timeRange1.EndHour = 8
```

```
$timeRange2 = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange2.StartWeekDay = "thursday"
$timeRange2.EndWeekDay = "friday"
$timeRange2.StartHour = 1
$timeRange2.EndHour = 6
Edit-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -TimeRange @($timeRange1, $timeRange2)
```

Untuk memodifikasi ekspresi cron jendela peristiwa

Gunakan Edit-EC2InstanceEventWindowcmdlet.

```
Edit-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -CronExpression "* 21-23 * * 2,3"
```

Hapus jendela acara

Anda dapat menghapus satu jendela acara pada satu waktu.

Console

Untuk menghapus jendela peristiwa

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Peristiwa.
3. Pilih Tindakan, Kelola jendela peristiwa.
4. Pilih jendela peristiwa yang akan dihapus, lalu pilih Tindakan, Hapus jendela peristiwa instans.
5. Saat diminta, masukkan **delete**, lalu pilih Hapus.

AWS CLI

Untuk menghapus jendela peristiwa

Gunakan delete-instance-event-windowperintah dan tentukan jendela acara yang akan dihapus.

```
aws ec2 delete-instance-event-window \
```

```
    --instance-event-window-id iew-0abcdef1234567890
```

Untuk menghapus paksa jendela acara

Gunakan parameter `--force-delete` jika jendela peristiwa saat ini dikaitkan dengan target.

```
aws ec2 delete-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

PowerShell

Untuk menghapus jendela peristiwa

Gunakan Remove-EC2InstanceEventWindowcmdlet.

```
Remove-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890
```

Untuk menghapus paksa jendela acara

Gunakan Remove-EC2InstanceEventWindowcmdlet.

```
Remove-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -ForceDelete $true
```

Pantau instans Anda menggunakan CloudWatch

Anda dapat memantau instans menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari Amazon EC2 menjadi metrik yang dapat dibaca dan mendekati waktu nyata. Statistik ini dicatat untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa aplikasi atau layanan web Anda.

Secara default, Amazon EC2 mengirimkan data metrik ke CloudWatch dalam periode 5 menit. Untuk mengirim data metrik untuk instans Anda CloudWatch dalam periode 1 menit, Anda dapat mengaktifkan pemantauan terperinci pada instans. Untuk informasi selengkapnya, lihat Mengelola pemantauan terperinci untuk instans EC2 Anda.

Konsol Amazon EC2 menampilkan serangkaian grafik berdasarkan data mentah dari Amazon. CloudWatch Bergantung pada kebutuhan Anda, Anda mungkin lebih suka mendapatkan data untuk instans Anda dari Amazon CloudWatch daripada grafik di konsol.

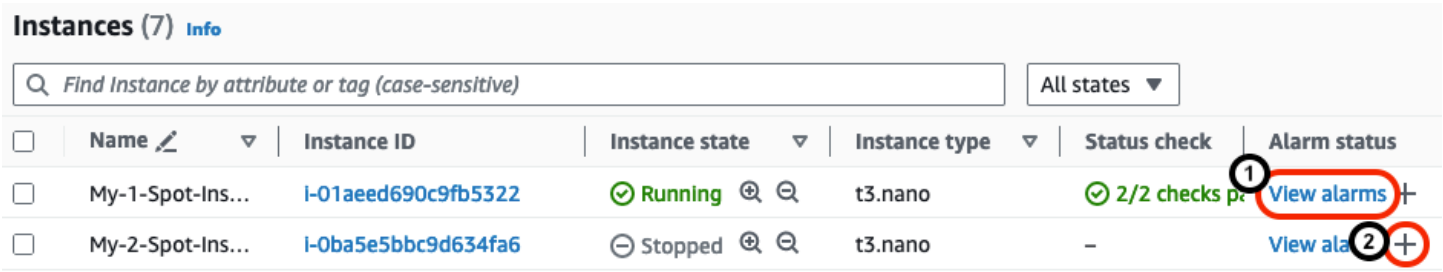
Untuk informasi CloudWatch penagihan dan biaya Amazon, lihat CloudWatch penagihan dan biaya di CloudWatch Panduan Pengguna Amazon.

Daftar Isi

- Mengelola CloudWatch alarm untuk instans EC2 Anda di konsol Amazon EC2
- Mengelola pemantauan terperinci untuk instans EC2 Anda
- CloudWatch metrik yang tersedia untuk instans Anda
- Instal dan konfigurasikan CloudWatch agen menggunakan konsol Amazon EC2 untuk menambahkan metrik tambahan
- Statistik untuk CloudWatch metrik untuk instans Anda
- Lihat grafik pemantauan untuk instans Anda
- Buat CloudWatch alarm untuk sebuah contoh
- Buat alarm yang menghentikan, mengakhiri, melakukan boot ulang, atau memulihkan instans

Mengelola CloudWatch alarm untuk instans EC2 Anda di konsol Amazon EC2

Dari layar Instans di konsol Amazon EC2, Anda dapat mengelola alarm CloudWatch Amazon untuk instans Anda. Dalam tabel Instans, kolom Status alarm menyediakan dua kontrol konsol: kontrol untuk melihat alarm, dan satu lagi untuk membuat atau mengeditnya. Tangkapan layar berikut menunjukkan kontrol konsol ini, bernomor 1 (Lihat alarm) dan 2 (tanda + untuk membuat atau mengedit alarm).



Melihat alarm dari layar Instans

Anda dapat melihat alarm setiap instans dari layar Instans.

Untuk melihat alarm instance dari layar Instances

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Dalam tabel Instances, untuk instance yang Anda pilih, pilih Lihat alarm (bernomor 1 pada tangkapan layar sebelumnya).
4. Di *i-1234567890abcdef0* jendela Detail alarm untuk, pilih nama alarm untuk melihat alarm di CloudWatch konsol.

Membuat alarm dari layar Instans

Anda dapat membuat alarm untuk setiap instance dari layar Instans.

Untuk membuat alarm untuk sebuah instance dari layar Instances

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Dalam tabel Instances, untuk contoh yang Anda pilih, pilih tanda plus (bernomor 2 pada tangkapan layar sebelumnya).
4. Di layar Kelola CloudWatch alarm, buat alarm Anda. Untuk informasi selengkapnya, lihat Buat CloudWatch alarm untuk sebuah contoh.

Mengedit alarm dari layar Instans

Anda dapat mengedit alarm untuk sebuah instance dari layar Instans.

Untuk mengedit alarm untuk sebuah instance dari layar Instances

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Dalam tabel Instances, untuk contoh yang Anda pilih, pilih tanda plus (bernomor 2 pada tangkapan layar sebelumnya).
4. Di layar Kelola CloudWatch alarm, edit alarm Anda. Untuk informasi selengkapnya, lihat Mengedit atau menghapus CloudWatch alarm di Panduan CloudWatch Pengguna Amazon.

Mengelola pemantauan terperinci untuk instans EC2 Anda

Amazon CloudWatch menyediakan dua kategori pemantauan: pemantauan dasar dan pemantauan terperinci. Secara default, instans Anda dikonfigurasi untuk pemantauan dasar. Anda dapat mengaktifkan pemantauan terperinci secara opsional untuk membantu Anda lebih cepat mengidentifikasi dan bertindak atas masalah operasional. Anda dapat mengaktifkan atau mematikan pemantauan terperinci saat peluncuran atau saat instance berjalan atau dihentikan.

Mengaktifkan pemantauan terperinci pada sebuah instans tidak memengaruhi pemantauan volume EBS terlampirnya. Untuk informasi selengkapnya, lihat CloudWatch Metrik Amazon untuk Amazon EBS.

Tabel berikut menyoroti perbedaan antara pemantauan dasar dan pemantauan terperinci untuk instans Anda.

Tipe pemantauan	Deskripsi	Biaya
Pemantauan dasar	Metrik pemeriksaan status tersedia dalam periode 1 menit. Semua metrik lainnya tersedia dalam periode 5 menit.	Tidak dikenai biaya.
Pemantauan terperinci	Anda bisa mendapatkan metrik dalam periode 1 menit, asalkan Anda mengaktifkan pemantauan terperinci untuk instance tersebut. Setelah mengaktifkan pemantauan terperinci, Anda dapat mengumpulkan data di seluruh grup instance serupa.	Anda dikenakan biaya per metrik yang dikirimkan Amazon EC2. CloudWatch Anda tidak dikenai biaya untuk penyimpanan data. Untuk informasi selengkapnya, lihat Tingkat berbayar di halaman CloudWatch harga Amazon.

Daftar Isi

- Izin yang diperlukan
- Aktifkan pemantauan terperinci saat peluncuran
- Kelola pemantauan terperinci

Izin yang diperlukan

Untuk mengaktifkan pemantauan terperinci pada instans, pengguna Anda harus memiliki izin untuk menggunakan tindakan API MonitorInstances. Untuk menonaktifkan pemantauan terperinci pada instans, pengguna Anda harus memiliki izin untuk menggunakan tindakan API UnmonitorInstances.

Aktifkan pemantauan terperinci saat peluncuran

Gunakan prosedur berikut untuk mengaktifkan pemantauan terperinci saat peluncuran. Secara default, instans Anda menggunakan pemantauan dasar.

Console

Untuk mengaktifkan pemantauan terperinci saat meluncurkan suatu instans

Saat meluncurkan instans menggunakan konsol Amazon EC2, di bawah Detail lanjutan, pilih kotak centang CloudWatch Pemantauan terperinci.

AWS CLI

Untuk mengaktifkan pemantauan terperinci saat meluncurkan suatu instans

Gunakan perintah run-instance dengan opsi. `--monitoring`

```
--monitoring Enabled=true
```

PowerShell

Untuk mengaktifkan pemantauan terperinci saat meluncurkan suatu instans

Gunakan New-EC2Instancecmdlet dengan parameter. `-Monitoring`

```
-Monitoring $true
```

Kelola pemantauan terperinci

Gunakan prosedur berikut untuk mengelola pemantauan terperinci untuk instance yang berjalan atau berhenti.

Console

Untuk mengelola pemantauan terperinci

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instans.
4. Pilih Tindakan, Pantau dan pecahkan masalah, Kelola pemantauan terperinci.
5. Pada halaman Pemantauan terperinci, untuk pemantauan terperinci, lakukan salah satu hal berikut:
   - Pemantauan terperinci - Pilih Aktifkan.
   - Pemantauan dasar - Hapus Aktifkan.
6. Pilih Konfirmasi.

AWS CLI

Untuk mengaktifkan pemantauan terperinci

Gunakan perintah monitor-instance berikut.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Untuk menonaktifkan pemantauan terperinci

Gunakan perintah unmonitor-instance.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk mengaktifkan pemantauan terperinci

Gunakan Start-EC2InstanceMonitoringcmdlet.

```
Start-EC2InstanceMonitoring -InstanceId i-1234567890abcdef0
```

Untuk menonaktifkan pemantauan terperinci

Gunakan Stop-EC2InstanceMonitoringcmdlet.

```
Stop-EC2InstanceMonitoring -InstanceId i-1234567890abcdef0
```

CloudWatch metrik yang tersedia untuk instans Anda

Amazon EC2 mengirimkan metrik ke Amazon. CloudWatch Anda dapat menggunakan, API Konsol Manajemen AWS AWS CLI, atau API untuk membuat daftar metrik yang dikirimkan Amazon EC2. CloudWatch Secara default, setiap titik data mencakup 5 menit yang mengikuti waktu mulai aktivitas untuk instans. Jika Anda telah mengaktifkan pemantauan terperinci, setiap poin data mencakup aktivitas menit berikutnya dari waktu mulai. Perhatikan bahwa untuk statistik Minimum, Maksimum, dan Rata-rata, perincian minimum untuk metrik yang disediakan EC2 adalah 1 menit.

Untuk informasi tentang cara melihat metrik yang tersedia menggunakan Konsol Manajemen AWS atau metrik AWS CLI, lihat Melihat metrik yang tersedia di CloudWatch Panduan Pengguna Amazon.

Untuk informasi cara mendapatkan statistik untuk metrik tersebut, lihat Statistik untuk CloudWatch metrik untuk instans Anda.

Daftar Isi

- Metrik instans
- Metrik akselerator
- Metrik kredit CPU
- Metrik Host Khusus
- Metrik Amazon EBS untuk instans berbasis Nitro
- Metrik pemeriksaan status
- Metrik pencerminan lalu lintas
- Metrik grup Auto Scaling
- Dimensi metrik Amazon EC2
- Metrik penggunaan Amazon EC2

Metrik instans

Namespace `AWS/EC2` mencakup metrik instans berikut.

Metrik	Deskripsi	Unit	Statistik yang bermakna
`CPUUtilization`	Persentase waktu CPU fisik yang digunakan Amazon EC2 untuk menjalankan instans EC2, yang mencakup waktu yang digunakan untuk menjalankan kode pengguna dan kode Amazon EC2. Pada tingkat yang sangat tinggi, `CPUUtilization` adalah jumlah `CPUUtilization` tamu dan `CPUUtilization` hypervisor. Alat dalam sistem operasi Anda dapat menunjukkan persentase yang berbeda dari CloudWatch faktor seperti simulasi perangkat lama, konfigurasi perangkat non-warisan, beban kerja interupsi berat, migrasi langsung, dan pembaruan langsung.	Percent	• Average • Minimum • Maximum
`DiskReadOps`	Operasi baca yang diselesaikan dari semua volume penyimpanan instans yang tersedia untuk instans tersebut dalam periode waktu yang ditentukan. Untuk menghitung rata-rata I/O operasi per detik (IOPS) untuk periode tersebut, bagilah total operasi dalam periode tersebut dengan jumlah detik dalam periode tersebut. Jika tidak ada volume penyimpanan instans, nilainya adalah 0 atau metrik tidak dilaporkan.	Count	• Sum • Average • Minimum • Maximum
`DiskWriteOps`	Operasi tulis yang diselesaikan ke semua volume penyimpanan instans yang tersedia untuk instans tersebut dalam periode waktu yang ditentukan.	Count	• Sum • Average • Minimum • Maximum

Metrik	Deskripsi	Unit	Statistik yang bermakna
	Untuk menghitung rata-rata I/O operasi per detik (IOPS) untuk periode tersebut, bagilah total operasi dalam periode tersebut dengan jumlah detik dalam periode tersebut. Jika tidak ada volume penyimpanan instans, nilainya adalah 0 atau metrik tidak dilaporkan.		

Metrik	Deskripsi	Unit	Statistik yang bermakna
`DiskReadBytes`	Bita yang dibaca dari semua volume penyimpanan instans yang tersedia untuk instans. Metrik ini digunakan untuk menentukan volume data yang dibaca aplikasi dari hard disk instans. Metrik ini dapat digunakan untuk menentukan kecepatan aplikasi. Jumlah yang dilaporkan adalah jumlah bita yang diterima selama periode tersebut. Jika menggunakan pemantauan dasar (5 menit), Anda dapat membagi jumlah ini dengan 300 untuk menemukan Bita/detik. Jika Anda memiliki pemantauan terperinci (1 menit), bagilah dengan 60. Anda juga dapat menggunakan fungsi matematika CloudWatch metrik `DIFF_TIME` untuk menemukan byte per detik. Misalnya, jika Anda telah membuat grafik `DiskReadBytes` CloudWatch sebagai`m1`, rumus matematika metrik `m1/(DIFF_TIME(m1))` mengembalikan metrik dalam byte/detik. Untuk informasi selengkapnya tentang `DIFF_TIME` dan fungsi matematika metrik lainnya, lihat Menggunakan matematika metrik di Panduan CloudWatch Pengguna Amazon. Jika tidak ada volume penyimpanan instans, nilainya adalah 0 atau metrik tidak dilaporkan.	Bytes	• Sum • Average • Minimum • Maximum

Metrik	Deskripsi	Unit	Statistik yang bermakna
`DiskWriteBytes`	Bita yang ditulis ke semua volume penyimpanan instans yang tersedia untuk instans. Metrik ini digunakan untuk menentukan volume data yang ditulis aplikasi ke hard disk instans. Metrik ini dapat digunakan untuk menentukan kecepatan aplikasi. Jumlah yang dilaporkan adalah jumlah bita yang diterima selama periode tersebut. Jika menggunakan pemantauan dasar (5 menit), Anda dapat membagi jumlah ini dengan 300 untuk menemukan Bita/detik. Jika Anda memiliki pemantauan terperinci (1 menit), bagilah dengan 60. Anda juga dapat menggunakan fungsi matematika CloudWatch metrik `DIFF_TIME` untuk menemukan byte per detik. Misalnya, jika Anda telah membuat grafik `DiskWriteBytes` CloudWatch sebagai`m1`, rumus matematika metrik `m1/(DIFF_TIME(m1))` mengembalikan metrik dalam byte/detik. Untuk informasi selengkapnya tentang `DIFF_TIME` dan fungsi matematika metrik lainnya, lihat Menggunakan matematika metrik di Panduan CloudWatch Pengguna Amazon. Jika tidak ada volume penyimpanan instans, nilainya adalah 0 atau metrik tidak dilaporkan.	Bytes	• Sum • Average • Minimum • Maximum

Metrik	Deskripsi	Unit	Statistik yang bermakna
`MetadataNoToken`	Berapa kali Layanan Metadata Instance (IMDS) berhasil diakses menggunakan metode yang tidak menggunakan token. Metrik ini digunakan untuk menentukan apakah ada proses yang mengakses metadata instance yang menggunakan Instance Metadata Service Version 1 (IMDSv1), yang tidak menggunakan token. Jika semua permintaan menggunakan sesi yang didukung token, yaitu, Layanan Metadata Instans Versi 2 (IMDSv2), nilainya adalah 0. Untuk informasi selengkapnya, lihat Transisi ke penggunaan Layanan Metadata Instans Versi 2.	Count	• Sum • Percentiles
`MetadataNoTokenRejected`	Berapa kali IMDSv1 panggilan dicoba setelah IMDSv1 dinonaktifkan. Jika metrik ini muncul, ini menunjukkan bahwa IMDSv1 panggilan telah dicoba dan ditolak. Anda dapat mengaktifkan kembali IMDSv1 atau memastikan semua panggilan Anda digunakan IMDSv2. Untuk informasi selengkapnya, lihat Transisi ke penggunaan Layanan Metadata Instans Versi 2.	Count	• Sum • Percentiles

Metrik	Deskripsi	Unit	Statistik yang bermakna
`NetworkIn`	Jumlah bita yang diterima oleh instans di semua antarmuka jaringan. Metrik ini mengidentifikasi volume lalu lintas jaringan yang masuk ke instans tunggal. Jumlah yang dilaporkan adalah jumlah bita yang diterima selama periode tersebut. Jika menggunakan pemantauan dasar (5 menit) dan statistiknya adalah Sum, Anda dapat membagi jumlah ini dengan 300 untuk menemukan Bita/detik. Jika Anda memiliki pemantauan terperinci (1 menit) dan statistiknya adalah Sum, bagilah dengan 60.	Bytes	• Sum • Average • Minimum • Maximum
`NetworkOut`	Jumlah bita yang dikirimkan oleh instans di semua antarmuka jaringan. Metrik ini mengidentifikasi volume lalu lintas jaringan yang keluar dari instans tunggal. Jumlah yang dilaporkan adalah jumlah bita yang dikirimkan selama periode tersebut. Jika menggunakan pemantauan dasar (5 menit) dan statistiknya adalah Sum, Anda dapat membagi jumlah ini dengan 300 untuk menemukan Bita/detik. Jika Anda memiliki pemantauan terperinci (1 menit) dan statistiknya adalah Sum, bagilah dengan 60.	Bytes	• Sum • Average • Minimum • Maximum

Metrik	Deskripsi	Unit	Statistik yang bermakna
`NetworkPackets In`	Jumlah paket yang diterima oleh instans di semua antarmuka jaringan. Metrik ini mengidentifikasi volume lalu lintas yang masuk dari segi jumlah paket pada instans tunggal. Metrik ini hanya tersedia untuk pemantauan dasar (periode 5 menit). Untuk menghitung jumlah paket per detik (PPS) yang diterima instans Anda selama 5 menit, bagi nilai Sum statistik dengan 300.	Count	• Sum • Average • Minimum • Maximum
`NetworkPackets Out`	Jumlah paket yang dikirimkan oleh instans di semua antarmuka jaringan. Metrik ini mengidentifikasi volume lalu lintas yang keluar dari segi jumlah paket pada instans tunggal. Metrik ini hanya tersedia untuk pemantauan dasar (periode 5 menit). Untuk menghitung jumlah paket per detik (PPS) yang dikirim oleh instans Anda selama 5 menit, bagilah nilai statistik Sum dengan 300.	Count	• Sum • Average • Minimum • Maximum

Metrik akselerator

`AWS/EC2`Namespace menyertakan metrik akselerator berikut untuk instans komputasi yang dipercepat. Hanya didukung pada subset tipe instans komputasi yang dipercepat.

Metrik	Deskripsi	Unit	Statistik yang bermakna
`GPUPowerUtilization`	Penggunaan daya aktif sebagai persentase daya aktif maksimum.	Persen	• Average • Minimum • Maximum

Metrik kredit CPU

Namespace `AWS/EC2` mencakup metrik kredit CPU berikut untuk instans performa yang dapat melonjak.

Metrik	Deskripsi	Unit	Statistik yang bermakna
`CPUCreditUsage`	Jumlah kredit CPU yang digunakan oleh instans untuk pemanfaatan CPU. Satu kredit CPU sama dengan satu vCPU yang berjalan pada pemanfaatan 100% selama satu menit atau kombinasi yang setara dari CPUs v, pemanfaatan, dan waktu (misalnya, satu vCPU berjalan pada pemanfaatan 50% selama dua menit atau dua CPUs v berjalan pada pemanfaatan 25% selama dua menit). Metrik kredit CPU hanya tersedia dengan frekuensi 5 menit. Jika Anda menentukan periode lebih dari lima menit, gunakan statistik `Sum`, bukan statistik `Average`.	Kredit (Menit vCPU)	• Sum • Average • Minimum • Maximum
`CPUCreditBalance`	Jumlah kredit CPU yang diperoleh yang diakumulasi oleh instans sejak diluncurkan atau dimulai. Untuk T2 Standar, `CPUCreditBalance` juga mencakup jumlah kredit peluncuran yang telah diakumulasi. Kredit diakumulasi ke saldo kredit setelah diperoleh, dan dihapus dari saldo kredit saat digunakan. Saldo kredit memiliki batas maksimum, yang ditentukan oleh ukuran instans. Setelah batas tercapai, setiap kredit yang baru diperoleh akan dibuang. Untuk T2 Standar, kredit peluncuran tidak termasuk dalam penghitungan batas.	Kredit (Menit vCPU)	• Sum • Average • Minimum • Maximum

Metrik	Deskripsi	Unit	Statistik yang bermakna
	Kredit dalam `CPUCreditBalance` tersedia untuk instans untuk digunakan hingga melonjak melebihi pemanfaatan CPU acuan. Saat sebuah instans berjalan, kredit dalam `CPUCreditBalance` tidak akan kedaluwarsa. Saat instans T3 atau T3a berhenti, nilai `CPUCreditBalance` akan bertahan selama tujuh hari. Setelah itu, semua kredit yang dikumpulkan akan hilang. Saat instans T2 berhenti, nilai `CPUCreditBalance` tidak bertahan, dan semua kredit yang masih harus dibayar hilang. Metrik kredit CPU hanya tersedia dengan frekuensi 5 menit.		
`CPUSurplusCreditBalance`	Jumlah kredit surplus yang telah digunakan oleh instans `unlimited` saat nilai `CPUCreditBalance` miliknya adalah nol. Nilai `CPUSurplusCreditBalance` dibayarkan oleh dengan kredit CPU yang diperoleh. Jika jumlah kredit surplus melebihi jumlah kredit maksimum yang dapat diperoleh instans dalam jangka waktu 24 jam, kredit surplus yang digunakan di atas jumlah maksimum akan dikenai biaya tambahan. Metrik kredit CPU hanya tersedia dengan frekuensi 5 menit.	Kredit (Menit vCPU)	• Sum • Average • Minimum • Maximum

Metrik	Deskripsi	Unit	Statistik yang bermakna
`CPUSurplusCreditsCharged`	Jumlah kredit surplus yang digunakan yang tidak ditutupi oleh kredit CPU yang diperoleh, sehingga menimbulkan biaya tambahan. Kredit surplus yang digunakan akan dikenai biaya jika salah satu dari hal berikut terjadi: • Kredit surplus yang digunakan melampaui jumlah kredit maksimum yang bisa didapatkan oleh instans dalam periode 24 jam. Kredit surplus yang digunakan di atas jumlah maksimum akan dikenai biaya pada akhir jam. • Instans dihentikan atau diakhiri. • instans dialihkan dari `unlimited` ke `standard`. Metrik kredit CPU hanya tersedia dengan frekuensi 5 menit.	Kredit (Menit vCPU)	• Sum • Average • Minimum • Maximum

Metrik Host Khusus

Namespace `AWS/EC2` mencakup metrik berikut untuk Host Khusus T3.

Metrik	Deskripsi	Unit	Statistik yang bermakna
`DedicatedHostCPUUtilization`	Persentase alokasi kapasitas komputasi yang saat ini digunakan oleh instans yang berjalan di Host Khusus.	Percent	• Sum • Average • Minimum • Maximum

Metrik Amazon EBS untuk instans berbasis Nitro

Namespace AWS/EC2 mencakup metrik Amazon EBS tambahan untuk volume yang dipasangkan ke instans berbasis Nitro yang bukan merupakan instans bare metal.

Metrik	Deskripsi	Unit	Statistik yang bermakna
InstanceEBSIOPSExceededCheck	Melaporkan apakah aplikasi mencoba mendorong IOPS yang melebihi batas maksimum IOPS EBS untuk instans dalam menit terakhir. Metrik ini dapat berupa 0 (IOPS tidak terlampaui) atau 1 (IOPS terlampaui).	Tidak ada	• Jumlah • Rata-rata • Minimum • Maksimum
InstanceEBSThroughputExceededCheck	Melaporkan apakah aplikasi mencoba mendorong throughput yang melebihi batas throughput EBS maksimum untuk instans dalam menit terakhir. Metrik ini dapat berupa 0 (throughput tidak terlampaui) atau 1 (throughput terlampaui).	Tidak ada	• Jumlah • Rata-rata • Minimum • Maksimum
EBSReadOps	Operasi baca yang diselesaikan dari semua volume Amazon EBS yang dilampirkan ke instans dalam periode waktu yang ditentukan. Untuk menghitung I/O operasi baca rata-rata per detik (Baca IOPS) untuk periode tersebut, bagilah total operasi dalam periode tersebut dengan jumlah detik dalam periode tersebut. Jika menggunakan pemantauan dasar (5 menit), Anda dapat membagi jumlah ini dengan 300 untuk menghitung nilai IOPS Baca. Jika Anda memiliki pemantauan terperinci (1 menit), bagilah dengan 60. Anda juga dapat menggunakan fungsi matematika CloudWatch metrik DIFF_TIME untuk menemukan operasi per detik. Misalnya, jika Anda telah membuat grafik EBSReadOps CloudWatc	Hitungan	• Jumlah • Rata-rata • Minimum • Maksimum

Metrik	Deskripsi	Unit	Statistik yang bermakna
	h sebagaim1, rumus matematika metrik `m1/(DIFF_TIME(m1))` mengembalikan metrik dalam operasi/detik. Untuk informasi selengkapnya tentang `DIFF_TIME` dan fungsi matematika metrik lainnya, lihat Menggunakan matematika metrik di Panduan CloudWatch Pengguna Amazon.		
`EBSWriteOps`	Operasi tulis yang diselesaikan ke semua volume EBS yang dilampirkan pada instans tersebut dalam periode waktu yang ditentukan. Untuk menghitung I/O operasi tulis rata-rata per detik (Tulis IOPS) untuk periode tersebut, bagilah total operasi dalam periode tersebut dengan jumlah detik dalam periode tersebut. Jika menggunakan pemantauan dasar (5 menit), Anda dapat membagi angka ini dengan 300 untuk menghitung nilai IOPS Tulis. Jika Anda memiliki pemantauan terperinci (1 menit), bagilah dengan 60. Anda juga dapat menggunakan fungsi matematika CloudWatch metrik `DIFF_TIME` untuk menemukan operasi per detik. Misalnya, jika Anda telah membuat grafik `EBSWriteOps` CloudWatch sebagaim1, rumus matematika metrik `m1/(DIFF_TIME(m1))` mengembalikan metrik dalam operasi/detik. Untuk informasi selengkapnya tentang `DIFF_TIME` dan fungsi matematika metrik lainnya, lihat Menggunakan matematika metrik di Panduan CloudWatch Pengguna Amazon.	Hitungan	• Jumlah • Rata-rata • Minimum • Maksimum

Metrik	Deskripsi	Unit	Statistik yang bermakna
`EBSReadBytes`	Bita yang dibaca dari semua volume EBS yang dilampirkan ke instans dalam jangka waktu tertentu. Jumlah yang dilaporkan adalah jumlah bita baca selama periode tersebut. Jika menggunakan pemantauan dasar (5 menit), Anda dapat membagi angka ini dengan 300 untuk menemukan Bita/detik dari Pembacaan. Jika Anda memiliki pemantauan terperinci (1 menit), bagilah dengan 60. Anda juga dapat menggunakan fungsi matematika CloudWatch metrik `DIFF_TIME` untuk menemukan byte per detik. Misalnya, jika Anda telah membuat grafik `EBSReadBytes` CloudWatch sebagai`m1`, rumus matematika metrik `m1/(DIFF_TIME(m1))` mengembalikan metrik dalam byte/detik. Untuk informasi selengkapnya tentang `DIFF_TIME` dan fungsi matematika metrik lainnya, lihat Menggunakan matematika metrik di Panduan CloudWatch Pengguna Amazon.	Byte	• Jumlah • Rata-rata • Minimum • Maksimum

Metrik	Deskripsi	Unit	Statistik yang bermakna
`EBSWriteBytes`	Bita yang ditulis ke semua volume EBS yang dilampirkan ke instans dalam jangka waktu tertentu. Jumlah yang dilaporkan adalah jumlah bita tulis selama periode tersebut. Jika menggunakan pemantauan dasar (5 menit), Anda dapat membagi jumlah ini dengan 300 untuk menemukan Bita/detik dari Penulisan. Jika Anda memiliki pemantauan terperinci (1 menit), bagilah dengan 60. Anda juga dapat menggunakan fungsi matematika CloudWatch metrik `DIFF_TIME` untuk menemukan byte per detik. Misalnya, jika Anda telah membuat grafik `EBSWriteBytes` CloudWatch sebagai`m1`, rumus matematika metrik `m1/(DIFF_TIME(m1))` mengembalikan metrik dalam byte/detik. Untuk informasi selengkapnya tentang `DIFF_TIME` dan fungsi matematika metrik lainnya, lihat Menggunakan matematika metrik di Panduan CloudWatch Pengguna Amazon.	Byte	• Jumlah • Rata-rata • Minimum • Maksimum
`EBSIOBalance%`	Memberikan informasi tentang persentase I/O kredit yang tersisa di ember burst. Metrik ini hanya tersedia untuk pemantauan dasar. Metrik ini hanya tersedia untuk beberapa ukuran instans `*.4xlarge` dan yang lebih kecil, yang melonjak hingga performa maksimum hanya selama 30 menit setidaknya setiap 24 jam sekali. Statistik `Sum` tidak berlaku untuk metrik ini.	Persen	• Minimum • Maksimum

Metrik	Deskripsi	Unit	Statistik yang bermakna
`EBSByteBalance%`	Memberikan informasi tentang persentase kredit throughput yang tersisa di bucket lonjakan. Metrik ini hanya tersedia untuk pemantauan dasar. Metrik ini hanya tersedia untuk beberapa ukuran instans `*.4xlarge` dan yang lebih kecil, yang melonjak hingga performa maksimum hanya selama 30 menit setidaknya setiap 24 jam sekali. Statistik `Sum` tidak berlaku untuk metrik ini.	Persen	• Minimum • Maksimum

Untuk informasi tentang metrik yang disediakan untuk volume EBS Anda, lihat Metrik untuk volume Amazon EBS di Panduan Pengguna Amazon EBS. Untuk informasi tentang metrik yang disediakan untuk Armada EC2 dan Armada Spot Anda, lihat. Pantau Armada EC2 atau Armada Spot Anda menggunakan CloudWatch

Metrik pemeriksaan status

Secara default, metrik pemeriksaan status tersedia dalam frekuensi 1 menit tanpa dikenai biaya. Untuk instans yang baru diluncurkan, data metrik pemeriksaan status hanya tersedia setelah instans tersebut menyelesaikan status inisialisasi (dalam waktu beberapa menit setelah instans memasuki status `running`). Untuk informasi selengkapnya tentang pemeriksaan status EC2, lihat Pemeriksaan status untuk instans Amazon EC2.

Namespace `AWS/EC2` mencakup metrik pemeriksaan status berikut.

Metrik	Deskripsi	Unit	Statistik yang bermakna
`StatusCheckFailed`	Melaporkan apakah instans telah lulus semua pemeriksaan status di menit terakhir. Metrik ini dapat berupa `0` (lulus) atau `1` (gagal).	Count	• Average • Minimum • Maximum

Metrik	Deskripsi	Unit	Statistik yang bermakna
	Secara default, metrik ini tersedia dalam frekuensi 1 menit tanpa dikenai biaya.		
`StatusCheckFailed_Instance`	Melaporkan apakah instans telah melalui pemeriksaan status instan pada menit terakhir. Metrik ini dapat berupa `0` (lulus) atau `1` (gagal). Secara default, metrik ini tersedia dalam frekuensi 1 menit tanpa dikenai biaya.	Count	• Average • Minimum • Maximum
`StatusCheckFailed_System`	Melaporkan apakah instans telah melalui pemeriksaan status sistem pada menit terakhir. Metrik ini dapat berupa `0` (lulus) atau `1` (gagal). Secara default, metrik ini tersedia dalam frekuensi 1 menit tanpa dikenai biaya.	Count	• Average • Minimum • Maximum
`StatusCheckFailed_AttachedEBS`	Melaporkan apakah instans telah melalui pemeriksaan status EBS yang terlampir pada menit terakhir. Metrik ini dapat berupa `0` (lulus) atau `1` (gagal). Secara default, metrik ini tersedia dalam frekuensi 1 menit tanpa dikenai biaya.	Count	• Average • Minimum • Maximum

`AWS/EBS`Namespace menyertakan metrik pemeriksaan status berikut.

Metrik	Deskripsi	Unit	Statistik yang bermakna
`VolumeStalledIOCheck`	Catatan: Khusus instans Nitro. Tidak dipublikasikan untuk volume yang dilampirkan ke Amazon ECS dan AWS Fargate tugas.	Tidak ada	• Average • Minimum • Maximum

Metrik	Deskripsi	Unit	Statistik yang bermakna
	Melaporkan apakah volume telah lulus atau gagal pemeriksaan IO yang macet di menit terakhir. Metrik ini dapat berupa `0` (lulus) atau `1` (gagal).		

Metrik pencerminan lalu lintas

Namespace `AWS/EC2` mencakup metrik untuk lalu lintas yang dicerminkan. Untuk informasi selengkapnya, lihat Memantau lalu lintas cermin menggunakan Amazon CloudWatch di Panduan Pencerminan Lalu Lintas VPC Amazon.

Metrik grup Auto Scaling

Namespace `AWS/AutoScaling` mencakup metrik untuk grup Auto Scaling. Untuk informasi selengkapnya, lihat Monitor CloudWatch metrik untuk grup dan instans Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling.

Dimensi metrik Amazon EC2

Anda dapat menggunakan dimensi berikut untuk mempersempit metrik yang terdaftar pada tabel sebelumnya.

Dimensi	Deskripsi
`AutoScalingGroupName`	Dimensi ini memfilter data yang Anda minta untuk semua instans dalam grup kapasitas yang ditentukan. Grup Auto Scaling adalah kumpulan instans yang Anda tentukan jika menggunakan Penskalaan Otomatis. Dimensi ini hanya tersedia untuk metrik Amazon EC2 ketika instans berada dalam grup Auto Scaling. Tersedia untuk instans dengan Pemantauan Terperinci atau Dasar yang diaktifkan.
`ImageId`	Dimensi ini memfilter data yang Anda minta untuk semua instans yang menjalankan Amazon Machine Image (AMI)

Dimensi	Deskripsi
	Amazon EC2 ini. Tersedia untuk instans dengan Pemantauan Terperinci yang diaktifkan.
`InstanceId`	Dimensi ini hanya memfilter data yang Anda minta untuk instans yang teridentifikasi. Hal ini membantu Anda menemukan instans yang tepat untuk memantau data.
`InstanceType`	Dimensi ini memfilter data yang Anda minta untuk semua instans yang berjalan dengan tipe instans yang ditentukan ini. Hal ini membantu Anda mengategorikan data berdasarkan tipe instans yang berjalan. Misalnya, Anda dapat membandin gkan data dari instans m1.small dan instans m1.large untuk menentukan instans yang memiliki nilai bisnis yang lebih baik bagi aplikasi Anda. Tersedia untuk instans dengan Pemantauan Terperinci yang diaktifkan.

Metrik penggunaan Amazon EC2

Anda dapat menggunakan metrik CloudWatch penggunaan untuk memberikan visibilitas ke dalam penggunaan sumber daya akun Anda. Gunakan metrik ini untuk memvisualisasikan penggunaan layanan Anda saat ini pada CloudWatch grafik dan dasbor.

Metrik penggunaan Amazon EC2 sesuai dengan kuota layanan. AWS Anda dapat mengonfigurasi alarm yang memberi tahu Anda saat penggunaan mendekati kuota layanan. Untuk informasi selengkapnya tentang CloudWatch integrasi dengan kuota layanan, lihat metrik AWS penggunaan di CloudWatch Panduan Pengguna Amazon.

Amazon EC2 menerbitkan metrik berikut di namespace `AWS/Usage`.

Metrik	Deskripsi
`ResourceCount`	Jumlah sumber daya yang ditentukan yang berjalan di akun Anda. Sumber daya tersebut ditentukan oleh dimensi yang dikaitkan dengan metrik.

Metrik	Deskripsi
	Statistik yang paling berguna untuk metrik ini adalah `MAXIMUM`, yang merepresentasikan jumlah maksimum sumber daya yang digunakan selama periode 1 menit.

Dimensi berikut digunakan untuk menyempurnakan metrik penggunaan yang diterbitkan oleh Amazon EC2.

Dimensi	Deskripsi
`Service`	Nama AWS layanan yang berisi sumber daya. Untuk metrik penggunaan Amazon EC2, nilai untuk dimensi ini adalah `EC2`.
`Type`	Tipe entitas yang dilaporkan. Saat ini, satu-satunya nilai yang valid untuk metrik penggunaan Amazon EC2 adalah `Resource`.
`Resource`	Tipe sumber daya yang sedang berjalan. Saat ini, satu-satunya nilai yang valid untuk metrik penggunaan Amazon EC2 adalah `vCPU`, yang mengembalikan informasi tentang instans yang sedang berjalan.
`Class`	Kelas sumber daya yang dilacak. Untuk metrik penggunaan Amazon EC2 dengan `vCPU` sebagai nilai dimensi `Resource`, nilai yang valid adalah `Standard/OnDemand` , `F/OnDemand` , `G/OnDemand` , `Inf/OnDemand` , `P/OnDemand` , dan `X/OnDemand` . Nilai untuk dimensi ini menentukan huruf pertama dari tipe instans yang dilaporkan oleh metrik. Misalnya, `Standard/OnDemand` mengembalikan informasi terkait semua instans yang berjalan dengan tipe yang dimulai dengan A, C, D, H, I, M, R, T, dan Z, lalu `G/OnDemand` mengembalikan informasi terkait semua instans yang berjalan dengan tipe yang dimulai dengan G.

Instal dan konfigurasikan CloudWatch agen menggunakan konsol Amazon EC2 untuk menambahkan metrik tambahan

Menginstal dan mengonfigurasi CloudWatch agen menggunakan konsol Amazon EC2 dalam versi beta untuk Amazon EC2 dan dapat berubah sewaktu-waktu.

Secara default, Amazon CloudWatch menyediakan metrik dasar, seperti `CPUUtilization` dan`NetworkIn`, untuk memantau instans Amazon EC2 Anda. Untuk mengumpulkan metrik tambahan, Anda dapat menginstal CloudWatch agen pada instans EC2, lalu mengonfigurasi agen untuk memancarkan metrik yang dipilih. Alih-alih menginstal dan mengonfigurasi CloudWatch agen secara manual pada setiap instans EC2, Anda dapat menggunakan konsol Amazon EC2 untuk melakukannya untuk Anda.

Anda dapat menggunakan konsol Amazon EC2 untuk menginstal CloudWatch agen pada instans Anda dan mengonfigurasi agen untuk memancarkan metrik yang dipilih.

Atau, untuk menyelesaikan proses ini secara manual, lihat Menginstal CloudWatch agen di Panduan CloudWatch Pengguna Amazon. Untuk informasi selengkapnya tentang CloudWatch agen, lihat Mengumpulkan metrik, log, dan jejak menggunakan CloudWatch agen.

Daftar Isi

- Prasyarat
- Cara kerjanya
- Biaya
- Instal dan konfigurasikan CloudWatch agen

Prasyarat

Untuk menggunakan Amazon EC2 untuk menginstal dan mengonfigurasi CloudWatch agen, Anda harus memenuhi prasyarat pengguna dan instans yang dijelaskan di bagian ini.

> **Tip**
>
> Fitur ini tidak tersedia di semua Wilayah AWS. Jika item menu yang dijelaskan dalam prosedur penginstalan di halaman ini tidak ada di konsol Amazon EC2 dan Anda fleksibel

tentang di mana instans Anda berjalan, coba Wilayah lain. Jika tidak, Anda dapat menggunakan petunjuk manual di Panduan CloudWatch Pengguna Amazon untuk menginstal dan mengonfigurasi agen.

Prasyarat pengguna

Untuk menggunakan fitur ini, pengguna atau peran konsol IAM Anda harus memiliki izin yang diperlukan untuk menggunakan Amazon EC2 dan izin IAM berikut:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Prasyarat instans

- Status contoh: `running`
- Sistem operasi yang didukung: Linux
- AWS Systems Manager Agen (Agen SSM): Dipasang. Dua catatan tentang Agen SSM:
  - Agen SSM sudah diinstal sebelumnya di beberapa Amazon Machine Images (AMIs) yang disediakan oleh AWS dan pihak ketiga tepercaya. Untuk informasi tentang dukungan AMIs dan petunjuk untuk menginstal Agen SSM, lihat Amazon Machine Images (AMIs) dengan Agen SSM yang telah diinstal sebelumnya di Panduan Pengguna.AWS Systems Manager
  - Jika Anda mengalami masalah dengan Agen SSM, lihat Memecahkan Masalah Agen SSM di Panduan Pengguna.AWS Systems Manager
- Izin IAM untuk instance: Kebijakan AWS terkelola berikut harus ditambahkan ke peran IAM yang dilampirkan ke instance:
  - Amazon SSMManaged InstanceCore — Mengaktifkan instans untuk menggunakan Systems Manager untuk menginstal dan mengonfigurasi CloudWatch agen.
  - CloudWatchAgentServerPolicy— Memungkinkan sebuah instance untuk menggunakan CloudWatch agen untuk menulis data ke CloudWatch.

  Untuk informasi tentang cara menambahkan izin IAM ke instans Anda, lihat Menggunakan profil instans di Panduan Pengguna IAM.

Cara kerjanya

Sebelum Anda dapat menggunakan konsol Amazon EC2 untuk menginstal dan mengonfigurasi CloudWatch agen, Anda harus memastikan bahwa pengguna atau peran IAM Anda, dan instance yang ingin Anda tambahkan metrik, memenuhi prasyarat tertentu. Kemudian, Anda dapat menggunakan konsol Amazon EC2 untuk menginstal dan mengonfigurasi CloudWatch agen pada instans yang Anda pilih.

Pertama memenuhi prasyarat

- Anda memerlukan izin IAM yang diperlukan — Sebelum memulai, pastikan bahwa pengguna atau peran konsol Anda memiliki izin IAM yang diperlukan untuk menggunakan fitur ini.

- Instans — Untuk menggunakan fitur ini, instans EC2 Anda harus instans Linux, memiliki Agen SSM diinstal, memiliki izin IAM yang diperlukan, dan berjalan.

Kemudian Anda dapat menggunakan fitur tersebut

1. Pilih instans Anda — Di konsol Amazon EC2, Anda memilih instans untuk menginstal dan mengonfigurasi agen. CloudWatch Anda kemudian memulai proses dengan memilih Configure CloudWatch agent.
2. Validasi Agen SSM - Amazon EC2 memeriksa apakah Agen SSM diinstal dan dimulai pada setiap instance. Setiap contoh yang gagal pemeriksaan ini dikecualikan dari proses. Agen SSM digunakan untuk melakukan tindakan pada instance selama proses ini.
3. Validasi izin IAM — Amazon EC2 memeriksa bahwa setiap instans memiliki izin IAM yang diperlukan untuk proses ini. Setiap contoh yang gagal pemeriksaan ini dikecualikan dari proses. Izin IAM memungkinkan CloudWatch agen untuk mengumpulkan metrik dari instance dan berintegrasi dengan menggunakan Agen AWS Systems Manager SSM.
4. CloudWatch Agen validasi — Amazon EC2 memeriksa apakah agen diinstal dan dijalankan pada setiap instance. CloudWatch Jika ada instans yang gagal dalam pemeriksaan ini, Amazon EC2 menawarkan untuk menginstal dan memulai CloudWatch agen untuk Anda. CloudWatch Agen akan mengumpulkan metrik yang dipilih pada setiap instance setelah proses ini selesai.
5. Pilih konfigurasi metrik — Anda memilih metrik yang akan dipancarkan CloudWatch agen dari instans Anda. Setelah dipilih, Amazon EC2 menyimpan file konfigurasi di Parameter Store, di mana ia tetap sampai proses selesai. Amazon EC2 akan menghapus file konfigurasi dari Parameter Store kecuali prosesnya terganggu. Perhatikan bahwa jika Anda tidak memilih metrik, tetapi sebelumnya Anda menambahkannya ke instance Anda, metrik tersebut akan dihapus dari instance Anda saat proses ini selesai.
6. Perbarui konfigurasi CloudWatch agen - Amazon EC2 mengirimkan konfigurasi metrik ke agen. CloudWatch Ini adalah langkah terakhir dalam prosesnya. Jika berhasil, instans Anda dapat memancarkan data untuk metrik yang dipilih dan Amazon EC2 menghapus file konfigurasi dari Parameter Store.

Biaya

Metrik tambahan yang Anda tambahkan selama proses ini ditagih sebagai metrik khusus. Untuk informasi selengkapnya tentang harga CloudWatch metrik, lihat CloudWatch Harga Amazon.

Instal dan konfigurasikan CloudWatch agen

Anda dapat menggunakan konsol Amazon EC2 untuk menginstal dan mengonfigurasi CloudWatch agen untuk menambahkan metrik tambahan.

> **Note**
>
> Setiap kali Anda melakukan prosedur ini, Anda menimpa konfigurasi CloudWatch agen yang ada. Jika Anda tidak memilih metrik yang dipilih sebelumnya, metrik tersebut akan dihapus dari instance.

Untuk menginstal dan mengonfigurasi CloudWatch agen menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance untuk menginstal dan mengkonfigurasi CloudWatch agen.
4. Pilih Tindakan, Pantau dan pecahkan masalah, Konfigurasikan CloudWatch agen.
5. Untuk setiap langkah dalam proses, baca teks konsol, lalu pilih Berikutnya.
6. Untuk menyelesaikan proses, pada langkah terakhir, pilih Lengkap.

Untuk memperbarui konfigurasi agen yang dibuat oleh konsol Amazon EC2

Anda dapat secara manual menyesuaikan konfigurasi yang dibuat konsol EC2. Untuk informasi selengkapnya, lihat Membuat atau mengedit file konfigurasi CloudWatch agen secara manual di Panduan CloudWatch Pengguna Amazon.

Statistik untuk CloudWatch metrik untuk instans Anda

Anda bisa mendapatkan statistik untuk CloudWatch metrik untuk instans Anda. Statistik adalah agregasi data metrik selama periode waktu tertentu. CloudWatch menyediakan statistik berdasarkan titik data metrik yang disediakan oleh data kustom Anda atau disediakan oleh layanan lain di dalamnya AWS CloudWatch. Agregasi dilakukan menggunakan namespace, nama metrik, dimensi, dan unit titik data dari ukuran, dalam periode waktu yang Anda tentukan. Tabel berikut menjelaskan statistik yang tersedia.

Statistik	Deskripsi
`Minimum`	Nilai terendah yang diamati selama periode yang ditentukan. Anda dapat menggunakan nilai ini untuk menentukan volume aktivitas yang rendah pada aplikasi Anda.
`Maximum`	Nilai tertinggi yang diamati selama periode yang ditentukan. Anda dapat menggunakan nilai ini untuk menentukan volume aktivitas yang tinggi pada aplikasi Anda.
`Sum`	Semua nilai yang dikirimkan untuk metrik yang cocok disatukan. Statistik ini dapat berguna untuk menentukan total volume metrik.
`Average`	Nilai dari `Sum` / `SampleCount` selama periode yang ditentukan. Dengan membandingkan statistik ini dengan `Minimum` dan `Maximum`, Anda dapat menentukan cakupan suatu metrik dan seberapa dekat rata-rata penggunaa n dengan `Minimum` dan `Maximum`. Perbandingan ini membantu Anda untuk mengetahui kapan harus menambah atau mengurangi sumber daya Anda sesuai kebutuhan.
`SampleCou nt`	Hitungan (jumlah) titik data yang digunakan untuk penghitungan statistik.
`pNN.NN`	Nilai persentil yang ditentukan. Anda dapat menentukan persentil apa pun, menggunakan hingga dua tempat desimal (misalnya, p95.45).

Daftar Isi

- Mendapatkan statistik untuk instans tertentu
- Mengagregasi statistik di seluruh instans
- Mengagregasi statistik menurut grup Auto Scaling
- Mengagregasi statistik menurut AMI

Mendapatkan statistik untuk instans tertentu

Anda dapat menggunakan Konsol Manajemen AWS atau AWS CLI untuk mendapatkan statistik untuk contoh tertentu. Contoh berikut menunjukkan kepada Anda cara menggunakan Konsol

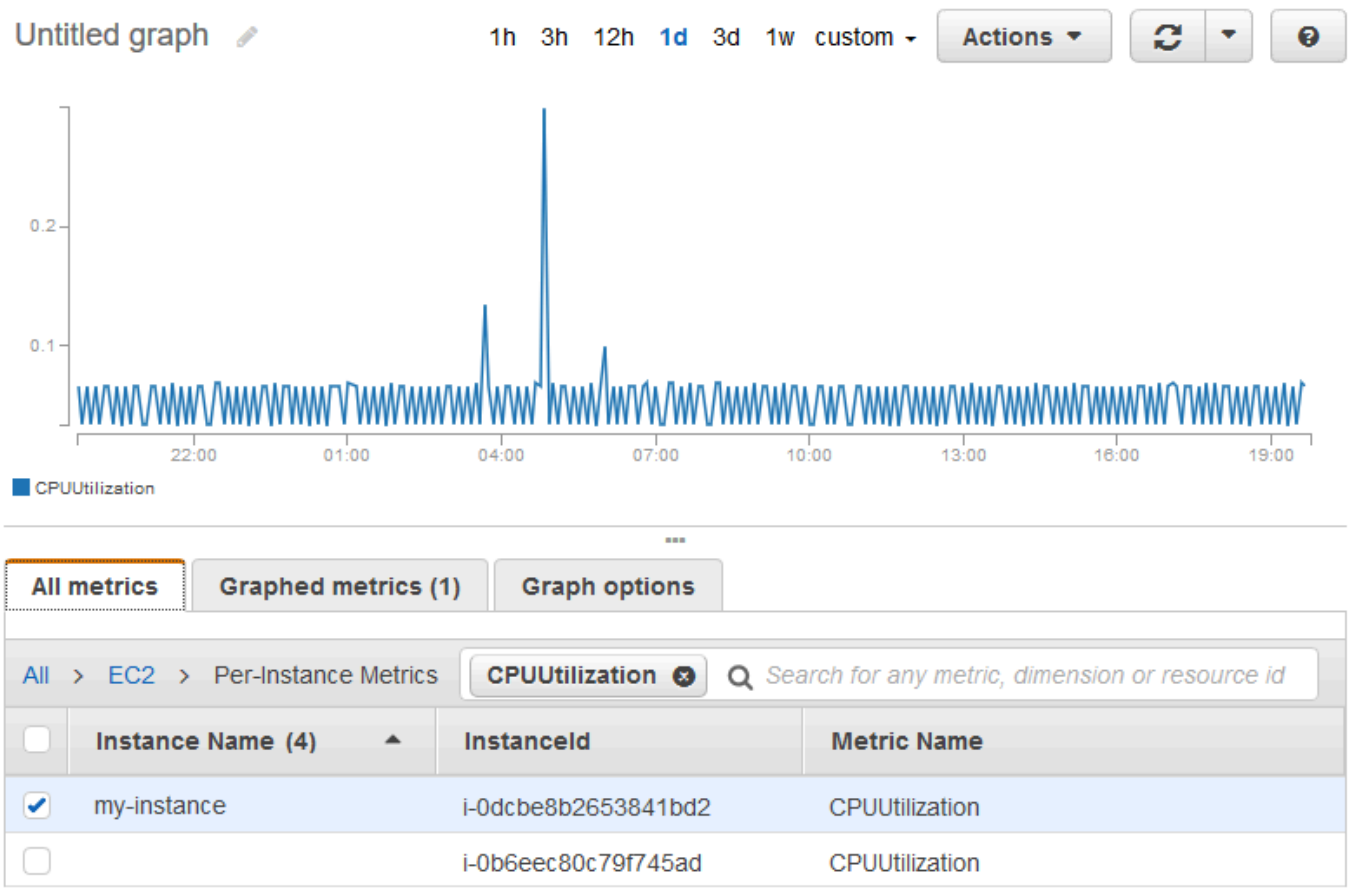
Manajemen AWS atau AWS CLI untuk menentukan pemanfaatan CPU maksimum dari instans EC2 tertentu.

Persyaratan

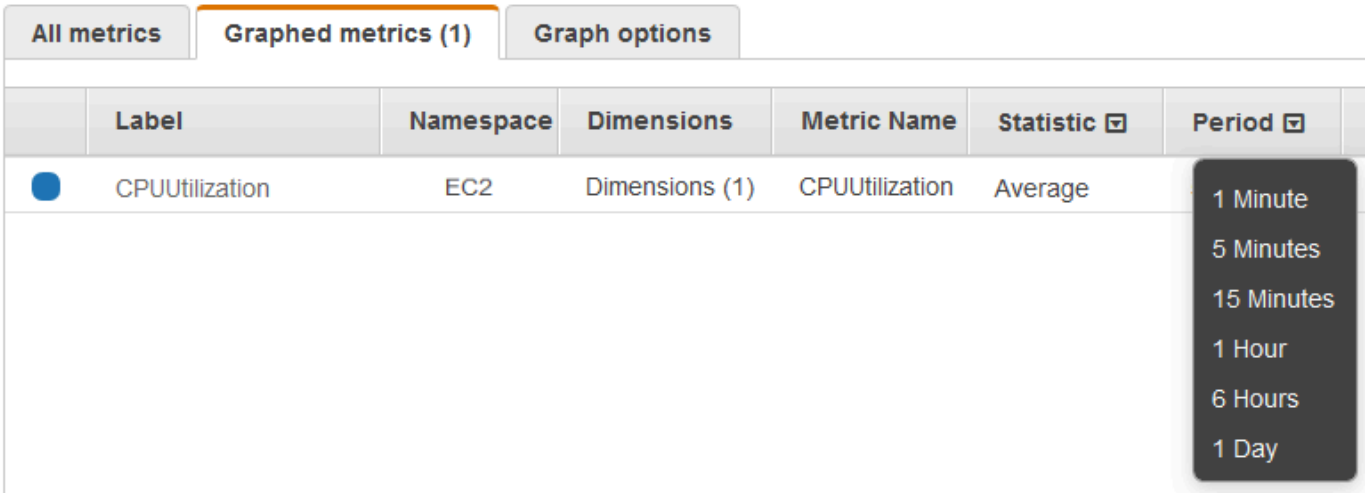
- Anda harus memiliki ID instans. Anda bisa mendapatkan ID instans menggunakan Konsol Manajemen AWS atau perintah describe-instances.
- Pemantauan dasar aktif secara default, tetapi Anda dapat mengaktifkan pemantauan terperinci. Untuk informasi selengkapnya, lihat Mengelola pemantauan terperinci untuk instans EC2 Anda.

Untuk menampilkan pemanfaatan CPU pada instans tertentu (konsol)

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Metrik.
3. Pilih namespace metrik EC2.
4. Pilih dimensi Metrik Per-Instans.
5. Pada bidang pencarian, masukkan **`CPUUtilization`** dan tekan Enter. Pilih baris untuk instans tertentu, yang menampilkan grafik untuk metrik CPUUtilization untuk instans tersebut. Untuk memberikan nama pada grafik, pilih ikon pensil. Untuk mengubah rentang waktu, pilih salah satu nilai yang telah ditentukan sebelumnya atau pilih sesuaikan.



6. Untuk mengubah statistik atau periode metrik, pilih tab Metrik grafik. Pilih judul kolom atau nilai individu, lalu pilih nilai yang berbeda.



Untuk mendapatkan pemanfaatan CPU pada instans tertentu (AWS CLI)

Gunakan get-metric-statisticsperintah berikut untuk mendapatkan CPUUtilizationmetrik untuk contoh yang ditentukan, menggunakan periode dan interval waktu yang ditentukan:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

Berikut contoh outputnya. Setiap nilai merepresentasikan persentase pemanfaatan CPU maksimum untuk satu instans EC2.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```

Mengagregasi statistik di seluruh instans

Statistik agregat tersedia untuk instans yang mengaktifkan pemantauan terperinci. Instans yang menggunakan pemantauan dasar tidak termasuk dalam agregat. Sebelum bisa mendapatkan

statistik agregat di seluruh instans, Anda harus mengaktifkan pemantauan terperinci (dengan biaya tambahan), yang menyediakan data dalam periode 1 menit.

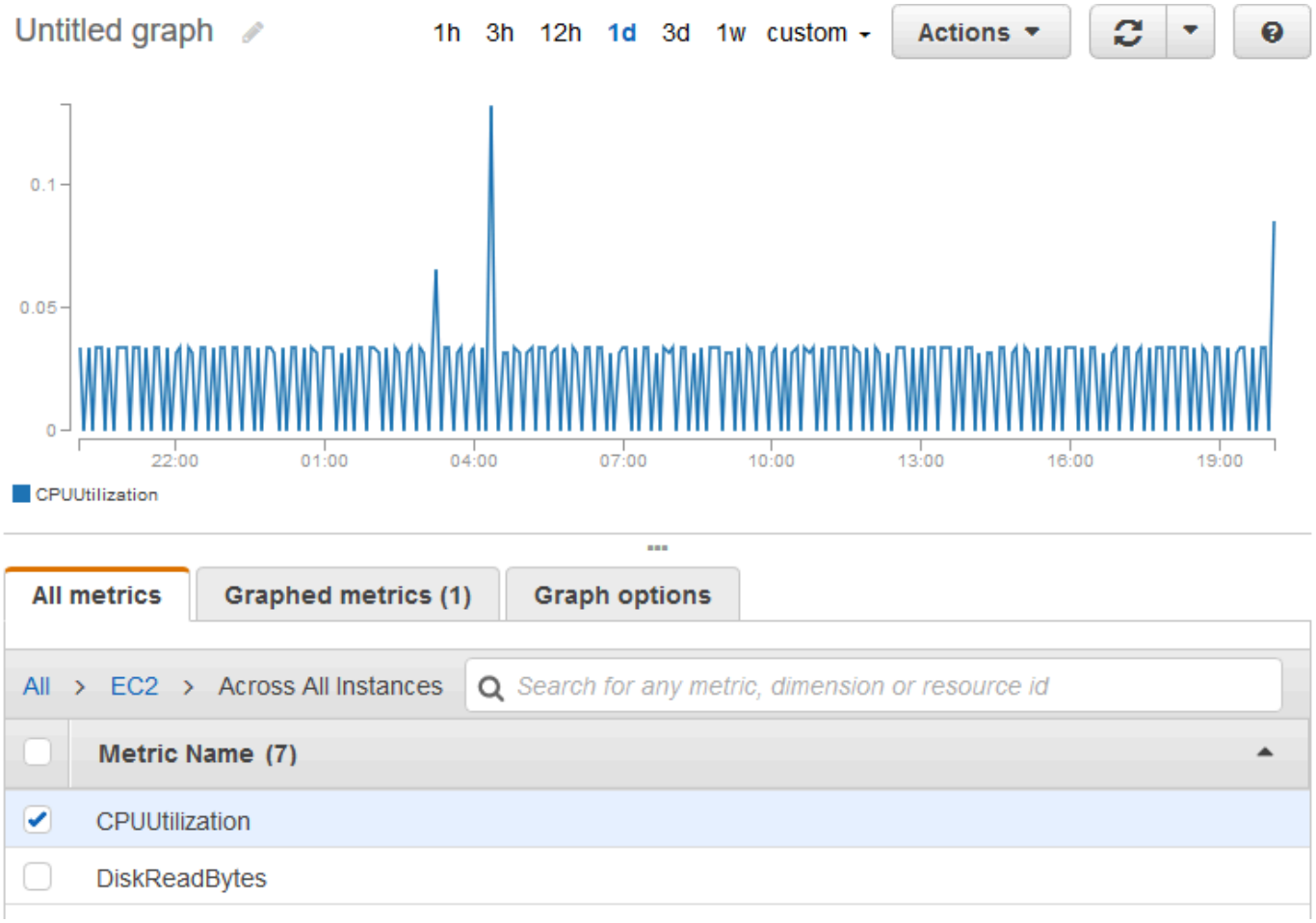
Perhatikan bahwa Amazon CloudWatch tidak dapat menggabungkan data di seluruh AWS Wilayah. Metrik benar-benar terpisah antar-Wilayah.

Contoh ini menunjukkan cara menggunakan pemantauan terperinci untuk mendapatkan penggunaan CPU rata-rata untuk instans EC2 Anda. Karena tidak ada dimensi yang ditentukan, CloudWatch mengembalikan statistik untuk semua dimensi di `AWS/EC2` namespace.

> **Important**
>
> Teknik untuk mengambil semua dimensi di seluruh AWS namespace ini tidak berfungsi untuk ruang nama khusus yang Anda terbitkan ke Amazon. CloudWatch Dengan namespace khusus, Anda harus menentukan rangkaian dimensi lengkap yang terkait dengan titik data mana pun untuk mengambil statistik yang mencakup titik data tersebut.

Untuk menampilkan rata-rata pemanfaatan CPU di seluruh instans Anda (konsol)

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Metrik.
3. Pilih namespace EC2, lalu pilih Di Semua Instans.
4. Pilih baris yang berisi CPUUtilization, yang menampilkan grafik metrik untuk semua instans EC2 Anda. Untuk memberikan nama pada grafik, pilih ikon pensil. Untuk mengubah rentang waktu, pilih salah satu nilai yang telah ditentukan sebelumnya atau pilih sesuaikan.



5. Untuk mengubah statistik atau periode metrik, pilih tab Metrik grafik. Pilih judul kolom atau nilai individu, lalu pilih nilai yang berbeda.

Untuk mendapatkan rata-rata pemanfaatan CPU di seluruh instans Anda (AWS CLI)

Gunakan get-metric-statisticsperintah sebagai berikut untuk mendapatkan rata-rata CPUUtilizationmetrik di seluruh instance Anda.

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

Berikut ini output contohnya:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```


Mengagregasi statistik menurut grup Auto Scaling

Anda dapat mengagregasi statistik untuk instans EC2 dalam grup Auto Scaling. Perhatikan bahwa Amazon CloudWatch tidak dapat menggabungkan data di seluruh AWS Wilayah. Metrik benar-benar terpisah antar-Wilayah.

Contoh ini menunjukkan cara mengambil total bita yang ditulis ke disk untuk satu grup Auto Scaling. Total tersebut dihitung selama periode 1 menit untuk interval 24 jam di seluruh instans EC2 dalam grup Auto Scaling tertentu.

DiskWriteBytes Untuk menampilkan instance dalam grup Auto Scaling (konsol)

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik.
3. Pilih namespace EC2 dan kemudian pilih Berdasarkan grup Auto Scaling.
4. Pilih baris untuk metrik DiskWriteBytes dan grup Auto Scaling tertentu, yang menampilkan grafik untuk metrik pada instans dalam grup Auto Scaling. Untuk memberikan nama pada grafik,

pilih ikon pensil. Untuk mengubah rentang waktu, pilih salah satu nilai yang telah ditentukan sebelumnya atau pilih sesuaikan.

5. Untuk mengubah statistik atau periode metrik, pilih tab Metrik grafik. Pilih judul kolom atau nilai individu, lalu pilih nilai yang berbeda.

DiskWriteBytes Untuk menampilkan instance dalam grup Auto Scaling ()AWS CLI

Gunakan perintah get-metric-statistics sebagai berikut.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

Berikut ini adalah output contoh:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "DiskWriteBytes"
}
```

Mengagregasi statistik menurut AMI

Anda dapat menggabungkan statistik berdasarkan AMI untuk instans Anda yang telah mengaktifkan pemantauan terperinci. Instans yang menggunakan pemantauan dasar tidak termasuk dalam agregat. Sebelum bisa mendapatkan statistik agregat di seluruh instans, Anda harus mengaktifkan pemantauan terperinci (dengan biaya tambahan), yang menyediakan data dalam periode 1 menit.

Perhatikan bahwa Amazon CloudWatch tidak dapat menggabungkan data di seluruh AWS Wilayah. Metrik benar-benar terpisah antar-Wilayah.

Contoh ini menunjukkan kepada Anda cara menentukan rata-rata pemanfaatan CPU untuk semua instans yang menggunakan Amazon Machine Image (AMI) tertentu. Rata-rata adalah interval waktu lebih dari 60 detik untuk periode satu hari.

Untuk menampilkan rata-rata pemanfaatan CPU berdasarkan AMI (konsol)

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik.
3. Pilih namespace EC2 dan kemudian pilih Berdasarkan Id Image (AMI).
4. Pilih baris untuk metrik CPUUtilization dan AMI tertentu, yang menampilkan grafik untuk metrik untuk AMI yang ditentukan. Untuk memberikan nama pada grafik, pilih ikon pensil. Untuk mengubah rentang waktu, pilih salah satu nilai yang telah ditentukan sebelumnya atau pilih sesuaikan.
5. Untuk mengubah statistik atau periode metrik, pilih tab Metrik grafik. Pilih judul kolom atau nilai individu, lalu pilih nilai yang berbeda.

Untuk mendapatkan rata-rata pemanfaatan CPU pada ID citra (AWS CLI)

Gunakan perintah get-metric-statistics sebagai berikut.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

Berikut ini adalah output contoh. Setiap nilai merepresentasikan persentase rata-rata pemanfaatan CPU untuk instans EC2 yang menjalankan AMI yang ditentukan.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
```

```
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```

Lihat grafik pemantauan untuk instans Anda

Setelah meluncurkan sebuah instans, Anda dapat membuka konsol Amazon EC2 dan melihat grafik pemantauan untuk instans tersebut pada tab Pemantauan. Setiap grafik didasarkan pada salah satu metrik Amazon EC2 yang tersedia.

Berikut adalah grafik yang tersedia:

- Rata-Rata Pemanfaatan CPU (Persen)
- Rata-Rata Pembacaan Disk (Bita)
- Rata-Rata Penulisan Disk (Bita)
- Jaringan Masuk Maksimum (Bita)
- Jaringan Keluar Maksimum (Bita)
- Ringkasan Operasi Baca Disk (Jumlah)
- Ringkasan Operasi Tulis Disk (Jumlah)
- Ringkasan Status (Apa saja)
- Ringkasan Status Instans (Jumlah)
- Ringkasan Status Sistem (Jumlah)

Untuk informasi selengkapnya tentang metrik dan data yang diberikan ke grafik, lihat CloudWatch metrik yang tersedia untuk instans Anda.

Metrik grafik menggunakan konsol CloudWatch

Anda juga dapat menggunakan CloudWatch konsol untuk membuat grafik data metrik yang dihasilkan oleh Amazon EC2 dan layanan lainnya AWS . Untuk informasi selengkapnya, lihat Metrik grafik di CloudWatch Panduan Pengguna Amazon.

Buat CloudWatch alarm untuk sebuah contoh

Anda dapat membuat CloudWatch alarm yang memantau CloudWatch metrik untuk salah satu instans Anda. CloudWatchakan secara otomatis mengirimi Anda pemberitahuan ketika metrik mencapai ambang batas yang Anda tentukan. Anda dapat membuat CloudWatch alarm menggunakan konsol Amazon EC2, atau menggunakan opsi yang lebih canggih yang disediakan oleh konsol. CloudWatch

Untuk membuat alarm menggunakan CloudWatch konsol

Sebagai contoh, lihat Membuat CloudWatch Alarm Amazon di Panduan CloudWatch Pengguna Amazon.

Untuk membuat alarm menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance dan pilih Actions, Monitor dan troubleshoot, Manage CloudWatch alarm.
4. Pada halaman Kelola detail CloudWatch alarm, di bawah Tambah atau edit alarm, pilih Buat alarm.
5. Untuk Notifikasi alarm, pilih apakah akan mengonfigurasi notifikasi Amazon Simple Notification Service (Amazon SNS). Masukkan topik Amazon SNS yang ada atau masukkan nama untuk membuat topik baru.
6. Untuk Tindakan alarm, pilih apakah akan menentukan tindakan yang akan dilakukan saat alarm dipicu. Pilih tindakan dari dalam daftar.
7. Untuk Ambang batas alarm, pilih metrik dan kriteria untuk alarm. Misalnya, untuk membuat alarm yang dipicu ketika pemanfaatan CPU mencapai 80% selama periode 5 menit, lakukan hal berikut:

    a. Pertahankan pengaturan default untuk Kelompokkan sampel berdasarkan (Rata-rata) dan Tipe data untuk sampel (Pemanfaatan CPU).

    b. Pilih >= untuk Waktu alarm dan masukkan **`0.80`** untuk Persen.

    c. Masukkan **`1`** untuk periode berturut-turut dan pilih 5 menit untuk Periode.

8. (Opsional) Untuk Data metrik sampel, pilih Tambahkan ke dasbor.
9. Pilih Buat.

Anda dapat mengedit pengaturan CloudWatch alarm dari konsol Amazon EC2 atau konsol. CloudWatch Jika Anda ingin menghapus alarm Anda, Anda dapat melakukannya dari CloudWatch konsol. Untuk informasi selengkapnya, lihat Mengedit atau menghapus CloudWatch alarm di Panduan CloudWatch Pengguna Amazon.

Buat alarm yang menghentikan, mengakhiri, melakukan boot ulang, atau memulihkan instans

Dengan menggunakan tindakan CloudWatch alarm Amazon, Anda dapat membuat alarm yang secara otomatis menghentikan, menghentikan, me-reboot, atau memulihkan instans Anda. Anda dapat menggunakan tindakan penghentian atau pengakhiran untuk membantu menghemat uang saat suatu instans tidak lagi diperlukan. Anda dapat menggunakan tindakan boot ulang dan pemulihan untuk secara otomatis melakukan boot ulang instans tersebut atau memulihkannya ke perangkat keras baru jika terjadi gangguan pada sistem.

> **Note**
>
> Untuk informasi penagihan dan harga CloudWatch alarm Amazon, lihat CloudWatch penagihan dan biaya di Panduan Pengguna Amazon CloudWatch .

Peran `AWSServiceRoleForCloudWatchEvents` terkait layanan memungkinkan AWS untuk melakukan tindakan alarm atas nama Anda. Pertama kali Anda membuat alarm di Konsol Manajemen AWS, API AWS CLI, atau IAM, CloudWatch membuat peran terkait layanan untuk Anda.

Ada sejumlah skenario yang mungkin akan membuat Anda ingin menghentikan atau mengakhiri instans secara otomatis. Misalnya, Anda mungkin memiliki instans khusus untuk membuat batch tugas pemrosesan penggajian atau tugas komputasi ilmiah yang berjalan selama jangka waktu tertentu dan telah menyelesaikan pekerjaannya. Alih-alih membiarkan instans tersebut menganggur (dan menambah biaya), Anda dapat menghentikan atau mengakhirinya, sehingga membantu Anda menghemat uang. Perbedaan utama antara menggunakan tindakan alarm penghentian dan pengakhiran adalah bahwa Anda dapat dengan mudah memulai instans yang dihentikan jika intans tersebut perlu dijalankan kembali nanti. Anda juga dapat menyimpan ID instans dan volume root yang sama. Namun, Anda tidak dapat memulai instans yang diakhiri. Sebaliknya, Anda harus meluncurkan

instans baru. Saat instans dihentikan atau diakhiri, data pada volume penyimpanan instans akan hilang.

Anda dapat menambahkan tindakan hentikan, akhiri, boot ulang, atau pulihkan ke alarm apa pun yang diatur pada metrik Amazon EC2 per-instans, termasuk metrik pemantauan dasar dan terperinci yang disediakan oleh Amazon CloudWatch (di ruang nama `AWS/EC2`), seperti serta metrik khusus apa pun yang menyertakan dimensi `InstanceId`, selama nilainya mengacu pada instans Amazon EC2 yang berjalan dan valid.

> **Important**
>
> Alarm pemeriksaan status dapat memasuki `INSUFFICIENT_DATA` status sementara jika ada titik data metrik yang hilang. Meskipun jarang, ini bisa terjadi ketika ada gangguan dalam sistem pelaporan metrik, bahkan ketika sebuah instance sehat. Sebaiknya Anda memperlakukan `INSUFFICIENT_DATA` status sebagai data yang hilang, bukan pelanggaran alarm, terutama saat mengonfigurasi alarm untuk menghentikan, menghentikan, me-reboot, atau memulihkan instance.

Dukungan konsol

Anda dapat membuat alarm menggunakan konsol Amazon EC2 atau CloudWatch konsol. Prosedur dalam dokumentasi ini menggunakan konsol Amazon EC2. Untuk prosedur yang menggunakan CloudWatch konsol, lihat Membuat alarm yang menghentikan, menghentikan, reboot, atau memulihkan instance di CloudWatch Panduan Pengguna Amazon.

Izin

Anda harus memiliki `iam:CreateServiceLinkedRole` untuk membuat atau memodifikasi alarm yang melakukan tindakan alarm EC2. Peran layanan adalah peran IAM yang diasumsikan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

Daftar Isi

- Tambahkan tindakan berhenti ke CloudWatch alarm Amazon
- Tambahkan tindakan penghentian ke alarm Amazon CloudWatch
- Tambahkan tindakan reboot ke CloudWatch alarm Amazon

- Tambahkan tindakan pemulihan ke CloudWatch alarm Amazon
- Skenario tindakan CloudWatch alarm Amazon

Tambahkan tindakan berhenti ke CloudWatch alarm Amazon

Anda dapat membuat alarm yang menghentikan instans Amazon EC2 ketika ambang batas tertentu telah terpenuhi. Misalnya, Anda dapat mengoperasikan pengembangan atau instans pengujian dan terkadang lupa untuk mematikannya. Anda dapat membuat alarm yang dipicu ketika persentase rata-rata pemanfaatan CPU kurang dari 10 persen selama 24 jam, yang menandakan bahwa alarm dalam keadaan menganggur dan tidak diperlukan lagi. Anda dapat menyesuaikan ambang batas, durasi, dan periode sesuai kebutuhan. Anda juga dapat menambahkan notifikasi Amazon Simple Notification Service (Amazon SNS) untuk menerima email saat alarm dipicu.

Instans yang menggunakan volume Amazon EBS sebagai volume root dapat dihentikan atau dihentikan, sedangkan instance yang menggunakan penyimpanan instance sebagai volume root hanya dapat dihentikan. Data pada volume penyimpanan instans hilang saat instans diakhiri atau dihentikan.

Untuk membuat alarm agar dapat menghentikan instans yang menganggur (konsol Amazon EC2)

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance dan pilih Actions, Monitor dan troubleshoot, Manage CloudWatch alarm.

   Atau, Anda dapat memilih tanda plus (

) pada kolom Status alarm.
4. Pada halaman Kelola CloudWatch alarm, lakukan hal berikut:

   a. Pilih Buat alarm.

   b. Untuk menerima email saat alarm dipicu, untuk Notifikasi alarm, pilih topik Amazon SNS yang ada. Anda harus terlebih dahulu membuat topik Amazon SNS menggunakan konsol Amazon SNS. Untuk informasi selengkapnya, lihat Menggunakan Amazon SNS untuk pesan application-to-person (A2P) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

   c. Aktifkan Tindakan alarm, lalu pilih Hentikan.

d. Untuk Kelompokkan sampel berdasarkan serta Tipe data untuk sampel, pilih statistik dan metrik. Dalam contoh ini, pilih Rata-rata dan Pemanfaatan CPU.

e. Untuk Waktu Alarm dan Persen, tentukan ambang batas metrik. Dalam contoh ini, pilih <= dan 10 persen.

f. Untuk Periode berturut-turut dan Periode, tentukan periode evaluasi alarm. Dalam contoh ini, pilih 1 periode berturut-turut 5 Menit.

g. Amazon CloudWatch secara otomatis membuat nama alarm untuk Anda. Untuk mengganti nama, pada Nama alarm, masukkan nama baru. Nama alarm hanya boleh berisi karakter ASCII.

> **Note**
>
> Anda dapat menyesuaikan konfigurasi alarm berdasarkan kebutuhan sebelum membuat alarm, atau Anda dapat mengeditnya nanti. Penyesuaian ini termasuk pengaturan metrik, ambang batas, durasi, tindakan, dan notifikasi. Namun, nama alarm yang telah dibuat sudah tidak dapat diedit.

h. Pilih Buat.

Tambahkan tindakan penghentian ke alarm Amazon CloudWatch

Anda dapat membuat alarm yang mengakhiri instans EC2 secara otomatis ketika ambang batas tertentu telah terpenuhi (selama perlindungan pengakhiran tidak diaktifkan untuk instans tersebut). Misalnya, Anda mungkin ingin mengakhiri instans ketika telah menyelesaikan pekerjaannya dan sudah tidak diperlukan lagi. Jika Anda mungkin ingin menggunakan instans tersebut nanti, Anda sebaiknya menghentikan instans tersebut dan tidak menghentikannya. Data pada volume penyimpanan instans hilang saat instans diakhiri. Untuk informasi tentang pengaktifan dan penonaktifan perlindungan pengakhiran pada instans, lihat Ubah perlindungan penghentian instance.

Untuk membuat alarm agar dapat mengakhiri instans yang menganggur (konsol Amazon EC2)

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance dan pilih Actions, Monitor dan troubleshoot, Manage CloudWatch alarm.

Atau, Anda dapat memilih tanda plus (

) pada kolom Status alarm.

4. Pada halaman Kelola CloudWatch alarm, lakukan hal berikut:

   a. Pilih Buat alarm.

   b. Untuk menerima email saat alarm dipicu, untuk Notifikasi alarm, pilih topik Amazon SNS yang ada. Anda harus terlebih dahulu membuat topik Amazon SNS menggunakan konsol Amazon SNS. Untuk informasi selengkapnya, lihat Menggunakan Amazon SNS untuk pesan application-to-person (A2P) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

   c. Aktifkan Tindakan alarm, lalu pilih Akhiri.

   d. Untuk Kelompokkan sampel berdasarkan serta Tipe data untuk sampel, pilih statistik dan metrik. Dalam contoh ini, pilih Rata-rata dan Pemanfaatan CPU.

   e. Untuk Waktu Alarm dan Persen, tentukan ambang batas metrik. Dalam contoh ini, pilih => dan 10 persen.

   f. Untuk Periode berturut-turut dan Periode, tentukan periode evaluasi alarm. Dalam contoh ini, pilih 24 periode berturut-turut dari 1 Jam.

   g. Amazon CloudWatch secara otomatis membuat nama alarm untuk Anda. Untuk mengganti nama, pada Nama alarm, masukkan nama baru. Nama alarm hanya boleh berisi karakter ASCII.

      > **Note**
      >
      > Anda dapat menyesuaikan konfigurasi alarm berdasarkan kebutuhan sebelum membuat alarm, atau Anda dapat mengeditnya nanti. Penyesuaian ini termasuk pengaturan metrik, ambang batas, durasi, tindakan, dan notifikasi. Namun, nama alarm yang telah dibuat sudah tidak dapat diedit.

   h. Pilih Buat.

Tambahkan tindakan reboot ke CloudWatch alarm Amazon

Anda dapat membuat CloudWatch alarm Amazon yang memantau instans Amazon EC2 dan secara otomatis me-reboot instans. Tindakan alarm boot ulang direkomendasikan untuk kegagalan

Pemeriksaan Kondisi instans (sebagai lawan dari tindakan alarm pemulihan, yang sesuai untuk kegagalan Pemeriksaan Kondisi Sistem). Sebuah instans yang melakukan boot ulang setara dengan penyalaan ulang sistem operasi. Dalam kebanyakan kasus, hanya diperlukan beberapa menit untuk menyalakan ulang instans Anda. Saat Anda melakukan boot ulang, instans tetap berada di host fisik yang sama, sehingga instans Anda tetap menggunakan nama DNS publik, alamat IP privat, dan setiap data pada volume penyimpanan instansnya.

Boot ulang instans tidak memulai periode penagihan instans baru (dengan biaya minimum satu menit), tidak seperti penghentian dan pemulaian ulang instans Anda. Data pada volume penyimpanan instans dipertahankan saat instans di-boot ulang. Volume penyimpanan instans harus dipasang kembali ke sistem file setelah boot ulang. Untuk informasi selengkapnya, lihat Nyalakan ulang EC2 instans Amazon Anda.

> **Important**
>
> Untuk menghindari kondisi pacu antara tindakan boot ulang dan pemulihan, jangan mengatur jumlah periode evaluasi yang sama untuk alarm boot ulang dan alarm pemulihan. Kami menyarankan Anda untuk mengatur alarm boot ulang ke tiga periode evaluasi, masing-masing selama satu menit. Untuk informasi selengkapnya, lihat Mengevaluasi alarm di Panduan CloudWatch Pengguna Amazon.

Untuk membuat alarm agar dapat melakukan boot ulang instans (konsol Amazon EC2)

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance dan pilih Actions, Monitor dan troubleshoot, Manage CloudWatch alarm.

   Atau, Anda dapat memilih tanda plus (

) pada kolom Status alarm.
4. Pada halaman Kelola CloudWatch alarm, lakukan hal berikut:

   a. Pilih Buat alarm.

   b. Untuk menerima email saat alarm dipicu, untuk Notifikasi alarm, pilih topik Amazon SNS yang ada. Anda harus terlebih dahulu membuat topik Amazon SNS menggunakan konsol Amazon SNS. Untuk informasi selengkapnya, lihat Menggunakan Amazon SNS untuk pesan

application-to-person (A2P) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

c. Aktifkan Tindakan alarm, lalu pilih Boot ulang.

d. Untuk Kelompokkan sampel berdasarkan serta Tipe data untuk sampel, pilih statistik dan metrik. Pada contoh ini, pilih Rata-rata dan Pemeriksaan status gagal: instans.

e. Untuk Periode berturut-turut dan Periode, tentukan periode evaluasi alarm. Dalam contoh ini, masukkan 3 periode berturut-turut 1 Menit. Jika 1 Menit dinonaktifkan, Anda harus mengaktifkan pemantauan terperinci, atau Anda dapat memilih 5 Menit sebagai gantinya.

f. Amazon CloudWatch secara otomatis membuat nama alarm untuk Anda. Untuk mengganti nama, pada Nama alarm, masukkan nama baru. Nama alarm hanya boleh berisi karakter ASCII.

g. Pilih Buat.

Tambahkan tindakan pemulihan ke CloudWatch alarm Amazon

Anda dapat membuat CloudWatch alarm Amazon yang memantau instans Amazon EC2. Jika instance menjadi terganggu karena kegagalan perangkat keras yang mendasarinya atau masalah yang memerlukan AWS keterlibatan untuk memperbaiki, Anda dapat memulihkan instance secara otomatis. Instans yang diakhiri tidak dapat dipulihkan. Instans yang dipulihkan identik dengan instans awal, termasuk ID instans , alamat IP privat, alamat IP Elastis, dan semua metadata instans.

CloudWatch mencegah Anda menambahkan tindakan pemulihan ke alarm yang ada di instance yang tidak mendukung tindakan pemulihan.

Ketika alarm `StatusCheckFailed_System` dipicu dan tindakan pemulihan dimulai, topik Amazon SNS yang Anda pilih akan mengirimkan notifikasi ketika Anda membuat alarm dan mengaitkan tindakan pemulihan. Selama pemulihan, instans dimigrasikan selama boot ulang instans, dan semua data yang berada dalam memori akan hilang. Saat proses selesai, informasi akan diterbitkan ke topik SNS yang telah Anda konfigurasikan untuk alarm. Setiap orang yang berlangganan topik SNS ini akan menerima notifikasi email yang meliputi status upaya pemulihan dan petunjuk lebih lanjut. Anda melihat boot ulang instans pada instans yang dipulihkan.

> **Note**
>
> Tindakan pemulihan hanya dapat digunakan dengan `StatusCheckFailed_System`, tidak dengan `StatusCheckFailed_Instance`.

Masalah berikut dapat menyebabkan kegagalan pemeriksaan status sistem:

- Hilangnya konektivitas jaringan
- Kehilangan daya sistem
- Masalah perangkat lunak pada host fisik
- Masalah perangkat keras pada host fisik yang memengaruhi jangkauan jaringan

Tindakan pemulihan hanya didukung pada instans yang memenuhi karakteristik tertentu. Untuk informasi selengkapnya, lihat Pemulihan instans otomatis.

Jika instans Anda memiliki alamat IP publik, instans tersebut akan mempertahankan alamat IP publik setelah pemulihan.

> **Important**
>
> Untuk menghindari kondisi pacu antara tindakan boot ulang dan pemulihan, jangan mengatur jumlah periode evaluasi yang sama untuk alarm boot ulang dan alarm pemulihan. Kami menyarankan Anda untuk mengatur alarm pemulihan ke dua periode evaluasi, masing-masing selama satu menit. Untuk informasi selengkapnya, lihat Mengevaluasi alarm di Panduan CloudWatch Pengguna Amazon.

Untuk membuat alarm agar dapat memulihkan instans (konsol Amazon EC2)

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance dan pilih Actions, Monitor dan troubleshoot, Manage CloudWatch alarm.

   Atau, Anda dapat memilih tanda plus (

) pada kolom Status alarm.
4. Pada halaman Kelola CloudWatch alarm, lakukan hal berikut:

   a. Pilih Buat alarm.

   b. Untuk menerima email saat alarm dipicu, untuk Notifikasi alarm, pilih topik Amazon SNS yang ada. Anda harus terlebih dahulu membuat topik Amazon SNS menggunakan konsol

Amazon SNS. Untuk informasi selengkapnya, lihat Menggunakan Amazon SNS untuk pesan application-to-person (A2P) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

> **Note**
>
> Pengguna harus berlangganan topik SNS yang ditentukan untuk menerima notifikasi email saat alarm dipicu. Pengguna root akun AWS Selalu menerima pemberitahuan email ketika tindakan pemulihan instans otomatis terjadi, bahkan jika topik SNS tidak ditentukan atau pengguna root tidak berlangganan ke topik SNS yang ditentukan.

c. Aktifkan Tindakan alarm, lalu pilih Pulihkan.

d. Untuk Kelompokkan sampel berdasarkan serta Tipe data untuk sampel, pilih statistik dan metrik. Pada contoh ini, pilih Rata-rata dan Pemeriksaan status gagal: sistem.

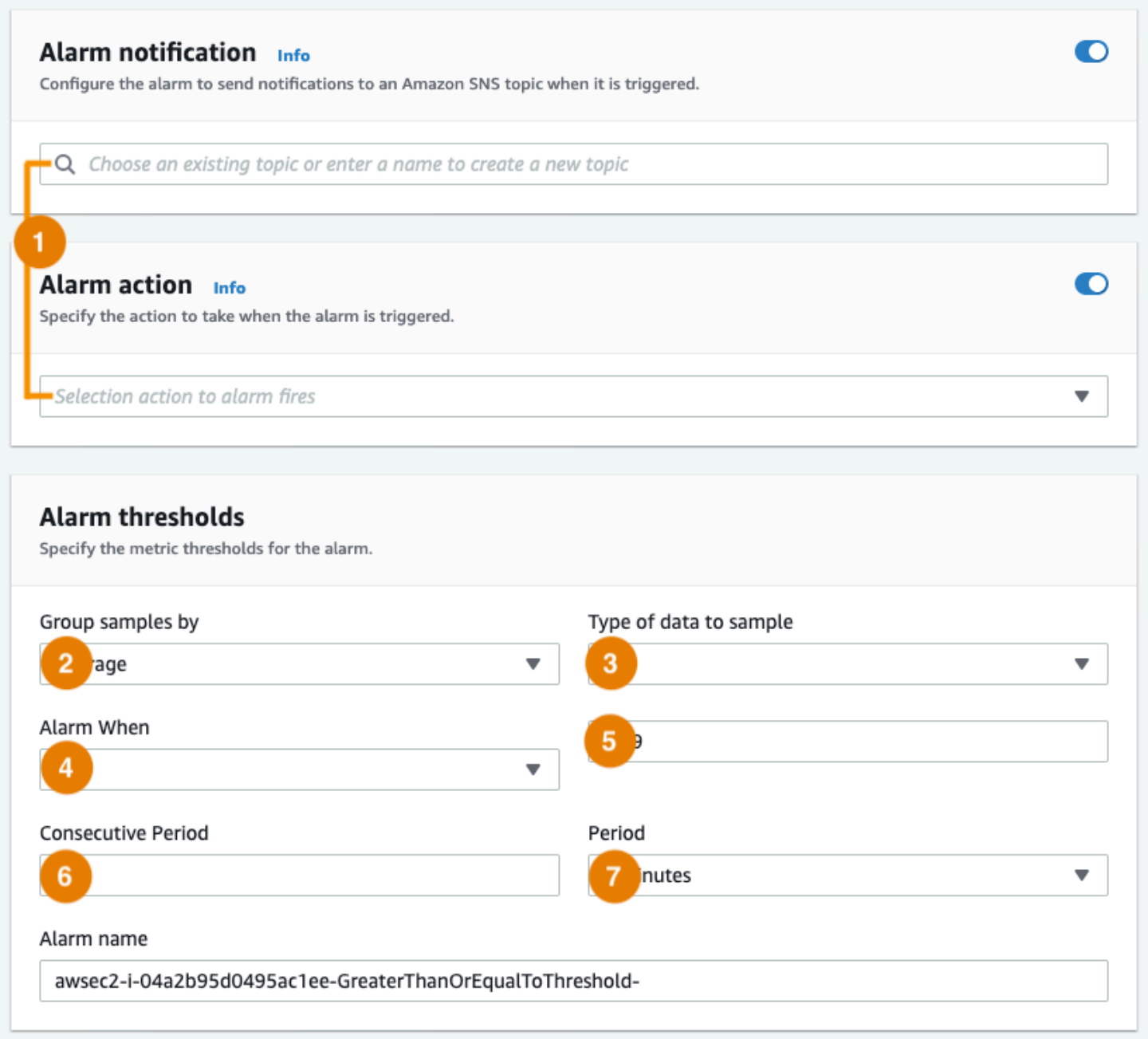
e. Untuk Periode berturut-turut dan Periode, tentukan periode evaluasi alarm. Dalam contoh ini, masukkan 2 periode berturut-turut 1 Menit. Jika 1 Menit dinonaktifkan, Anda harus mengaktifkan pemantauan terperinci, atau Anda dapat memilih 5 Menit sebagai gantinya.

f. Amazon CloudWatch secara otomatis membuat nama alarm untuk Anda. Untuk mengganti nama, pada Nama alarm, masukkan nama baru. Nama alarm hanya boleh berisi karakter ASCII.

g. Pilih Buat.

Skenario tindakan CloudWatch alarm Amazon

Anda dapat menggunakan konsol Amazon EC2 untuk membuat tindakan alarm yang menghentikan atau mengakhiri instans Amazon EC2 ketika kondisi tertentu terpenuhi. Pada tangkapan layar halaman konsol tempat Anda mengatur tindakan alarm berikut, kami telah menomori pengaturannya. Kami juga telah menomori pengaturan dalam skenario yang mengikuti untuk membantu Anda membuat tindakan yang tepat.



Skenario 1: Menghentikan instans pengembangan dan pengujian yang menganggur

Buat alarm yang menghentikan instans yang digunakan untuk pengembangan atau pengujian perangkat lunak saat sedang menganggur selama setidaknya satu jam.

Pengaturan	Nilai
1	Berhenti

Pengaturan	Nilai
2	Maksimum
3	Pemanfaatan CPU
4	<=
5	10%
6	1
7	1 Jam

Skenario 2: Menghentikan instans yang menganggur

Buat alarm yang menghentikan sebuah instans dan mengirimkan email saat instans tersebut sudah menganggur selama 24 jam.

Pengaturan	Nilai
1	Hentikan dan kirim email
2	Rata-rata
3	Pemanfaatan CPU
4	<=
5	5%
6	24
7	1 Jam

Skenario 3: Mengirimkan email mengenai server web dengan lalu lintas yang luar biasa tinggi

Buat alarm yang mengirimkan email ketika sebuah instans melebihi 10 GB lalu lintas jaringan keluar per hari.

Pengaturan	Nilai
1	Email
2	Jumlah
3	Jaringan Keluar
4	>
5	10 GB
6	24
7	1 Jam

Skenario 4: Menghentikan server web dengan lalu lintas yang luar biasa tinggi

Buat alarm yang menghentikan instans dan kirim pesan teks (SMS) jika lalu lintas keluar melebihi 1 GB per jam.

Pengaturan	Nilai
1	Hentikan dan kirim SMS
2	Jumlah
3	Jaringan Keluar
4	>
5	1 GB
6	1
7	1 Jam

Skenario 5: Menghentikan instans yang terganggu

Buat alarm yang menghentikan instans yang gagal dalam tiga pemeriksaan status berturut-turut (dilakukan dengan interval 5 menit).

Pengaturan	Nilai
1	Berhenti
2	Rata-rata
3	Pemeriksaan Status Gagal: (Sistem)
4	-
5	-
6	1
7	15 Menit

Skenario 6: Mengakhiri instans ketika pembuatan batch pekerjaan pemrosesan selesai

Buat alarm yang mengakhiri instans yang menjalankan tugas batch jika tidak lagi mengirimkan data hasil.

Pengaturan	Nilai
1	Akhiri
2	Maksimum
3	Jaringan Keluar
4	<=
5	100.000 bita
6	1

Pengaturan	Nilai
7	5 Menit

Otomatiskan Amazon menggunakan EC2 EventBridge

Anda dapat menggunakan Amazon EventBridge untuk mengotomatiskan Layanan AWS dan merespons peristiwa sistem secara otomatis, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu dekat. Anda dapat membuat aturan untuk menunjukkan peristiwa yang sesuai kepentingan Anda, dan tindakan yang akan diambil ketika peristiwa sesuai dengan aturan. Tindakan yang dapat dipicu secara otomatis meliputi hal-hal berikut:

- Memanggil fungsi AWS Lambda
- Memanggil Amazon EC2 Run Command
- Menyampaikan peristiwa ke Amazon Kinesis Data Streams
- Aktifkan mesin AWS Step Functions negara
- Mengirim notifikasi topik Amazon SNS
- Mengirim notifikasi antrean Amazon SQS

Berikut ini adalah contoh bagaimana Anda dapat menggunakan EventBridge dengan Amazon EC2:

- Aktifkan fungsi Lambda setiap kali instans memasuki status berjalan.
- Notifikasi topik Amazon SNS saat volume Amazon EBS dibuat atau dimodifikasi.
- Kirim perintah ke satu atau beberapa EC2 instans Amazon menggunakan Amazon EC2 Run Command setiap kali peristiwa tertentu di AWS layanan lain terjadi.

Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Jenis EC2 acara Amazon

Amazon EC2 mendukung jenis acara berikut:

- EC2 Perubahan Negara AMI
- EC2 Pemberitahuan Perubahan Status Peluncuran Cepat

- EC2 Kesalahan Armada
- EC2 Informasi Armada
- EC2 Perubahan Instans Armada
- EC2 Perubahan Permintaan Instans Fleet Spot
- EC2 Perubahan Negara Armada
- EC2 Rekomendasi Penyeimbangan Ulang Instance
- EC2 Pemberitahuan Perubahan Status Instance
- EC2 Kesalahan Armada Spot
- EC2 Informasi Armada Spot
- EC2 Perubahan Instans Armada Spot
- EC2 Perubahan Permintaan Instans Spot Armada Spot
- EC2 Perubahan Negara Armada Spot
- EC2 Peringatan Gangguan Instans Spot
- EC2 Pemenuhan Permintaan Instans Spot
- EC2 Pemberitahuan Kurangnya Pemanfaatan ODCR

Untuk informasi tentang jenis acara yang didukung oleh Amazon EBS, lihat Amazon EventBridge untuk Amazon EBS.

Log panggilan EC2 API Amazon menggunakan AWS CloudTrail

Amazon EC2 API terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. CloudTrail menangkap semua panggilan Amazon EC2 API sebagai peristiwa. Panggilan yang ditangkap termasuk panggilan yang dilakukan oleh konsol. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon EC2 API, alamat IP dari mana permintaan itu dibuat, dan kapan permintaan itu dibuat.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut hal ini:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.

- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. AWS Region Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan Konsol Manajemen AWS Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. AWS Region Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Penyimpanan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengubah peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda

kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Acara manajemen EC2 API Amazon di CloudTrail

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. Ini juga dikenal sebagai operasi bidang kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

Semua tindakan Amazon EC2 API dicatat sebagai peristiwa manajemen. Untuk daftar tindakan API yang dicatat CloudTrail, lihat Referensi EC2 API Amazon. Misalnya, panggilan ke RunInstancesDescribeInstances, dan StopInstancestindakan dicatat sebagai peristiwa manajemen.

Contoh acara Amazon EC2 API

Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang operasi API yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Catatan file log berikut menunjukkan bahwa pengguna telah mengakhiri sebuah instans.


```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"Root",
            "principalId":"123456789012",
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
```

```
        "eventTime":"2016-05-20T08:27:45Z",
        "eventSource":"ec2.amazonaws.com",
        "eventName":"TerminateInstances",
        "awsRegion":"us-west-2",
        "sourceIPAddress":"198.51.100.1",
        "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
        "requestParameters":{
           "instancesSet":{
              "items":[{
                 "instanceId":"i-1a2b3c4d"
              }]
           }
        },
        "responseElements":{
           "instancesSet":{
              "items":[{
                 "instanceId":"i-1a2b3c4d",
                 "currentState":{
                    "code":32,
                    "name":"shutting-down"
                 },
                 "previousState":{
                    "code":16,
                    "name":"running"
                 }
              }]
           }
        },
        "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
        "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
     }
   ]
}
```


Untuk informasi tentang konten CloudTrail rekaman, lihat konten CloudTrail rekaman di Panduan AWS CloudTrail Pengguna.

Koneksi audit dibuat menggunakan EC2 Instance Connect

Anda dapat menggunakan AWS CloudTrail untuk mengaudit pengguna yang terhubung ke instans menggunakan EC2 Instance Connect.

Untuk mengaudit aktivitas SSH melalui EC2 Instance Connect menggunakan konsol AWS CloudTrail

1. Buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pastikan Anda berada di Wilayah yang benar.
3. Di panel navigasi, pilih Riwayat Peristiwa.
4. Untuk Filter, pilih Sumber peristiwa, ec2-instance-connect.amazonaws.com.
5. (Opsional) Untuk Rentang waktu, pilih satu rentang waktu.
6. Pilih ikon Segarkan peristiwa.
7. Halaman ini menampilkan peristiwa yang sesuai dengan panggilan API SendSSHPublicKey. Perluas acara menggunakan panah untuk melihat detail tambahan, seperti nama pengguna dan kunci AWS akses yang digunakan untuk membuat koneksi SSH, dan alamat IP sumber.
8. Untuk menampilkan informasi peristiwa yang lengkap dalam format JSON, pilih Lihat peristiwa. Bidang requestParameters berisi ID instans tujuan, nama pengguna OS, dan kunci publik yang digunakan untuk membuat koneksi SSH.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
```

```
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```


Jika Anda telah mengonfigurasi AWS akun Anda untuk mengumpulkan CloudTrail acara dalam bucket S3, Anda dapat mengunduh dan mengaudit informasi secara terprogram. Untuk informasi selengkapnya, lihat Mendapatkan dan melihat file CloudTrail log Anda di Panduan AWS CloudTrail Pengguna.

Pantau aplikasi.NET dan SQL Server menggunakan Application CloudWatch Insights

CloudWatch Application Insights membantu Anda memantau aplikasi.NET dan SQL Server yang menggunakan instans Amazon EC2 bersama dengan sumber daya aplikasi lainnya.AWS Ini mengidentifikasi dan mengatur log metrik utama dan alarm di seluruh sumber daya aplikasi dan tumpukan teknologi Anda (misalnya, database Microsoft SQL Server, web (IIS) dan server aplikasi, OS, penyeimbang beban, dan antrian). Wawasan Aplikasi CloudWatch terus memantau metrik dan log untuk mendeteksi serta menghubungkan anomali dan kesalahan. Ketika kesalahan dan anomali terdeteksi, Application Insights menghasilkan peristiwa yang dapat Anda gunakan untuk mengatur notifikasi atau mengambil tindakan. Untuk membantu memecahkan masalah, Wawasan Aplikasi membuat dasbor otomatis pada masalah yang terdeteksi, yang mencakup anomali metrik dan kesalahan log yang berhubungan, beserta wawasan tambahan untuk menunjukkan kemungkinan akar masalah. Dasbor otomatis tersebut membantu Anda mengambil tindakan perbaikan untuk menjaga aplikasi agar tetap sehat dan mencegah dampak bagi pengguna akhir aplikasi Anda.

Informasi yang diberikan terkait masalah yang terdeteksi:

- Ringkasan singkat masalah
- Waktu dan tanggal mulai masalah
- Tingkat keparahan masalah: High/Medium/Low
- Status masalah yang terdeteksi: Sedang Berlangsung/Terselesaikan

- Wawasan: Secara otomatis menghasilkan wawasan terkait masalah yang terdeteksi dan kemungkinan akar masalah
- Umpan balik tentang wawasan: Umpan balik yang Anda berikan tentang kegunaan wawasan yang dihasilkan oleh Wawasan CloudWatch Aplikasi untuk.NET dan SQL Server
- Observasi terkait: Tampilan terperinci dari anomali metrik dan cuplikan kesalahan dari log yang relevan terkait masalah di berbagai komponen aplikasi

Umpan Balik

Anda dapat memberikan umpan balik mengenai wawasan yang dihasilkan secara otomatis terkait masalah yang terdeteksi dengan menetapkannya sebagai berguna atau tidak berguna. Umpan balik mengenai wawasan tersebut, beserta diagnostik aplikasi Anda (anomali metrik dan pengecualian log), digunakan untuk meningkatkan deteksi masalah serupa pada masa mendatang.

Untuk informasi selengkapnya, lihat dokumentasi Wawasan CloudWatch Aplikasi di Panduan CloudWatch Pengguna Amazon.

Lacak penggunaan Tingkat Gratis Anda untuk Amazon EC2

Saat Anda membuat Akun AWS, Anda dapat memulai dengan Amazon EC2 secara gratis menggunakan Tingkat AWS Gratis. Manfaat Tingkat Gratis Anda berbeda tergantung pada apakah Anda membuat akun sebelum 15 Juli 2025, atau pada atau setelah 15 Juli 2025. Untuk informasi selengkapnya, lihat Menjelajahi AWS layanan dengan Tingkat AWS Gratis di Panduan AWS Billing Pengguna.

Manfaat Tingkat Gratis sebelum dan sesudah 15 Juli 2025

Tabel berikut membandingkan manfaat Tingkat Gratis berdasarkan tanggal Akun AWS pembuatan Anda:

Manfaat Tingkat Gratis	Akun dibuat sebelum 15 Juli 2025	Akun dibuat pada atau setelah 15 Juli 2025
Jenis instans ditandai Tingkat gratis memenuhi syarat	`t2.micro`, `t3.micro`	`t3.micro`, `t3.small`, `t4g.micro` , `t4g.small` , `c7i-flex.large` , `m7i-flex.large`

Manfaat Tingkat Gratis	Akun dibuat sebelum 15 Juli 2025	Akun dibuat pada atau setelah 15 Juli 2025
Jenis volume Amazon EBS ditandai Tingkat gratis memenuhi syarat	`standard`,`st1`,`sc1`,`gp2`, dan `gp3`	`standard`,`st1`,`sc1`,`gp2`, dan `gp3`
AMIs ditandai Tingkat gratis memenuhi syarat	Periksa untuk memenuhi syarat tingkat Gratis yang AMIs ditandai.	Periksa untuk memenuhi syarat tingkat Gratis yang AMIs ditandai.
Batas penggunaan	Dibatasi pada batas penggunaan, setelah itu Anda ditagih pay-as-you-go tarif.	Dapatkan kredit pendaftar an USD $100 dan dapatkan hingga $100 dalam kredit tambahan.
Durasi Tingkat Gratis	Tingkat Gratis Anda berlangsu ng selama 12 bulan sejak tanggal Anda membuat akun. Selama waktu ini, jika Anda melebihi batas penggunaa n Tingkat Gratis, Anda akan ditagih pay-as-you-go tarif.	Tingkat Gratis Anda berlangsu ng selama 6 bulan sejak tanggal Anda membuat akun, atau ketika kredit Anda habis, mana yang terjadi lebih dulu. Anda tidak dapat melebihi batas Tingkat Gratis Anda.

Untuk mencantumkan jenis instans yang memenuhi syarat tingkat gratis

Gunakan describe-instance-typesperintah dengan `free-tier-eligible` filter.

```
aws ec2 describe-instance-types \
    --filters Name=free-tier-eligible,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Untuk daftar AMIs yang memenuhi syarat tingkat gratis

Gunakan perintah deskripsi-gambar dengan filter. `free-tier-eligible`

```
aws ec2 describe-images \
```

```
    --filters Name=free-tier-eligible,Values=true \
    --query "Images[*].[ImageId]" \
    --output text | sort
```

Lacak penggunaan Tingkat Gratis untuk akun yang dibuat sebelum 15 Juli 2025

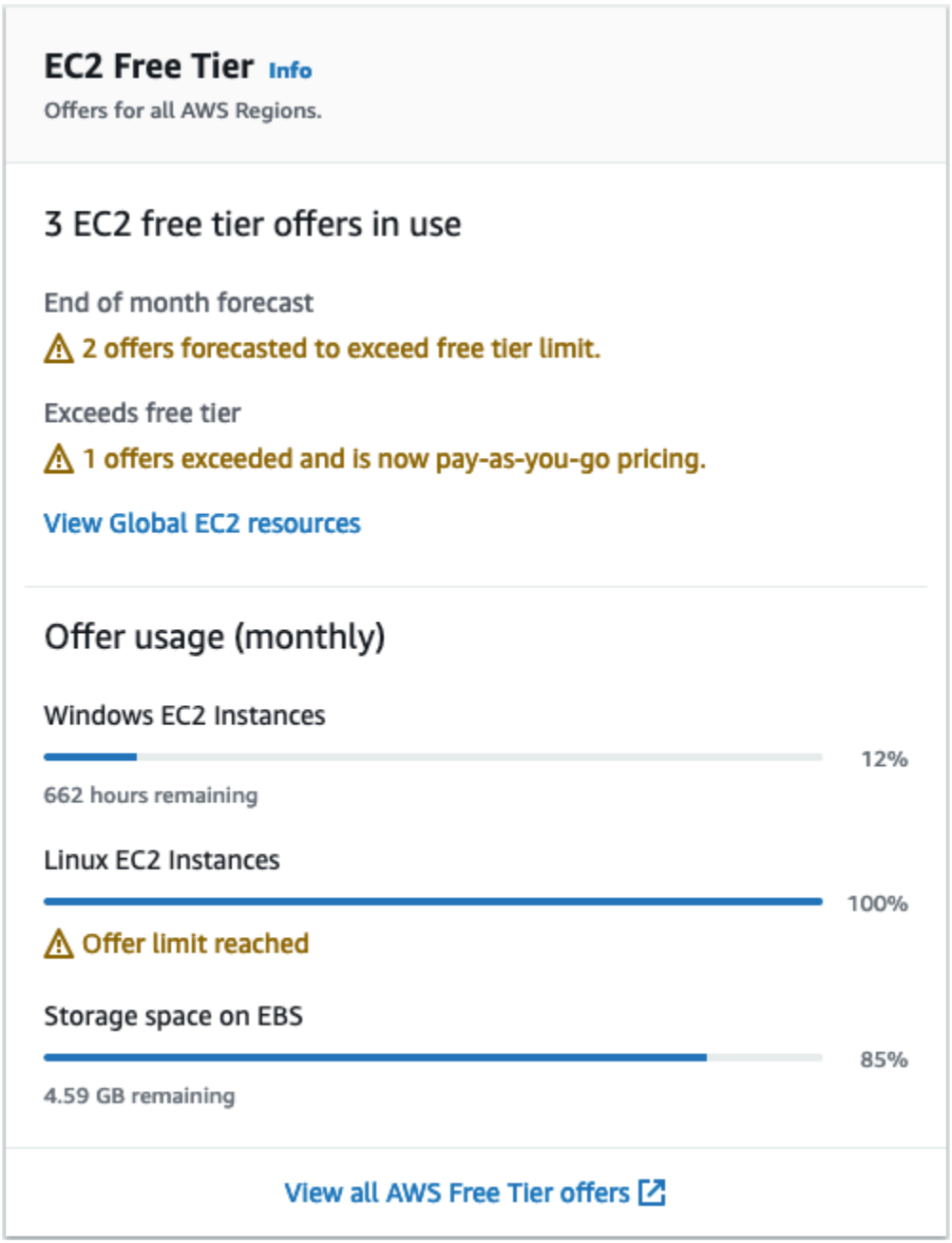
> **Note**
>
> Bagian ini hanya berlaku untuk pengguna Tingkat Gratis yang membuat Akun AWS sebelum 15 Juli 2025. Jika Anda membuat akun pada atau setelah 15 Juli 2025, lihat Melacak penggunaan Tingkat AWS Gratis Anda di Panduan AWS Billing Pengguna.

Jika Anda membuat akun sebelum 15 Juli 2025, Anda dapat menggunakan Amazon EC2 tanpa dikenakan biaya jika Anda telah AWS menjadi pelanggan kurang dari 12 bulan dan Anda tetap dalam batas penggunaan. AWS Tingkat Gratis Penting untuk melacak penggunaan Tingkat Gratis Anda guna menghindari tagihan yang tidak terduga. Jika Anda melebihi batas Tingkat Gratis, Anda akan dikenakan pay-as-go biaya standar. Untuk informasi selengkapnya, lihat AWS Tingkat Gratis.

> **Note**
>
> Jika Anda telah menjadi AWS pelanggan selama lebih dari 12 bulan, Anda tidak lagi memenuhi syarat untuk penggunaan Tingkat Gratis dan Anda tidak akan melihat kotak Tingkat Gratis EC2 yang dijelaskan dalam prosedur berikut.

Untuk melacak penggunaan Tingkat Gratis Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor EC2.
3. Temukan kotak Tingkat Gratis EC2 (di bagian kanan atas).



4. Di kotak Tingkat Gratis EC2, centang penggunaan Tingkat Gratis Anda, sebagai berikut:

   - Di bawah penawaran Tingkat Gratis EC2 yang digunakan, perhatikan peringatannya:
     - Prakiraan akhir bulan – Ini memberikan peringatan bahwa Anda akan dikenai biaya bulan ini jika melanjutkan dengan pola penggunaan saat ini.
     - Melebihi Tingkat Gratis – Ini memberikan peringatan bahwa Anda telah melebihi batas Tingkat Gratis dan Anda sudah dikenai biaya.

- Di bawah Penggunaan penawaran (bulanan), perhatikan penggunaan instans Linux, instans Windows, dan penyimpanan EBS Anda. Persentase menunjukkan jumlah batas Tingkat Gratis yang telah Anda gunakan bulan ini. Jika telah mencapai 100%, Anda akan dikenai biaya untuk penggunaan lebih lanjut.

> **Note**
>
> Informasi ini muncul hanya setelah Anda membuat instans. Namun, informasi penggunaan tidak diperbarui secara waktu nyata; informasi ini diperbarui tiga kali sehari.

5. Untuk menghindari biaya lebih lanjut, hapus sumber daya apa pun yang dikenai biaya saat ini, atau akan dikenai biaya jika Anda melebihi batas penggunaan Tingkat Gratis.

   - Untuk instruksi untuk menghapus instance Anda, lihatMengakhiri instans Amazon EC2.
   - Untuk memeriksa apakah Anda memiliki sumber daya di Wilayah lain yang mungkin menimbulkan biaya, di kotak Tingkat Gratis EC2, pilih Lihat sumber daya EC2 Global untuk membuka Tampilan Global EC2. Untuk informasi selengkapnya, lihat Melihat sumber daya di seluruh Wilayah menggunakan Tampilan AWS Global.

6. Untuk melihat penggunaan sumber daya Anda untuk semua Layanan AWS di bawah AWS Tingkat Gratis, di bagian bawah kotak Tingkat Gratis EC2, pilih Lihat semua AWS Tingkat Gratis penawaran. Untuk informasi selengkapnya, lihat Mencoba layanan yang digunakan AWS Tingkat Gratis dalam Panduan Pengguna AWS Penagihan.

Memahami kode untuk Amazon EC2 dalam laporan penagihan dan penggunaan

Saat Anda menggunakan Amazon EC2, kami menyertakan kode terkait dalam laporan AWS penagihan dan penggunaan Anda. Meninjau kode ini membantu Anda memahami biaya dan pola penggunaan untuk Amazon EC2. Melacak dan mengelola pengeluaran Anda sangat penting untuk mengoptimalkan biaya Anda.

Tabel berikut menjelaskan kode untuk Amazon EC2 yang muncul di laporan penagihan dan penggunaan Anda. Untuk daftar kode Wilayah yang digunakan dalam laporan penagihan dan penggunaan, lihat Kode penagihan AWS wilayah.

Kode penagihan untuk:

- Contoh
- Instans bare metal
- Host Khusus
- Instans Khusus
- Optimisasi EBS
- Reservasi Kapasitas

Sumber daya terkait

- the section called “Opsi penagihan dan pembelian”
- the section called “Memahami penagihan AMI”
- EC2 Harga Amazon

Contoh

Kode	Deskripsi	Unit
region-BoxUsage :*instance-type*	Waktu berjalan untuk Instans Sesuai Permintaan.	Jam
region-HostBoxUsage :*instance-type*	Waktu berjalan untuk instans pada Host Khusus.	Jam
region-SpotUsage :*instance-type*	Waktu berjalan untuk Instans Spot.	Jam

Instans bare metal

Kode	Deskripsi	Unit
region-BoxUsage : *instance-family* .logam	Waktu berjalan untuk Instans On-Demand bare metal.	Jam
region-HostBoxUsage : *instance-family* .logam	Waktu berjalan untuk instans bare metal di Host Khusus.	Jam
region-SpotUsage : *instance-family* .logam	Waktu berjalan untuk Instans Spot bare metal.	Jam

Host Khusus

Kode	Deskripsi	Unit
region-HostUsage :*host-type*	Waktu dimana Dedicated Host disediakan.	Jam
region-ReservedHostUsage :*host-type*	Waktu Reservasi Tuan Rumah Khusus diterapkan.	Jam

Instans Khusus

Kode	Deskripsi	Unit
region-DedicatedUsage :*instance-type*	Waktu berjalan untuk Instans Khusus.	Jam+Biaya per wilayah

Optimisasi EBS

Kode	Deskripsi	Unit
region-EBSOptimized :*instance-type*	Waktu optimasi EBS diaktifkan.	Jam

Reservasi Kapasitas

Kode	Deskripsi	Unit
region-Reservation :*instance-type*	Waktu instans yang dicadangkan untuk Reservasi Kapasitas.	Jam
region-UnusedBox :*instance-type*	Waktu instans cadangan yang tidak digunakan untuk Reservasi Kapasitas.	Jam
region-DedicatedRes :*instance-type*	Waktu instans yang dipesan untuk Reservasi Kapasitas Khusus.	Jam
region-UnusedDed :*instance-type*	Waktu instans cadangan yang tidak digunakan untuk Reservasi Kapasitas Khusus.	Jam

Buat inventaris EC2 instans Anda

Amazon EC2 menyediakan kapasitas komputasi sesuai permintaan dan skalabel. EC2 Instance adalah server virtual yang berjalan di AWS jaringan.

Tabel berikut menjelaskan karakteristik kunci dari sebuah EC2 instance. Administrator sistem dapat menggunakan panduan yang disediakan dalam panduan ini untuk mendapatkan informasi tentang

karakteristik ini dan menggunakannya untuk mengonfigurasi server yang setara secara fungsional yang berjalan di tempat atau di jaringan Penyedia Cloud lain.

Karakteristik	Deskripsi
Lokasi geografis	Amazon EC2 di-host di semua AWS Wilayah di seluruh dunia. Anda memilih lokasi untuk instans Anda yang menempatkan mereka dekat dengan pelanggan Anda. Anda dapat meluncurkan instance di beberapa lokasi.
Spesifikasi perangkat keras	Amazon EC2 menyediakan berbagai pilihan jenis instans, dioptimalkan untuk kasus penggunaan yang berbeda. Jenis instans yang Anda pilih untuk instans menentukan sumber daya komputasi, memori, jaringan, dan penyimpanannya.
Gambar	Amazon Machine Image (AMI) menyertakan perangkat lunak untuk diinstal pada instans Anda saat peluncuran. Ini termasuk sistem operasi, paket perangkat lunak, dan konfigurasi khusus.
Alamat IP dan nama host DNS	Instans menerima alamat IP pribadi dan nama host DNS pribadi. Jika Anda mengonfigurasi alamat IP publik untuk sebuah instance, itu juga menerima nama host DNS publik.
Aturan grup keamanan	Aturan grup keamanan yang terkait dengan instans Anda menentukan lalu lintas masuk dan lalu lintas keluar yang diizinkan.
Data pengguna	Data pengguna tersedia untuk instance saat peluncuran. Ini terdiri dari skrip shell (Linux) atau PowerShell skrip (Windows).

Lokasi geografis

Amazon EC2 tersedia di setiap AWS Wilayah di seluruh dunia. Setiap Wilayah adalah wilayah geografis yang terpisah. Anda dapat menurunkan latensi jaringan ketika Anda memilih Wilayah untuk server Anda yang dekat dengan mayoritas pengguna Anda.

Anda dapat menggunakan Amazon EC2 Global View untuk mencantumkan EC2 instans Amazon Anda di semua Wilayah. Dengan API Konsol Manajemen AWS dan API, Anda harus mencantumkan instance untuk setiap Wilayah satu per satu.

Mengapa ini penting

Setelah menentukan lokasi instans, Anda dapat memutuskan apakah akan menggunakan server yang setara secara fungsional di lokasi yang sama atau lokasi berbeda, tergantung pada kebutuhan Anda.

Untuk mendapatkan ringkasan EC2 instans Anda di semua Wilayah

1. Buka konsol Amazon EC2 Global View di https://console.aws.amazon.com/ec2globalview/rumah.
2. Pada tab Region explorer, di bawah Ringkasan, periksa jumlah sumber daya untuk Instans, yang mencakup jumlah instance dan jumlah Wilayah. Klik teks yang digarisbawahi untuk melihat bagaimana jumlah instance tersebar di seluruh Wilayah.
3. Pada tab Pencarian global, pilih filter klien Jenis sumber daya = Instance. Anda dapat memfilter hasil lebih lanjut dengan menentukan Wilayah atau tag.

Untuk mendapatkan jumlah EC2 instance di Wilayah menggunakan AWS CLI

Gunakan perintah describe-instance berikut untuk menghitung instance di Region yang ditentukan. Anda harus menjalankan perintah ini di setiap Wilayah di mana Anda memiliki instance.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "length(Reservations[*].Instances[])"
```

Berikut ini adalah output contoh.

```
27
```

Untuk mendapatkan daftar instance IDs alih-alih hitungan instance, gunakan `--query` parameter berikut sebagai gantinya.

```
--query "Reservations[*].Instances[].InstanceId"
```

Spesifikasi perangkat keras

Jenis instans yang Anda tentukan untuk sebuah EC2 instance menentukan komputasi, memori, penyimpanan, dan sumber daya jaringan yang tersedia untuknya. Setiap keluarga instance menawarkan keseimbangan sumber daya komputasi, memori, jaringan, dan penyimpanan yang berbeda. Untuk informasi selengkapnya, lihat Panduan Jenis EC2 Instans Amazon.

Mengapa ini penting

Setelah Anda menentukan spesifikasi perangkat keras untuk instans Anda, Anda dapat memutuskan spesifikasi minimum yang diperlukan untuk server yang setara secara fungsional.

Untuk mendapatkan ringkasan dari jenis instans yang digunakan oleh instans Anda

Gunakan perintah describe-instance berikut. sedPerintah menghapus baris dengan tanda kurung dan baris kosong. Anda harus menjalankan perintah ini di setiap Wilayah di mana Anda memiliki instance.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].InstanceType" | sed 's/[][]//g;/^$/d' | sort |
 uniq -c | sort -nr
```

Berikut ini adalah output contoh.

```
  20    "c6i.4xlarge",
   5    "t2.micro",
   2    "g6e.2xlarge",
```

Untuk mendapatkan informasi tentang jenis instance tertentu

Gunakan describe-instance-typesperintah berikut untuk menggambarkan jenis instance. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Ini adalah karakteristik dasar. Anda dapat menyertakan bidang tambahan apa pun yang Anda perlukan, atau Anda dapat merujuk ke spesifikasi jenis EC2 instans Amazon di Panduan Jenis EC2 Instans Amazon.

```
aws ec2 describe-instance-types \
```

```
    --instance-types c6i.4xlarge t2.micro g6e.2xlarge \
    --query "InstanceTypes[*].
[InstanceType,VCpuInfo.DefaultVCpus,MemoryInfo.SizeInMiB,NetworkInfo.NetworkPerformance]"
 \
    --output table
```

Berikut ini adalah output contoh. Kolom adalah tipe instance, vCPUs, memori (GiB), dan bandwidth jaringan (Gbps).

```
-----------------------------------------------------
|               DescribeInstanceTypes               |
+--------------+-----+--------+----------------------+
|  t2.micro    |  1  |  1024  |  Low to Moderate     |
|  c6i.4xlarge |  16 |  32768 |  Up to 12.5 Gigabit  |
|  g6e.2xlarge |  8  |  65536 |  Up to 20 Gigabit    |
+--------------+-----+--------+----------------------+
```

Citra

Amazon Machine Image (AMI) menyediakan perangkat lunak yang diinstal pada instans Anda saat peluncuran, seperti sistem operasi, layanan, alat pengembangan, dan aplikasi. Anda dapat mengekspor AMI ke format lain untuk digunakan dengan server lain.

Mengapa ini penting

Setelah menentukan instans, Anda dapat merencanakan gambar yang diperlukan untuk server yang setara secara fungsional. AMIs Dimungkinkan untuk mengekspor Anda AMIs ke format yang dapat Anda gunakan di tempat lain. Atau, Anda mungkin perlu menyambung ke instance yang diluncurkan dari setiap AMI, mengonfirmasi apa yang diinstal dan bagaimana konfigurasinya, dan memastikan bahwa Anda memiliki salinan semua yang Anda butuhkan.

Untuk mendapatkan AMIs contoh Anda

Gunakan perintah describe-instance berikut. sedPerintah menghapus baris dengan tanda kurung dan baris kosong. Anda harus menjalankan perintah ini di setiap Wilayah di mana Anda memiliki instance.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].ImageId" | sed 's/[][]//g;/^$/d' | sort | uniq
 -c | sort -nr
```

Berikut ini adalah output contoh.

```
20     "ami-0a70b9d193ae8a79",
 5     "ami-07d9cf938edb0739b",
 2     "ami-09245d5773578a1d6",
```

Untuk mendapatkan informasi tentang spesifik AMIs

Gunakan perintah deskripsi-gambar berikut. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan apa pun yang Anda butuhkan.

```
aws ec2 describe-images \
    --image-id ami-0a70b9d193ae8a79 ami-07d9cf938edb0739b ami-09245d5773578a1d6 \
    --query "Images[*].
{ID:ImageId,CreateDate:CreationDate,Name:Name,Description:Description}"
```

Berikut ini adalah output contoh.

```
[
    {
        "ID": "ami-0a70b9d193ae8a799",
        "CreateDate": "2025-03-01T02:22:41.000Z",
        "Name": "web-server-3.1",
        "Description": "Image for web servers"
    },
    {
        "ID": "ami-07d9cf938edb0739b",
        "CreateDate": "2025-02-01T23:59:03.000Z",
        "Name": "awesome-application-11.5",
        "Description": "Image for Awesome Application"
    },
    {
        "ID": "ami-09245d5773578a1d6",
        "CreateDate": "2025-01-31T02:22:41.000Z",
        "Name": "monitoring-4.2",
        "Description": "Monitoring software"
    }
]
```

Untuk membuat file VM dari AMI

Gunakan perintah export-image. Format gambar yang didukung adalah VHD (kompatibel dengan Citrix Xen dan Microsoft Hyper-V), VMDK (kompatibel VMware dengan ESX dan vSphere), VMware

dan format mentah (kompatibel dengan hypervisor KVM dan Xen). Untuk informasi tentang persyaratan dan batasan Impor/Ekspor VM, lihat persyaratan VM. Import/Export

Alamat IP dan nama host DNS

Pengguna Anda terhubung ke EC2 instans Anda melalui internet menggunakan nama host DNS publik mereka. Nama host DNS publik dari sebuah EC2 instans menyelesaikan ke alamat IP publiknya. EC2 instance dapat berkomunikasi satu sama lain menggunakan alamat IP pribadi mereka.

Mengapa ini penting

Alamat IP memungkinkan perangkat untuk berkomunikasi satu sama lain melalui jaringan lokal atau internet. Dengan mencatat alamat IP dan nama DNS dari instans Anda, Anda dapat membantu memastikan bahwa server yang setara secara fungsional dapat berkomunikasi dengan klien atau perangkat yang sama dengan instans Anda. Misalnya, Anda dapat memperbarui konfigurasi penyeimbang beban atau catatan DNS yang Anda buat untuk penyedia DNS Anda.

Untuk mendapatkan alamat IP dan nama host DNS untuk instans Anda

Gunakan perintah describe-instance berikut. Anda harus menjalankan perintah ini di setiap Wilayah di mana Anda memiliki instance. `--query`Parameter hanya mencakup bidang yang ditentukan dalam output. Anda dapat menyertakan bidang tambahan apa pun yang Anda butuhkan.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].[InstanceId,PrivateIpAddress,PublicDnsName]" \
    --output table
```

Berikut ini adalah output contoh. Kolom tersebut adalah ID instance, IPv4 alamat pribadi, dan nama IPv4 DNS publik.

```
----------------------------------------------------------------------------------
|                                DescribeInstances                               |
 |
+---------------------+-----------+-------------------------------------------------
+
| i-0bac57d7472c89bac | 10.0.2.139 | ec2-192-0-2-142.us-east-2.compute.amazonaws.com
 |
| i-0fa8b7678975a3fff | 10.0.14.85 | ec2-198-51-100-56.us-east-2.compute.amazonaws.com
 |
```

```
  ...
  ...
| i-08fd74f3f1595fdbd | 10.0.1.241 | ec2-203.0.113.13.us-east-2.compute.amazonaws.com
 |
+--------------------+-----------+-------------------------------------------------
+
```

Aturan-aturan grup keamanan

Grup keamanan bertindak sebagai firewall virtual. Setelah Anda mengaitkan grup keamanan dengan EC2 instans, aturannya mengizinkan lalu lintas masuk dan keluar untuk EC2 instance melalui port dan protokol tertentu.

Mengapa ini penting

Setelah Anda menentukan lalu lintas masuk yang diizinkan untuk mencapai server Anda dan lalu lintas keluar yang diizinkan untuk meninggalkan server Anda, Anda dapat merencanakan aturan firewall yang diperlukan untuk server yang setara secara fungsional.

Untuk mendapatkan grup keamanan untuk instans Anda

Gunakan perintah describe-instance berikut. sedPerintah menghapus baris dengan tanda kurung dan baris kosong. Anda harus menjalankan perintah ini di setiap Wilayah di mana Anda memiliki instance.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].SecurityGroups[].GroupId" | sed 's/[][]//g;/^
$/d' | sort | uniq -c | sort -nr
```

Berikut ini adalah output contoh.

```
27     "sg-01dd3383691d02f42",
10     "sg-08c77cc910c0b3b2c",
 2     "sg-00f4e409629f1a42d",
```

Untuk mendapatkan aturan masuk untuk grup keamanan

Gunakan describe-security-group-rulesperintah berikut untuk menampilkan aturan untuk grup keamanan yang ditentukan di mana `IsEgress` berada`false`.

```
aws ec2 describe-security-group-rules \
```

```
    --filters Name=group-id,Values=sg-01dd3383691d02f42 \
    --query 'SecurityGroupRules[?IsEgress==`false`]'
```

Berikut ini adalah output contoh. Aturan pertama adalah aturan masuk default, yang memungkinkan lalu lintas masuk dari semua sumber daya yang ditetapkan ke grup keamanan ini. Aturan lain memungkinkan lalu lintas SSH dari alamat IP dalam daftar awalan yang ditentukan. Untuk menggambarkan blok CIDR dalam daftar awalan, gunakan perintah. describe-prefix-lists

```
[
    {
        "SecurityGroupRuleId": "sgr-06c8b42574a91db1b",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": false,
        "IpProtocol": "-1",
        "FromPort": -1,
        "ToPort": -1,
        "ReferencedGroupInfo": {
            "GroupId": "sg-01dd3383691d02f42",
            "UserId": "123456789012"
        },
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-west-2:123456789012:security-group-
rule/sgr-06c8b42574a91db1b"
    },
    {
        "SecurityGroupRuleId": "sgr-0886a5d46afcd1758",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": false,
        "IpProtocol": "tcp",
        "FromPort": 22,
        "ToPort": 22,
        "PrefixListId": "pl-f8a6439125e7bf465",
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:123456789012:security-group-
rule/sgr-0886a5d46afcd1758"
    }
]
```

Untuk mendapatkan aturan keluar untuk grup keamanan

Gunakan describe-security-group-rulesperintah berikut untuk menampilkan aturan untuk grup keamanan yang ditentukan di mana `IsEgress` beradatrue.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-01dd3383691d02f42 \
    --query 'SecurityGroupRules[?IsEgress==`true`]'
```

Berikut ini adalah output contoh. Ini hanya berisi aturan keluar default, yang memungkinkan semua lalu lintas keluar IPv4 .

```
[
    {
        "SecurityGroupRuleId": "sgr-048f09a719247dce7",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": true,
        "IpProtocol": "-1",
        "FromPort": -1,
        "ToPort": -1,
        "CidrIpv4": "0.0.0.0/0",
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:123456789012:security-group-
rule/sgr-048f09a719247dce7"
    }
]
```

Data pengguna

Saat meluncurkan EC2 instance, Anda dapat meneruskan skrip shell ke instance menggunakan data pengguna. Perhatikan bahwa data pengguna dikodekan base64, jadi Anda perlu memecahkan kode data pengguna untuk membaca skrip.

Mengapa ini penting

Jika menjalankan perintah saat peluncuran sebagai bagian dari pengaturan instance, Anda mungkin perlu melakukan tugas yang sama saat menyiapkan server yang setara secara fungsional.

Untuk melihat data pengguna yang didekodekan untuk sebuah instance

Gunakan perintah berikut describe-instance-attribute. base64Perintah menerjemahkan data pengguna.

```
aws ec2 describe-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --attribute userData \
    --output text \
    --query "UserData.Value" | base64 --decode
```

Berikut ini adalah output contoh.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Sumber daya terkait

Berikut ini adalah karakteristik tambahan dari EC2 contoh:

- Pasangan kunci
- Penyimpanan
- Tanda

Anda dapat memverifikasi apakah Anda menggunakan yang berikut ini untuk meluncurkan EC2 instance atau mendistribusikan lalu lintas antar EC2 instans Anda:

- Grup Auto Scaling
- EC2 Armada
- Elastic Load Balancing

Memecahkan masalah dengan instans Amazon EC2

Prosedur dan tips berikut dapat membantu Anda memecahkan masalah dengan instans Amazon EC2 Anda.

Masalah

- Memecahkan masalah peluncuran instans Amazon EC2
- Memecahkan masalah penghentian EC2 instans Amazon
- Memecahkan masalah penghentian instans Amazon EC2
- Memecahkan masalah instans Amazon EC2 yang tidak terjangkau
- Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda
- Memecahkan masalah instans Amazon EC2 Linux dengan pemeriksaan status yang gagal
- Memecahkan masalah booting instans Amazon EC2 Linux dari volume yang salah
- Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Windows
- Memecahkan masalah awal instans Amazon EC2 Windows
- Memecahkan masalah dengan instans Windows Amazon EC2
- Setel ulang kata sandi administrator Windows untuk instans Windows Amazon EC2
- Memecahkan masalah Sysprep dengan instans Windows Amazon EC2
- Memecahkan masalah instans Amazon EC2 Linux yang terganggu menggunakan Rescue EC2
- Memecahkan masalah instans Windows Amazon EC2 yang terganggu menggunakan Rescue EC2
- EC2 Serial Console untuk instans
- Kirim interupsi diagnostik untuk men-debug instans Amazon EC2 yang tidak dapat dijangkau

Memecahkan masalah peluncuran instans Amazon EC2

Berikut ini adalah tips pemecahan masalah untuk membantu Anda memecahkan masalah saat meluncurkan instans Amazon EC2.

Masalah Peluncuran

- Nama perangkat tidak valid
- Batas instans terlampaui

- Kapasitas instans tidak cukup
- Konfigurasi yang diminta saat ini tidak didukung. Periksa dokumentasi untuk konfigurasi yang didukung.
- Instans langsung terhenti
- Izin tidak cukup
- Penggunaan CPU yang tinggi segera setelah Windows dimulai (hanya instance Windows)
- Meluncurkan instance IMDSv1 -enabled gagal

Nama perangkat tidak valid

Deskripsi

Anda mendapatkan kesalahan `Invalid device name` *`device_name`* saat mencoba meluncurkan instans baru.

Penyebab

Jika Anda mendapatkan kesalahan ini saat mencoba meluncurkan instans, nama perangkat yang ditentukan untuk satu atau beberapa volume dalam permintaan memiliki nama perangkat yang tidak valid. Kemungkinan penyebabnya meliputi:

- Nama perangkat mungkin digunakan oleh AMI yang dipilih.
- Nama perangkat mungkin dipesan untuk volume root.
- Nama perangkat mungkin digunakan untuk volume lain dalam permintaan.
- Nama perangkat mungkin tidak valid untuk sistem operasi.

Solusi

Untuk mengatasi masalah ini:

- Pastikan nama perangkat tidak digunakan di AMI yang Anda pilih. Jalankan perintah berikut untuk menampilkan nama perangkat yang digunakan oleh AMI.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890 --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Pastikan Anda tidak menggunakan nama perangkat yang dipesan untuk volume root. Untuk informasi selengkapnya, lihat Nama perangkat yang tersedia.
- Pastikan setiap volume yang ditentukan dalam permintaan Anda memiliki nama perangkat yang unik.
- Pastikan nama perangkat yang Anda tentukan berada menggunakan format yang benar. Untuk informasi selengkapnya, lihat Nama perangkat yang tersedia.

Batas instans terlampaui

Deskripsi

Anda mendapatkan kesalahan `InstanceLimitExceeded` saat mencoba meluncurkan instans baru atau memulai ulang instans yang terhenti.

Penyebab

Jika Anda mendapatkan kesalahan `InstanceLimitExceeded` saat mencoba meluncurkan instans baru atau memulai ulang instans yang terhenti, Anda telah mencapai batas jumlah instans yang dapat Anda luncurkan di Wilayah. Saat Anda membuat AWS akun, kami menetapkan batas default pada jumlah instans yang dapat Anda jalankan per wilayah.

Solusi

Anda dapat meminta kenaikan batas instans berdasarkan wilayah. Untuk informasi selengkapnya, lihat Kuota EC2 layanan Amazon.

Kapasitas instans tidak cukup

Deskripsi

Anda mendapatkan kesalahan `InsufficientInstanceCapacity` saat mencoba meluncurkan instans baru atau memulai ulang instans yang terhenti.

Penyebab

Jika Anda mendapatkan kesalahan ini saat mencoba meluncurkan instans atau memulai ulang instans yang terhenti, saat ini, AWS tidak memiliki kapasitas Sesuai Permintaan yang cukup untuk memenuhi permintaan Anda.

Solusi

Untuk mengatasi masalah ini, coba lakukan hal berikut:

- Tunggu beberapa menit, lalu kirim permintaan Anda lagi; kapasitas sering kali dapat berubah.
- Kirim permintaan baru dengan jumlah instans yang lebih sedikit. Misalnya, jika Anda membuat permintaan tunggal untuk meluncurkan 15 instans, cobalah membuat 3 permintaan untuk 5 instans, atau 15 permintaan untuk 1 instans.
- Jika Anda meluncurkan instans, kirimkan permintaan baru tanpa menentukan Zona Ketersediaan.
- Jika Anda meluncurkan instans, kirimkan permintaan baru menggunakan tipe instans yang berbeda (yang dapat diubah ukurannya di tahap berikutnya). Untuk informasi selengkapnya, lihat Perubahan jenis instans Amazon EC2.
- Jika Anda meluncurkan instans ke grup penempatan klaster, Anda bisa mendapatkan kesalahan kapasitas yang tidak memadai.

Konfigurasi yang diminta saat ini tidak didukung. Periksa dokumentasi untuk konfigurasi yang didukung.

Deskripsi

Anda mendapatkan kesalahan `Unsupported` saat mencoba meluncurkan instans baru karena konfigurasi instans tidak didukung.

Penyebab

Pesan kesalahan memberikan detail tambahan. Misalnya, tipe instans atau opsi pembelian instans mungkin tidak didukung di dalam Wilayah atau Zona Ketersediaan tertentu.

Solusi

Coba konfigurasi instans yang berbeda. Untuk mencari tipe instans yang memenuhi persyaratan Anda, lihat Temukan jenis EC2 instans Amazon.

Instans langsung terhenti

Deskripsi

Instans Anda berubah dari status `pending` menjadi status `terminated`.

Penyebab

Berikut ini adalah beberapa alasan instans dapat langsung terhenti:

- Anda telah melebihi batas volume EBS. Untuk informasi selengkapnya, lihat Batas volume Amazon EBS untuk instans Amazon EC2.
- Snapshot EBS rusak.
- Volume EBS root terenkripsi dan Anda tidak memiliki izin guna mengakses kunci KMS untuk dekripsi.
- Snapshot yang ditentukan dalam pemetaan perangkat blok untuk AMI dienkripsi dan Anda tidak memiliki izin guna mengakses kunci KMS untuk dekripsi atau Anda tidak memiliki akses ke kunci KMS untuk mengenkripsi volume yang dipulihkan.
- AMI yang didukung Amazon S3 yang Anda gunakan untuk meluncurkan instance tidak memiliki bagian wajib (image.part. berkas xx).

Untuk informasi selengkapnya, dapatkan alasan penghentian menggunakan salah satu metode berikut.

Untuk mendapatkan alasan penghentian menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, dan pilih instans.
3. Di tab pertama, cari alasannya di samping Alasan transisi status.

Untuk mendapatkan alasan penghentian menggunakan AWS CLI

1. Gunakan perintah describe-instances dan tentukan ID instans.

   ```
   aws ec2 describe-instances --instance-id i-1234567890abcdef0
   ```

2. Tinjau respons JSON yang dikembalikan oleh perintah dan perhatikan nilainya di elemen respons `StateReason`.

   Blok kode berikut ini menunjukkan contoh elemen respons `StateReason`.

   ```
   "StateReason": {
     "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
     "Code": "Server.InternalError"
   ```

```
},
```

Untuk mendapatkan alasan penghentian menggunakan AWS CloudTrail

Untuk informasi selengkapnya, lihat Melihat CloudTrail peristiwa dengan riwayat peristiwa di Panduan AWS CloudTrail Pengguna.

Solusi

Dengan bergantung pada alasan penghentian, lakukan salah satu tindakan berikut:

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** – Hapus volume yang tak terpakai. Anda dapat mengirim permintaan untuk meningkatkan batas volume.
- **`Client.InternalError: Client error on launch`**— Pastikan Anda memiliki izin yang diperlukan untuk mengakses yang AWS KMS keys digunakan untuk mendekripsi dan mengenkripsi volume. Untuk informasi selengkapnya, lihat Menggunakan kebijakan kunci di AWS KMS dalam Panduan Developer AWS Key Management Service .

Izin tidak cukup

Deskripsi

Anda mendapatkan kesalahan `"errorMessage": "You are not authorized to perform this operation."` saat mencoba meluncurkan instans baru, dan peluncuran tersebut gagal.

Penyebab

Jika Anda mendapatkan kesalahan ini saat mencoba meluncurkan instans, Anda tidak memiliki izin IAM yang diperlukan untuk meluncurkan instans tersebut.

Kemungkinan izin yang ada mencakup:

- `ec2:RunInstances`
- `iam:PassRole`

Izin lain mungkin juga tidak ada. Untuk daftar izin yang diperlukan guna meluncurkan instans, lihat contoh kebijakan IAM di bawah Contoh: Menggunakan wizard peluncuran instans EC2 dan Luncurkan instance () RunInstances.

Solusi

Untuk mengatasi masalah ini:

- Jika Anda membuat permintaan sebagai pengguna IAM, verifikasi bahwa Anda memiliki izin berikut:
  - `ec2:RunInstances` dengan sumber daya wildcard ("*")
  - `iam:PassRole` dengan sumber daya yang cocok dengan ARN peran (misalnya, `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Jika Anda tidak memiliki izin sebelumnya, edit kebijakan IAM yang terkait dengan peran atau pengguna IAM untuk menambahkan izin penting yang tidak ada.

Jika masalah tidak teratasi dan Anda terus menerima kesalahan kegagalan peluncuran, Anda dapat melakukan dekode pesan kegagalan otorisasi yang disertakan dalam kesalahan. Pesan yang didekodekan mencakup izin yang tidak ada dari kebijakan IAM. Untuk informasi selengkapnya, lihat Bagaimana cara memecahkan kode pesan kegagalan otorisasi setelah saya menerima kesalahan "UnauthorizedOperation" selama peluncuran instans EC2?

Penggunaan CPU yang tinggi segera setelah Windows dimulai (hanya instance Windows)

> **Note**
>
> Tip pemecahan masalah ini hanya untuk instance Windows.

Jika Pembaruan Windows diatur ke Periksa pembaruan, tetapi biarkan saya memilih apakah akan mengunduh dan menginstalnya (pengaturan instans default), pemeriksaan ini dapat menghabiskan sekitar 50 - 99% CPU pada instans. Jika penggunaan CPU ini menyebabkan masalah pada aplikasi, Anda dapat mengubah pengaturan Pembaruan Windows secara manual di Panel Kontrol atau Anda dapat menggunakan skrip berikut di bidang data pengguna Amazon EC2:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Saat Anda menjalankan skrip ini, tentukan nilai untuk /d. Nilai default-nya adalah 3. Kemungkinan nilainya mencakup berikut ini:

1. Jangan pernah memeriksa pembaruan
2. Periksa pembaruan, tetapi biarkan saya memilih apakah akan mengunduh dan menginstalnya
3. Unduh pembaruan, tetapi biarkan saya memilih apakah akan menginstalnya
4. Instal pembaruan secara otomatis

Setelah Anda memodifikasi data pengguna untuk instans, Anda dapat menjalankannya. Untuk informasi selengkapnya, lihat Menjalankan perintah pada instans Windows Anda saat diluncurkan.

Meluncurkan instance IMDSv1 -enabled gagal

Deskripsi

Anda mendapatkan `UnsupportedOperation` pengecualian dengan pesan berikut:

```
You can't launch instances with IMDSv1 because httpTokensEnforced
is enabled for this account. Either launch the instance with
httpTokens=required or contact your account owner to disable
httpTokensEnforced using the ModifyInstanceMetadataDefaults API or the
account settings in the EC2 console.
```

Penyebab

Kesalahan ini muncul saat Anda mencoba meluncurkan instance baru untuk IMDSv1 diaktifkan (`httpTokens = optional`) di akun tempat pengaturan akun EC2 atau kebijakan deklaratif AWS Organisasi memberlakukan penggunaan IMDSv2 (). `httpTokensEnforced = enabled`

Solusi

Jika Anda IMDSv2 hanya siap untuk menggunakan, luncurkan instance Anda dengan IMDSv1 disabled (`httpTokens = required`). Untuk memeriksa apakah Anda siap, lihatTransisi ke penggunaan Layanan Metadata Instans Versi 2.

Jika Anda masih memerlukan IMDSv1 dukungan pada instans baru atau yang sudah ada, Anda harus menonaktifkan IMDSv2 penegakan hukum untuk akun di Wilayah. Untuk menonaktifkan IMDSv2 penegakan, atur `HttpTokensEnforced` ke`disabled`. Untuk informasi selengkapnya, lihat ModifyInstanceMetadataDefaultsdi Referensi API Amazon EC2. Jika Anda lebih suka mengonfigurasi pengaturan ini menggunakan konsol, lihatMenegakkan IMDSv2 di tingkat akun.

Memecahkan masalah penghentian EC2 instans Amazon

Jika instans yang didukung Amazon EBS Anda tampak macet di `stopping` status, masalahnya mungkin ada pada komputer host yang mendasarinya.

Untuk mengatasi masalah ini, ikuti langkah-langkah berikut:

1. Paksa hentikan instance

   Gunakan EC2 konsol Amazon atau AWS CLI untuk menghentikan instance secara paksa. Untuk langkah-langkahnya, lihatPaksa menghentikan sebuah instance.

   Instance pertama-tama akan mencoba shutdown yang anggun, yang mencakup pembilasan cache sistem file dan metadata (meskipun Anda dapat secara opsional melewati shutdown yang anggun). Jika shutdown yang anggun gagal diselesaikan dalam periode batas waktu, instance dimatikan secara paksa tanpa membilas cache dan metadata sistem file.

2. Setelah berhenti paksa

   Lakukan prosedur pemeriksaan dan perbaikan sistem file.

   > **Important**
   >
   > Melakukan prosedur ini sangat penting karena penghentian paksa mencegah pembilasan cache dan metadata sistem file.

3. Jika force stop gagal

   Jika, setelah 10 menit, instance belum berhenti, lakukan hal berikut:

   a. Posting permintaan bantuan di AWS re:Post. Untuk membantu mempercepat resolusi, sertakan ID instans, dan jelaskan langkah-langkah yang telah Anda ambil.

   b. Atau, jika Anda memiliki paket dukungan, buat kasus dukungan teknis dalam Pusat Dukungan.

   c. Sambil menunggu bantuan, Anda dapat membuat instance pengganti jika diperlukan. Untuk langkah-langkahnya, lihat(Opsional) Buat instance pengganti.

Tidak ada biaya untuk penggunaan instans selagi instans dalam status `stopping` atau dalam status lain kecuali, `running`. Anda tidak dikenai biaya untuk penggunaan instans saat instans dalam status `running`.

Daftar Isi

- Paksa menghentikan sebuah instance
- (Opsional) Buat instance pengganti

Paksa menghentikan sebuah instance

Anda dapat memaksa sebuah instance untuk berhenti. Jika setelah 10 menit instans tidak berhenti, unggah permintaan bantuan AWS re:Post. Untuk membantu mempercepat resolusi, sertakan ID instans, dan jelaskan langkah-langkah yang telah Anda ambil. Atau, jika Anda memiliki paket dukungan, buat kasus dukungan teknis dalam Pusat Dukungan.

> **Note**
>
> Dengan menggunakan konsol, Anda dapat memaksa instance untuk berhenti saat instance hanya dalam `stopping` status. Dengan menggunakan AWS CLI, Anda dapat memaksa sebuah instance untuk berhenti saat instance berada dalam`pending`,`running`, atau `stopping` status.

Console

Untuk memaksa menghentikan sebuah instance

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans, kemudian pilih instans yang macet.
3. Pilih status Instance, Force stop instance.

   Perhatikan bahwa Penghentian paksa instans hanya tersedia di konsol jika instans Anda dalam status `stopping`. Jika instance Anda dalam keadaan lain (kecuali `shutting-down` dan`terminated`), Anda dapat menggunakan AWS CLI untuk menghentikan instance Anda secara paksa.
4. (Opsional) Untuk melewati shutdown OS yang anggun selama force stop, pilih kotak centang Lewati OS shutdown.

5. Pilih Force stop.

AWS CLI

Untuk memaksa menghentikan sebuah instance

Gunakan perintah stop-instance dengan opsi. `--force`

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --force
```

Untuk melewati shutdown OS yang anggun selama force stop, sertakan opsi. `--skip-os-shutdown`

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --force \
    --skip-os-shutdown
```

PowerShell

Untuk memaksa menghentikan sebuah instance

Gunakan Stop-EC2Instancecmdlet dan atur `-Enforce` ke. `true`

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true
```

Untuk melewati shutdown OS yang anggun selama force stop, sertakan. `-SkipOsShutdown $true`

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true `
    -SkipOsShutdown $true
```

(Opsional) Buat instance pengganti

Saat Anda menunggu bantuan dari AWS re:Postatau Support Center, Anda dapat membuat instance pengganti jika diperlukan. Buat AMI dari instance yang macet, dan luncurkan instance baru menggunakan AMI baru.

> **Important**
>
> Anda dapat membuat instance pengganti jika instance yang macet hanya menghasilkan pemeriksaan status sistem, karena pemeriksaan status instance akan mengakibatkan AMI menyalin replika sistem operasi yang rusak. Setelah Anda mengonfirmasi pesan status, buat AMI dan luncurkan instance baru menggunakan AMI baru.

Console

Untuk membuat instance pengganti

1. Buka EC2 konsol Amazon di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Instans, kemudian pilih instans yang macet.
3. Pilih Tindakan, Gambar dan templat, Buat gambar.
4. Pada halaman Buat gambar, lakukan hal berikut:
   a. Masukkan nama dan deskripsi untuk AMI.
   b. Hapus contoh Reboot.
   c. Pilih Buat gambar.

   Untuk informasi selengkapnya, lihat the section called “Buat AMI dari sebuah instance”.
5. Luncurkan instans baru dari AMI dan verifikasi bahwa instans baru tersebut berfungsi.
6. Pilih instance yang macet, dan pilih Actions, Instance state, Terminate (delete) instance. Jika instance juga macet saat dihentikan, Amazon EC2 secara otomatis memaksanya untuk berhenti dalam beberapa jam.

Jika Anda tidak dapat membuat AMI dari instans seperti yang dijelaskan dalam prosedur sebelumnya, Anda dapat mengatur instans pengganti sebagai berikut:

(Alternatif) Untuk membuat instans pengganti menggunakan konsol

1. Pilih instans dan pilih Deskripsi, Perangkat blok. Pilih setiap volume dan catat ID volumenya. Pastikan untuk mencatat volume yang merupakan volume root.
2. Di panel navigasi, pilih Volume. Pilih setiap volume untuk instans tersebut, lalu pilih Tindakan, Buat Snapshot.
3. Di panel navigasi, pilih Snapshot. Pilih snapshot yang baru saja Anda buat, lalu pilih Tindakan, Buat Volume.
4. Luncurkan instans menggunakan sistem operasi yang sama dengan instans yang macet. Catat ID volume dan nama perangkat volume root-nya.
5. Di panel navigasi, pilih Instans, pilih instans yang baru saja Anda luncurkan, lalu pilih Status instans, Hentikan instans.
6. Di panel navigasi, pilih Volume, pilih volume root dari instans yang dihentikan, lalu pilih Tindakan, Copot Volume.
7. Pilih volume root yang Anda buat dari instans yang macet, pilih Tindakan, Lampirkan Volume, dan lampirkan ke instans yang baru sebagai volume root-nya (menggunakan nama perangkat yang Anda catat). Lampirkan volume non-root tambahan ke instans.
8. Di panel navigasi, pilih Instans, lalu pilih instans pengganti. Pilih Status instans, Mulai instans. Verifikasi bahwa instans berfungsi.
9. Pilih instance yang macet, pilih Instance state, Terminate (delete) instance. Jika instance juga macet saat dihentikan, Amazon EC2 secara otomatis memaksanya untuk berhenti dalam beberapa jam.

AWS CLI

Untuk membuat instance pengganti

1. Buat AMI dari instance macet menggunakan perintah create-image dengan opsi. `--no-reboot`

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "my-replacement-ami" \
    --description "AMI for replacement instance" \
    --no-reboot
```

2. Luncurkan instance baru dari AMI yang baru saja Anda buat, menggunakan perintah run-instance.
3. Verifikasi bahwa instans baru berfungsi.
4. (Opsional) Hentikan instance yang macet menggunakan perintah terminate-instance.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Untuk membuat instance pengganti

1. Buat AMI dari instance yang macet menggunakan New-EC2Imagecmdlet dan atur `-NoReboot` ke. `true`

```
New-EC2Image `
    -InstanceId i-1234567890abcdef0 `
    -Name "my-replacement-ami" `
    -Description "AMI for replacement instance" `
    -NoReboot $true
```

2. Luncurkan instance baru dari AMI yang baru saja Anda buat, menggunakan New-EC2Instancecmdlet.
3. Verifikasi bahwa instans baru berfungsi.
4. (Opsional) Hentikan instance yang macet menggunakan Remove-EC2Instancecmdlet.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Memecahkan masalah penghentian instans Amazon EC2

Mematikan atau menghapus instance Anda dikenal sebagai penghentian instance. Informasi berikut dapat membantu Anda memecahkan masalah saat Anda menghentikan instans Anda.

Anda tidak ditagih atas penggunaan instans apa pun saat instans tidak berada dalam status `running`. Dengan kata lain, saat Anda menghentikan sebuah instans, Anda tidak lagi dibebani biaya untuk instans tersebut segera setelah statusnya berubah menjadi `shutting-down`.

Instans langsung terhenti

Beberapa masalah dapat menyebabkan instans langsung terhenti pada saat memulai. Lihat Instans langsung terhenti untuk informasi selengkapnya.

Penghentian instans yang tertunda

Jika instans Anda tetap dalam `shutting-down` status lebih dari beberapa menit, itu mungkin karena:

- Instance menjalankan skrip shutdown.
- Ada masalah dengan komputer host yang mendasarinya.

Setelah beberapa jam di `shutting-down` negara bagian, Amazon EC2 memperlakukan instance sebagai macet dan secara paksa menghentikannya.

Untuk menyelesaikan sendiri instance yang macet:

1. Paksa menghentikan instance

   Gunakan konsol Amazon EC2 atau AWS CLI untuk menghentikan instans secara paksa. Untuk langkah-langkahnya, lihatPaksa menghentikan sebuah instance.

   Instance pertama-tama akan mencoba shutdown yang anggun, yang mencakup pembilasan cache sistem file dan metadata (meskipun Anda dapat secara opsional melewati shutdown yang anggun). Jika shutdown yang anggun gagal diselesaikan dalam periode batas waktu, instance dimatikan secara paksa tanpa membilas cache dan metadata sistem file.

2. Jika force terminate gagal

   Jika, setelah beberapa jam, instance belum dihentikan dan tampaknya macet berhenti, lakukan hal berikut:

   a. Posting permintaan bantuan di AWS re:Post. Untuk membantu mempercepat resolusi, sertakan ID instans, dan jelaskan langkah-langkah yang telah Anda ambil.

   b. Atau, jika Anda memiliki paket dukungan, buat kasus dukungan teknis dalam Pusat Dukungan.

Paksa menghentikan sebuah instance

Jika tampaknya instance Anda macet terminating, Anda dapat memaksa instance Anda untuk dihentikan. Jika, setelah beberapa jam, instance belum dihentikan, kirimkan permintaan bantuan ke AWS re:post. Untuk membantu mempercepat resolusi, sertakan ID instans dan jelaskan langkah-langkah yang telah Anda ambil. Atau, jika Anda memiliki paket dukungan, buat kasus dukungan teknis dalam Pusat Dukungan.

Console

Untuk memaksa menghentikan sebuah instance

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, kemudian pilih instans yang macet.
3. Pilih status Instance, Force terminate instance.

   Perhatikan bahwa instance Force terminate hanya tersedia di konsol jika instance Anda dalam `stopping` status. Jika instance Anda berada dalam status lain (kecuali `shutting-down` dan`terminated`), Anda dapat menggunakan AWS CLI untuk memaksa menghentikan instance Anda.
4. (Opsional) Untuk melewati shutdown OS yang anggun selama force terminate, pilih kotak centang Lewati OS shutdown.
5. Pilih Force terminate.

AWS CLI

Untuk memaksa menghentikan sebuah instance

Gunakan perintah terminate-instance dengan opsi. `--force`

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --force
```

Untuk melewati shutdown OS yang anggun selama force terminate, sertakan opsi. `--skip-os-shutdown`

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
```

```
    --force \
    --skip-os-shutdown
```

PowerShell

Untuk memaksa menghentikan sebuah instance

Gunakan Remove-EC2Instancecmdlet dan atur `-Enforce` ke. `true`

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true
```

Untuk melewati shutdown OS yang anggun selama force terminate, sertakan. `-SkipOsShutdown $true`

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true `
    -SkipOsShutdown $true
```

Instans yang dihentikan masih ditampilkan

Setelah Anda menghentikan suatu instans, instans tersebut akan tetap terlihat selama beberapa saat sebelum dihapus. Statusnya menunjukkan `terminated`. Jika entri tersebut tidak dihapus setelah beberapa jam, hubungi Dukungan.

Kesalahan: Instans mungkin tidak dihentikan. Memodifikasi atribut instance disableApiTermination "

Jika Anda mencoba menghentikan instans dan mendapatkan pesan kesalahan `The instance i-1234567890abcdef0 may not be terminated. Modify its 'disableApiTermination' instance attribute`, pesan ini menunjukkan bahwa instans telah diaktifkan untuk perlindungan penghentian. Perlindungan penghentian mencegah instans dihentikan secara tidak sengaja.

Anda harus menonaktifkan perlindungan penghentian sebelum Anda dapat menghentikan instans.

Untuk informasi selengkapnya, lihat Ubah perlindungan penghentian instance.

Instans diluncurkan atau dihentikan secara otomatis

Secara umum, perilaku berikut ini berarti Anda telah menggunakan Amazon EC2 Auto Scaling, Armada EC2, atau Armada Spot untuk menskalakan sumber daya komputasi Anda secara otomatis berdasarkan kriteria yang telah ditentukan:

- Anda menghentikan sebuah instans dan sebuah instans baru diluncurkan secara otomatis.
- Anda meluncurkan sebuah instans dan salah satu instans Anda dihentikan secara otomatis.
- Anda menghentikan sebuah instans dan instans tersebut akan terhenti, lalu instans baru akan diluncurkan secara otomatis.

Untuk menghentikan penskalaan otomatis, cari grup Auto Scaling atau armada yang meluncurkan instans dan atur kapasitasnya ke 0 atau hapus.

Memecahkan masalah instans Amazon EC2 yang tidak terjangkau

Informasi berikut dapat membantu Anda memecahkan masalah instans Amazon EC2 yang tidak terjangkau. Anda dapat menangkap tangkapan layar atau mengakses keluaran konsol untuk membantu mendiagnosis masalah dan menentukan apakah Anda harus me-reboot instance Anda. Untuk instance Windows yang tidak terjangkau, pecahkan masalah dengan meninjau tangkapan layar yang dikembalikan oleh layanan.

Daftar Isi

- Boot ulang instans
- Output konsol instans
- Mengambil tangkapan layar instans yang tidak dapat dijangkau
- Tangkapan layar umum untuk memecahkan masalah instance Windows yang tidak dapat dijangkau
- Pemulihan instans saat komputer host gagal
- Instance muncul offline dan secara tak terduga di-boot ulang

Boot ulang instans

Kemampuan untuk boot ulang instans yang tidak dapat dijangkau sangat berguna untuk pemecahan masalah dan manajemen instans umum.

Sama seperti Anda dapat mengatur ulang komputer dengan menekan tombol reset, Anda dapat mengatur ulang instans EC2 menggunakan konsol Amazon EC2, CLI, atau API. Untuk informasi selengkapnya, lihat Nyalakan ulang EC2 instans Amazon Anda.

Output konsol instans

Output konsol adalah alat yang berguna untuk mendiagnosis masalah. Alat ini sangat berguna untuk memecahkan masalah kernel dan masalah konfigurasi layanan yang dapat menyebabkan sebuah instans diakhiri atau tidak dapat dijangkau sebelum daemon SSH-nya dapat dimulai.

- Instance Linux — Output konsol instance menampilkan output konsol yang tepat yang biasanya ditampilkan pada monitor fisik yang terpasang ke komputer. Output konsol menampilkan informasi singkat yang di-posting segera setelah status transisi instans (mulai, hentikan, mulai ulang, dan akhiri). Output yang di-posting tidak terus-menerus diperbarui; hanya jika kemungkinan besar nilainya paling tinggi.
- Instans Windows — Output konsol instance mencakup tiga kesalahan log peristiwa sistem terakhir.

Hanya pemilik instans yang dapat mengakses output konsol.

Anda dapat mengambil output konsol serial terbaru selama siklus hidup instance. Opsi ini hanya didukung pada instance berbasis Nitro.

Console

Untuk mendapatkan output konsol

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans.
3. Pilih instans.
4. Pilih Tindakan, Memantau dan memecahkan masalah, Dapatkan sistem log.

AWS CLI

Untuk mendapatkan output konsol

Gunakan perintah get-console-output.

```
aws ec2 get-console-output --instance-id i-1234567890abcdef0
```

PowerShell

Untuk mendapatkan output konsol

Gunakan Get-EC2ConsoleOutputcmdlet.

```
Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0
```

Mengambil tangkapan layar instans yang tidak dapat dijangkau

Jika Anda tidak dapat terhubung ke instans Anda, Anda dapat mengambil tangkapan layar dari instans Anda dan melihatnya sebagai gambar. Gambar tersebut dapat memberikan visibilitas tentang status instans, dan memungkinkan pemecahan masalah yang lebih cepat.

Anda dapat menghasilkan tangkapan layar saat instans sedang berjalan atau setelah mengalami crash. Gambar dihasilkan dalam format JPG dan tidak lebih besar dari 100 kb. Tidak ada biaya transfer data untuk tangkapan layar ini.

Batasan

Fitur ini tidak didukung untuk hal-hal berikut:

- Instans bare metal (instans tipe `*.metal`)
- Instans menggunakan driver NVIDIA GRID
- Instans yang didukung oleh prosesor Graviton berbasis ARM
- Instance Windows aktif AWS Outposts
- Instans Windows di AWS Local Zones

Dukungan wilayah

Fitur ini tidak tersedia di Wilayah berikut:

- Asia Pasifik (Thailand)
- Meksiko (Tengah)
- GovCloud Daerah

Console

Untuk mendapatkan tangkapan layar suatu instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi kiri, pilih Instans.
3. Pilih instans yang akan diambil gambarnya.
4. Pilih Tindakan, Pantau dan atasi masalah, Dapatkan tangkapan layar instans.
5. Pilih Unduh, atau klik kanan gambar untuk mengunduh dan menyimpannya.

AWS CLI

Untuk mengambil tangkapan layar suatu instans

Gunakan perintah get-console-screenshot. Output-nya dikodekan base64.

```
aws ec2 get-console-screenshot --instance-id i-1234567890abcdef0
```

PowerShell

Untuk mengambil tangkapan layar suatu instans

Gunakan Get-EC2ConsoleScreenshotcmdlet. Output-nya dikodekan base64.

```
Get-EC2ConsoleScreenshot -InstanceId i-1234567890abcdef0
```

Tangkapan layar umum untuk memecahkan masalah instance Windows yang tidak dapat dijangkau

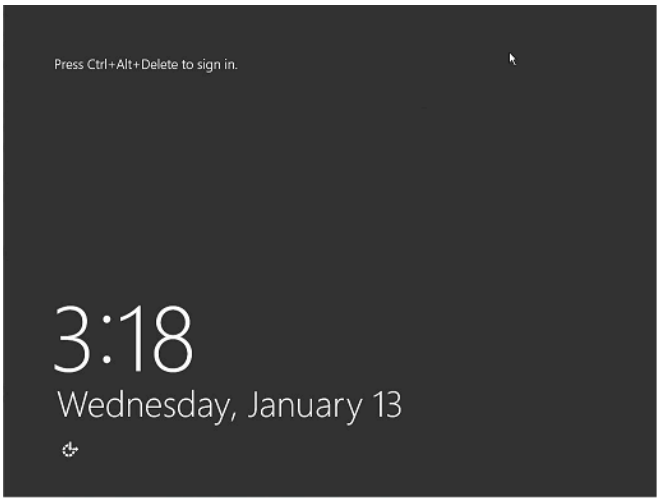
Anda dapat menggunakan informasi berikut untuk membantu memecahkan masalah instans yang tidak terjangkau berdasarkan tangkapan layar yang dikembalikan oleh layanan.

- Layar masuk (Ctrl + Alt + Delete)
- Layar konsol pemulihan
- Layar Windows boot manager
- Layar Sysprep

- Layar persiapan
- Layar Pembaruan Windows
- Chkdsk

Layar masuk (Ctrl + Alt + Delete)

Layanan Tangkapan Layar Konsol mengembalikan hal-hal berikut ini.



Jika sebuah instans tidak dapat dijangkau selama proses masuk, mungkin ada masalah dengan konfigurasi jaringan Anda atau Remote Desktop Services Windows. Instans juga bisa menjadi tidak responsif jika suatu proses menggunakan CPU dalam jumlah besar.

Konfigurasi jaringan

Gunakan informasi berikut untuk memverifikasi bahwa konfigurasi jaringan Anda AWS, Microsoft Windows, dan lokal (atau lokal) tidak memblokir akses ke instans.

AWS konfigurasi jaringan

Konfigurasi	Verifikasi
Konfigurasi grup keamanan	Verifikasi bahwa port 3389 terbuka untuk grup keamanan Anda. Verifikasi bahwa Anda terhubung ke alamat IP publik yang benar. Jika instans tidak terkait dengan IP Elastic, IP publik

Konfigurasi	Verifikasi
	berubah setelah instans berhenti/dimulai. Untuk informasi selengkapnya, lihat Desktop Jarak Jauh tidak dapat terhubung ke komputer jarak jauh.
Konfigurasi VPC (Jaringan) ACLs	Verifikasi bahwa daftar kontrol akses (ACL) untuk Amazon VPC Anda tidak memblokir akses. Untuk informasi lebih lanjut, lihat dan subnet ACLs di Panduan Pengguna Amazon VPC.
Konfigurasi VPN	Jika Anda menghubungkan ke VPC menggunakan jaringan privat virtual (VPN), verifikasi konektivitas tunnel VPN. Untuk informasi selengkapnya, lihat Memecahkan Masalah AWS Client VPN: Masalah konektivitas terowongan ke VPC.

Konfigurasi jaringan Windows

Konfigurasi	Verifikasi
Windows Firewall	Verifikasi bahwa Windows Firewall tidak memblokir koneksi ke instans Anda. Nonaktifkan Windows Firewall seperti yang dijelaskan pada poin 7 di bagian pemecahan masalah Desktop Jarak Jauh, Desktop Jarak Jauh tidak dapat terhubung ke komputer jarak jauh.
TCP/IP Konfigurasi lanjutan (Penggunaan IP statis)	Instans mungkin menjadi tidak responsif karena Anda mengonfigurasi alamat IP statis. Untuk VPC, buat antarmuka jaringan dan lampirkan ke instans.

Konfigurasi Jaringan Lokal atau on-premise

Verifikasi bahwa konfigurasi jaringan lokal tidak memblokir akses. Coba hubungkan ke instans lain di VPC yang sama dengan instans tak terjangkau milik Anda. Jika Anda tidak dapat mengakses instans lain, bekerja sama dengan administrator jaringan lokal Anda untuk mencari tahu apakah kebijakan lokal membatasi akses.

Masalah Remote Desktop Services

Jika instans tidak dapat dijangkau selama proses masuk, mungkin ada masalah dengan Remote Desktop Services (RDS) pada instans.

> **Tip**
>
> Anda dapat menggunakan runbook `AWSSupport-TroubleshootRDP` untuk memeriksa dan mengubah berbagai pengaturan yang mungkin memengaruhi koneksi Remote Desktop Protocol (RDP). Untuk informasi selengkapnya, lihat `AWSSupport-TroubleshootRDP` di referensi buku runbook Otomatisasi AWS Systems Manager .

Konfigurasi Remote Desktop Services

Konfigurasi	Verifikasi
RDS sedang berjalan	Verifikasi bahwa RDS sedang berjalan di instans. Hubungkan ke instans menggunakan snap-in Layanan Microsoft Managemen t Console (MMC) (`services.msc`). Dalam daftar layanan, verifikasi bahwa Remote Desktop Services sedang Berjalan. Jika tidak, mulai dan atur tipe startup ke Otomatis. Jika Anda tidak dapat terhubung ke instans dengan menggunakan snap-in Layanan, lepaskan volume root dari instans, ambil snapshot volume atau buat AMI darinya, lampirkan volume asli ke instans lain di Zona Ketersediaan yang sama sebagai volume sekunder, dan ubah kunci registri Mulai. Setelah Anda selesai, lampirkan kembali volume root ke instans asli.
RDS diaktifkan	Bahkan jika layanan dimulai, RDS mungkin dinonaktifkan. Lepaskan volume root dari instans, ambil snapshot volume atau buat AMI darinya, lampirkan volume asli ke instans lain di Zona Ketersediaan yang sama sebagai volume sekunder, dan aktifkan layanan dengan mengubah kunci registri Server

Konfigurasi	Verifikasi
	Terminal seperti yang dijelaskan dalam Aktifkan Desktop Jarak Jauh pada instans EC2 dengan registri jarak jauh. Setelah Anda selesai, lampirkan kembali volume root ke instans asli.

Penggunaan CPU yang tinggi

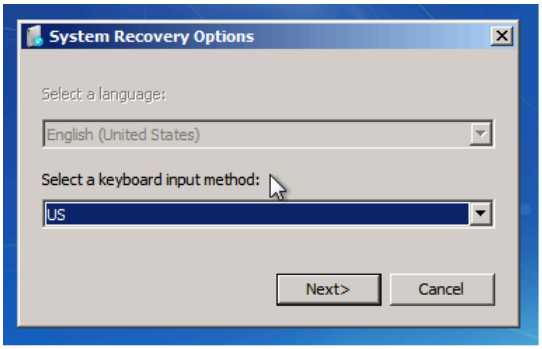
Periksa metrik CPUUtilization (Maksimum) pada instans Anda dengan menggunakan Amazon CloudWatch. Jika CPUUtilization (Maksimum) adalah angka tinggi, tunggu CPU turun dan coba sambungkan lagi. Penggunaan CPU yang tinggi dapat disebabkan oleh:

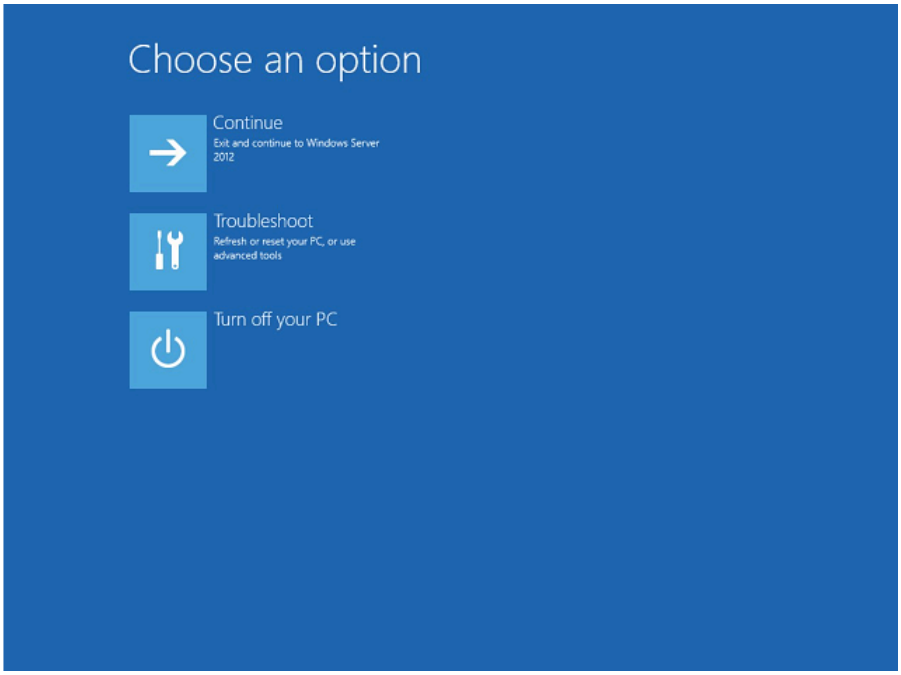
- Pembaruan Windows
- Pemindaian Perangkat Lunak Keamanan
- Skrip Startup Kustom
- Penjadwal Tugas

Untuk informasi selengkapnya, lihat Mendapatkan Statistik untuk Sumber Daya Tertentu di Panduan CloudWatch Pengguna Amazon. Untuk kiat-kiat pemecahan masalah tambahan, lihat Penggunaan CPU yang tinggi segera setelah Windows dimulai (hanya instance Windows).

Layar konsol pemulihan

Layanan Tangkapan Layar Konsol mengembalikan hal-hal berikut ini.





Sistem operasi mungkin melakukan boot ke konsol Pemulihan dan terjebak di status ini jika `bootstatuspolicy` tidak diatur ke `ignoreallfailures`. Gunakan prosedur berikut untuk mengubah konfigurasi `bootstatuspolicy` ke `ignoreallfailures`.

Secara default, konfigurasi kebijakan untuk Windows publik yang AMIs disediakan oleh AWS disetel `keignoreallfailures`.

1. Hentikan instans tak terjangkau.
2. Buat snapshot dari volume root. Volume root dilampirkan ke instans sebagai `/dev/sda1`.

   Lepaskan volume root dari instans tak terjangkau, ambil snapshot volume atau buat AMI darinya, dan lampirkan ke instans lain di Zona Ketersediaan yang sama dengan volume sekunder.

   > **Warning**
   >
   > Jika instans sementara dan asli Anda diluncurkan menggunakan AMI yang sama, Anda harus menyelesaikan langkah-langkah tambahan atau Anda tidak akan dapat melakukan boot instans asli setelah memulihkan volume root-nya karena tabrakan tanda tangan disk. Jika Anda harus membuat instans sementara menggunakan AMI yang sama, untuk menghindari tabrakan tanda tangan disk, selesaikan langkah-langkah di Tabrakan tanda tangan disk.

Atau, pilih AMI yang berbeda untuk instans sementara. Misalnya, jika instance asli menggunakan AMI untuk Windows Server 2016, luncurkan instance sementara menggunakan AMI untuk Windows Server 2019.

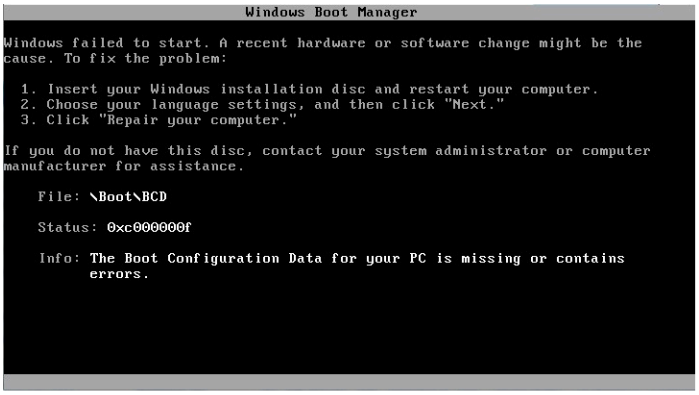
3. Masuk ke instans dan jalankan perintah berikut dari prompt perintah untuk mengubah konfigurasi `bootstatuspolicy` ke `ignoreallfailures`.

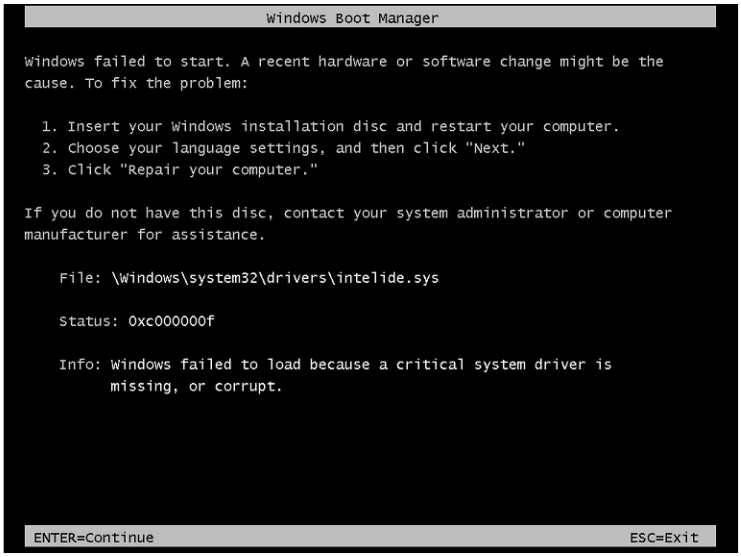
```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
 ignoreallfailures
```

4. Lampirkan kembali volume ke instans tak terjangkau dan mulai instans lagi.

Layar Windows boot manager

Layanan Tangkapan Layar Konsol mengembalikan hal-hal berikut ini.

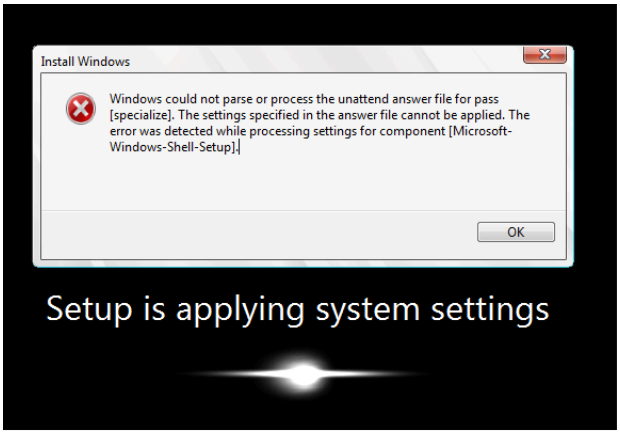


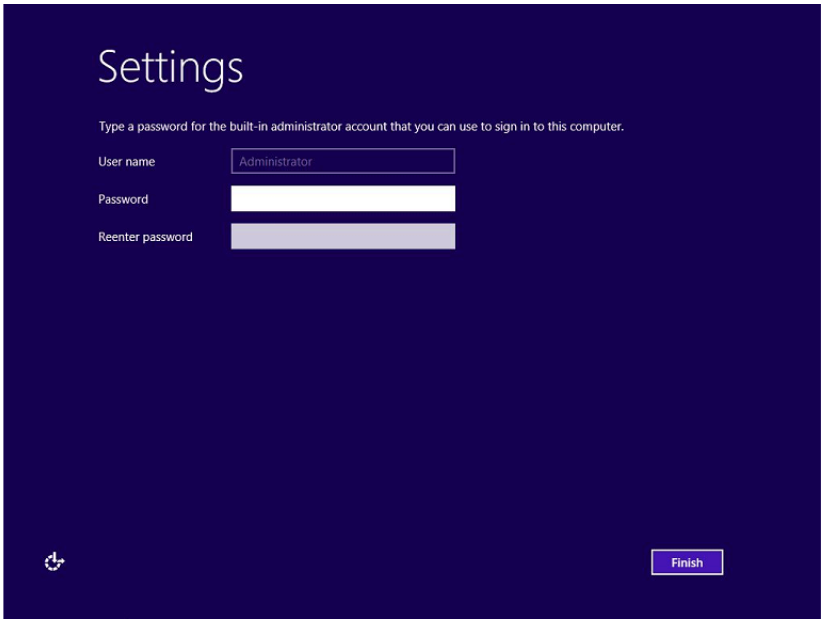


Sistem operasi mengalami korupsi fatal dalam file and/or sistem registri. Saat instans terjebak dalam status ini, Anda harus memulihkan instans dari AMI cadangan terbaru atau meluncurkan instans pengganti. Jika Anda perlu mengakses data pada instans, lepaskan volume root apa pun dari instans tak terjangkau, ambil snapshot dari volume tersebut atau buat AMI darinya, dan lampirkan ke instans lain di Zona Ketersediaan yang sama dengan volume sekunder.

Layar Sysprep

Layanan Tangkapan Layar Konsol mengembalikan hal-hal berikut ini.

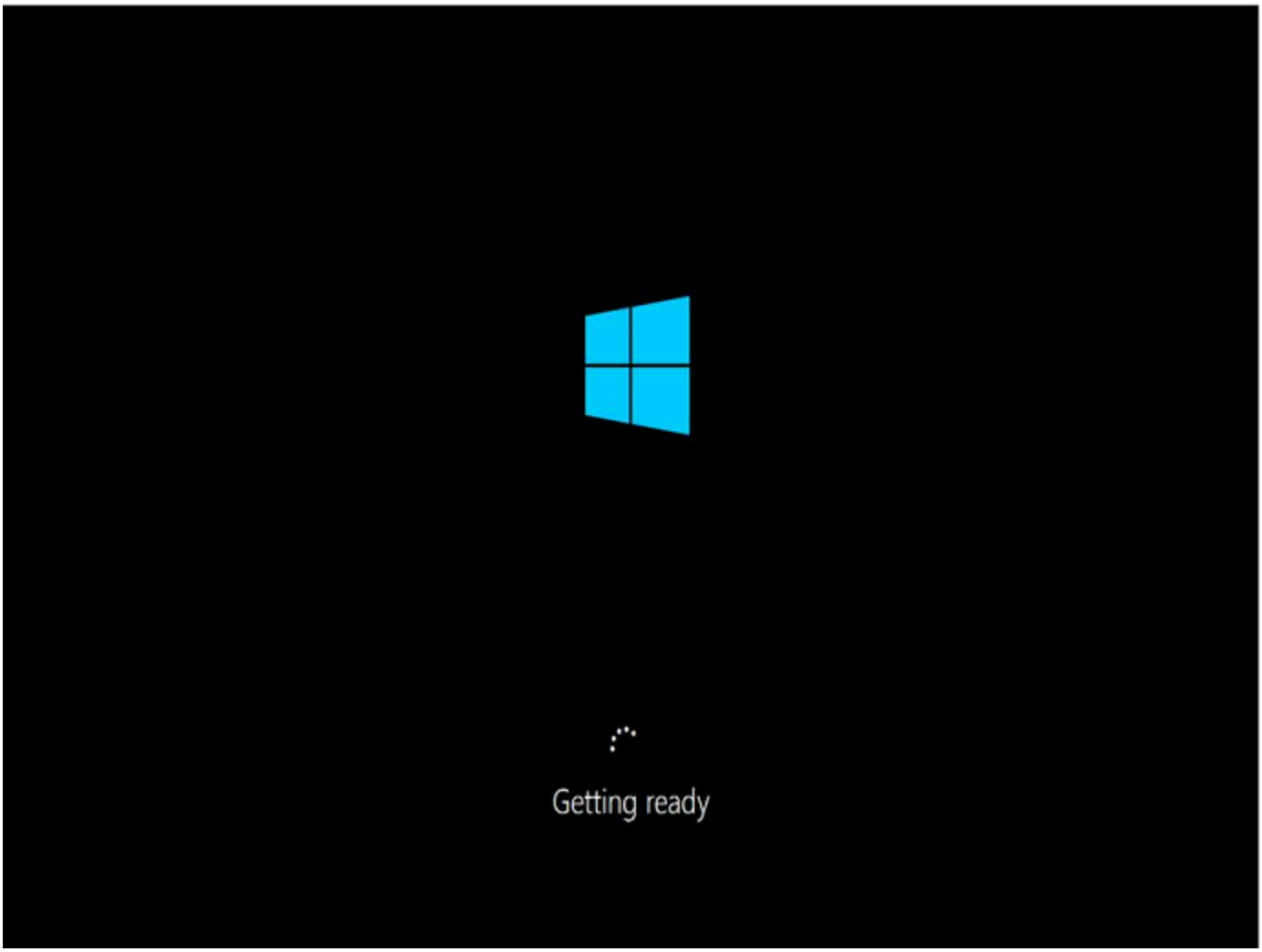




Anda mungkin melihat layar ini jika Anda tidak menggunakan Layanan EC2 Config untuk memanggil Sysprep atau jika sistem operasi gagal saat menjalankan Sysprep. Anda dapat mengatur ulang kata sandi menggunakan EC2Rescue. Jika tidak, lihat Buat Amazon EC2 AMI menggunakan Windows Sysprep.

Layar persiapan

Layanan Tangkapan Layar Konsol mengembalikan hal-hal berikut ini.



Segarkan Layanan Tangkapan Layar Konsol Instans berulang kali untuk memverifikasi bahwa ring progres sedang berputar. Jika ring berputar, tunggu sistem operasi untuk memulai. Anda juga dapat memeriksa metrik CPUUtilization (Maksimum) pada instans Anda dengan menggunakan Amazon CloudWatch untuk melihat apakah sistem operasi aktif. Jika ring progres tidak berputar, instans akan terjebak saat proses boot. Boot ulang instans. Jika melakukan boot ulang tidak menyelesaikan masalah, pulihkan instans dari AMI cadangan terbaru atau luncurkan instans pengganti. Jika Anda perlu mengakses data pada instans, lepaskan volume root dari instans tak terjangkau, ambil snapshot volume atau buat AMI darinya. Kemudian, lampirkan ke instans lain di Zona Ketersediaan yang sama dengan volume sekunder.

Layar Pembaruan Windows

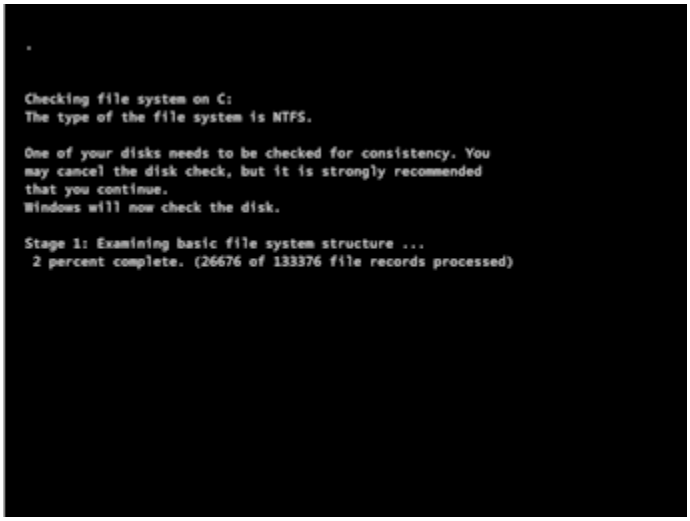
Layanan Tangkapan Layar Konsol mengembalikan hal-hal berikut ini.

Proses Pembaruan Windows sedang memperbarui registri. Tunggu hingga pembaruan selesai. Jangan lakukan boot ulang atau penghentian instans karena ini dapat menyebabkan kerusakan data selama pembaruan.

> **Note**
>
> Proses Pembaruan Windows dapat menghabiskan sumber daya di server selama pembaruan. Jika Anda sering mengalami masalah ini, pertimbangkan untuk menggunakan tipe instans yang lebih cepat dan volume EBS yang lebih cepat.

Chkdsk

Layanan Tangkapan Layar Konsol mengembalikan hal-hal berikut ini.



Windows menjalankan alat sistem chkdsk pada drive untuk memverifikasi integritas sistem file dan memperbaiki kesalahan sistem file logis. Tunggu hingga prosesnya selesai.

Pemulihan instans saat komputer host gagal

Jika terdapat masalah yang tidak dapat dipulihkan dengan perangkat keras komputer host yang mendasarinya, AWS dapat menjadwalkan peristiwa penghentian instans. Anda akan terlebih dahulu diberi tahu tentang peristiwa tersebut melalui email.

Untuk memulihkan instans yang didukung Amazon EBS yang berjalan di komputer host yang gagal

1. Cadangkan semua data penting pada volume penyimpanan instans Anda ke Amazon EBS atau Amazon S3.
2. Hentikan instans.
3. Mulai instans.
4. Pulihkan setiap data penting.

Untuk informasi selengkapnya, lihat Hentikan dan mulai instans Amazon EC2.

Untuk memulihkan instance dengan volume root penyimpanan instance yang berjalan di komputer host yang gagal

1. Buat AMI dari instans.
2. Unggah gambar ke Amazon S3.
3. Cadangkan data penting ke Amazon EBS atau Amazon S3.
4. Akhiri instans.
5. Luncurkan instans baru dari AMI.
6. Pulihkan setiap data penting ke instans baru.

Instance muncul offline dan secara tak terduga di-boot ulang

Jika instans Anda tampaknya telah offline dan kemudian di-boot ulang secara tak terduga, itu mungkin telah mengalami pemulihan instans otomatis. Ini terjadi ketika AWS mendeteksi bahwa instance tidak tersedia karena masalah perangkat keras atau perangkat lunak yang mendasarinya, dan pemulihan otomatis yang disederhanakan atau pemulihan berbasis CloudWatch tindakan diaktifkan pada instance.

Selama proses pemulihan, AWS upaya mengembalikan ketersediaan instans dengan memigrasikannya ke perangkat keras yang berbeda. Untuk memverifikasi apakah pemulihan instans otomatis terjadi untuk instans Anda, lihatVerifikasi apakah pemulihan instans otomatis terjadi.

> **Note**
>
> Jika beban kerja atau aplikasi Anda tidak responsif, periksa apakah itu berjalan pada instance. Jika tidak, mulailah secara manual. Untuk mencegah masalah ini di masa mendatang, terapkan rencana pemulihan untuk memastikan beban kerja atau aplikasi Anda berfungsi dengan benar setelah pemulihan instance.

Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Linux Anda

Informasi berikut dan kesalahan umum dapat membantu Anda memecahkan masalah saat terhubung ke instans Linux Anda.

Masalah koneksi

- Penyebab umum masalah koneksi
- Kesalahan saat menghubungkan instans Anda: Waktu koneksi habis
- Kesalahan: tidak dapat memuat kunci ... Mengharapkan: KUNCI PRIVAT APA PUN
- Kesalahan: Kunci pengguna tidak dikenali oleh server
- Kesalahan: Izin ditolak atau koneksi ditutup oleh [instans] port 22
- Kesalahan: File kunci privat yang tidak dilindungi
- Kesalahan: Kunci privat harus dimulai dengan “-----BEGIN RSA PRIVATE KEY-----” dan diakhiri dengan “-----END RSA PRIVATE KEY-----”
- Kesalahan: Verifikasi kunci host gagal
- Kesalahan: Server menolak kunci kami atau Tidak tersedia metode autentikasi yang didukung
- Tidak dapat melakukan ping pada instans
- Kesalahan: Server menutup koneksi jaringan secara tidak terduga
- Kesalahan: Validasi kunci host gagal untuk EC2 Instance Connect
- Tidak dapat terhubung ke instans Ubuntu menggunakan EC2 Instance Connect

- Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance saya?

Penyebab umum masalah koneksi

Sebaiknya Anda mulai memecahkan masalah koneksi instans dengan memverifikasi bahwa Anda telah melakukan tugas-tugas berikut secara akurat.

Verifikasi nama pengguna untuk instans Anda

Anda dapat terhubung ke instans menggunakan nama pengguna untuk akun pengguna Anda atau nama pengguna default untuk AMI yang Anda gunakan untuk meluncurkan instans Anda.

- Dapatkan nama pengguna untuk akun pengguna Anda.

  Untuk informasi selengkapnya tentang cara membuat akun pengguna, lihat Kelola pengguna sistem di instans Amazon EC2 Linux Anda.
- Dapatkan nama pengguna default untuk AMI yang Anda gunakan untuk meluncurkan instans Anda.

AMI digunakan untuk meluncurkan instans	Nama pengguna default
Amazon Linux	`ec2-user`
CentOS	`centos` atau `ec2-user`
Debian	`admin`
Fedora	`fedora` atau `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` atau `root`
SEGAR	`ec2-user` atau `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`

AMI digunakan untuk meluncurkan instans	Nama pengguna default
Linux Rocky	`rocky`
Lainnya	Periksa dengan penyedia AMI

Verifikasi bahwa aturan grup keamanan mengizinkan lalu lintas

Pastikan grup keamanan yang terkait dengan instans Anda mengizinkan lalu lintas SSH masuk dari alamat IP Anda. Grup keamanan default untuk VPC tidak mengizinkan lalu lintas SSH masuk secara default. Grup keamanan yang dibuat oleh wizard peluncuran instans mengaktifkan lalu lintas SSH secara default. Untuk langkah-langkah guna menambahkan aturan lalu lintas SSH masuk ke instans Linux Anda, lihat. Aturan-aturan untuk terhubung ke instans dari komputer Anda Untuk langkah-langkah verifikasi, lihat Kesalahan saat menghubungkan instans Anda: Waktu koneksi habis.

Verifikasi bahwa instans Anda sudah siap

Setelah Anda meluncurkan sebuah instance, dibutuhkan beberapa menit agar instans siap menerima permintaan koneksi. Periksa instans Anda untuk memastikan ia berfungsi dan telah melewati pemeriksaan status.

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Instans, kemudian pilih instans Anda.
3. Verifikasi hal berikut:

    a. Di kolom Status instans, verifikasi bahwa instans Anda berada dalam status `running`.
    b. Di kolom Pemeriksaan status, verifikasi bahwa instans Anda telah melewati semua pemeriksaan status.

Verifikasi bahwa Anda telah memenuhi semua prasyarat untuk terhubung

Pastikan Anda memiliki semua informasi yang Anda butuhkan untuk terhubung. Untuk informasi selengkapnya, lihat Hubungkan ke instans Linux Anda, menggunakan SSH..

Connect dari Linux atau macOS X

Jika sistem operasi komputer lokal Anda adalah Linux atau macOS X, periksa prasyarat spesifik berikut untuk menghubungkan ke instance Linux:

- Klien SSH

- EC2 Instance Connect
- AWS Systems Manager Manajer Sesi

Hubungkan dari Windows

Jika sistem operasi komputer lokal Anda adalah Windows, periksa prasyarat khusus berikut untuk menghubungkan ke instance Linux:

- OpenSSH
- PuTTY
- AWS Systems Manager Manajer Sesi
- Subsistem Windows untuk Linux

Periksa apakah instance tersebut adalah instance terkelola

Koneksi yang diprakarsai pengguna ke instans terkelola tidak diizinkan. Untuk menentukan apakah instance dikelola, cari bidang Managed untuk instance. Jika nilainya benar, itu adalah instance terkelola. Untuk informasi selengkapnya, lihat Instans terkelola Amazon EC2.

Kesalahan saat menghubungkan instans Anda: Waktu koneksi habis

Jika Anda mencoba terhubung ke instans Anda dan mendapatkan pesan kesalahan `Network error: Connection timed out` atau`Error connecting to [instance], reason: -> Connection timed out: connect`, coba yang berikut ini:

Periksa aturan grup keamanan Anda.

Anda memerlukan aturan grup keamanan yang memungkinkan lalu lintas masuk dari IPv4 alamat publik komputer lokal Anda di port yang tepat.

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Instans, kemudian pilih instans Anda.
3. Pada tab Keamanan di bagian bawah halaman konsol, di bawah Aturan Masuk, periksa daftar aturan yang memengaruhi instans terpilih. Verifikasi bahwa ada aturan yang memungkinkan lalu lintas dari komputer lokal Anda ke port 22 (SSH).

   Jika grup keamanan Anda tidak memiliki aturan yang mengizinkan lalu lintas masuk dari komputer lokal Anda, tambahkan aturan ke grup keamanan Anda. Untuk informasi selengkapnya, lihat Aturan-aturan untuk terhubung ke instans dari komputer Anda.

4. Untuk aturan yang memungkinkan lalu lintas masuk, periksa bidang Sumber. Jika nilainya adalah alamat IP tunggal, dan jika alamat IP tidak statis, alamat IP baru akan ditetapkan setiap kali Anda memulai ulang komputer Anda. Ini akan mengakibatkan aturan tidak menyertakan lalu lintas alamat IP komputer Anda. Alamat IP mungkin tidak statis jika komputer Anda berada di jaringan perusahaan, atau Anda terhubung melalui penyedia layanan internet (ISP), atau alamat IP komputer Anda dinamis dan berubah setiap kali Anda memulai ulang komputer Anda. Untuk memastikan bahwa aturan grup keamanan Anda mengizinkan lalu lintas masuk dari komputer lokal Anda, alih-alih menentukan satu alamat IP untuk Sumber, lebih baik tentukan rentang alamat IP yang digunakan oleh komputer klien Anda.

   Untuk informasi selengkapnya tentang aturan grup keamanan, lihat Aturan grup keamanan di Panduan Pengguna Amazon VPC.

Periksa tabel rute untuk subnet.

Anda memerlukan rute yang mengirimkan semua lalu lintas yang ditujukan di luar VPC ke gateway internet untuk VPC.

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Instans, kemudian pilih instans Anda.
3. Pada tab Jaringan, catat nilai untuk ID VPC dan ID subnet.
4. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
5. Di panel navigasi, pilih Gateway Internet. Verifikasi bahwa ada gateway internet yang dilampirkan ke VPC Anda. Jika tidak ada, pilih Buat gateway internet, masukkan nama untuk gateway internet, dan pilih Buat gateway internet. Kemudian, untuk gateway internet yang Anda buat, pilih Tindakan, Lampirkan ke VPC, pilih VPC Anda, lalu pilih Lampirkan gateway internet untuk melampirkannya ke VPC anda.
6. Di panel navigasi, pilih Subnet, lalu pilih subnet Anda.
7. Di tab Tabel Rute, verifikasi bahwa ada rute dengan `0.0.0.0/0` sebagai tujuan dan gateway internet untuk VPC Anda sebagai target. Jika Anda terhubung ke instans menggunakan IPv6 alamatnya, verifikasi bahwa ada rute untuk semua IPv6 lalu lintas (`::/0`) yang mengarah ke gateway internet. Jika tidak, lakukan tindakan berikut:

   a. Pilih ID tabel rute (rtb-xxxxxxxx) untuk menavigasi ke tabel rute.

b. Di tab Rute, pilih Edit rute. Pilih Tambahkan rute, gunakan `0.0.0.0/0` sebagai tujuan, dan gateway internet sebagai target. Untuk IPv6, pilih Tambahkan rute, gunakan `::/0` sebagai tujuan dan gateway internet sebagai target.

c. Pilih Simpan rute.

Periksa jaringan daftar kontrol akses (ACL) untuk subnet.

Jaringan ACLs harus mengizinkan lalu lintas SSH masuk dari alamat IP lokal Anda pada port 22. Hal ini juga mengizinkan lalu lintas keluar ke port sementara (1024-65535).

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih Pengguna.
3. Pilih subnet Anda.
4. Pada tab ACL Jaringan, untuk Aturan masuk, verifikasi bahwa aturan mengizinkan lalu lintas masuk dari komputer Anda di port yang diperlukan. Jika tidak, hapus atau ubah aturan yang memblokir lalu lintas.
5. Untuk Aturan keluar, verifikasi bahwa aturan mengizinkan lalu lintas keluar ke komputer Anda pada port sementara. Jika tidak, hapus atau ubah aturan yang memblokir lalu lintas.

Jika komputer Anda berada di jaringan perusahaan

Tanyakan administrator jaringan Anda apakah firewall internal memungkinkan lalu lintas masuk dan keluar dari komputer Anda pada port 22.

Jika Anda memiliki firewall di komputer Anda, verifikasi bahwa itu memungkinkan lalu lintas masuk dan keluar dari komputer Anda pada port 22.

Periksa apakah instans Anda memiliki IPv4 alamat publik.

Jika tidak, Anda dapat mengaitkan alamat IP Elastis dengan instans Anda. Untuk informasi selengkapnya, lihat Alamat Elastic IP.

Periksa beban CPU pada instans Anda; server mungkin kelebihan beban.

AWS secara otomatis menyediakan data seperti CloudWatch metrik Amazon dan status instans, yang dapat Anda gunakan untuk melihat berapa banyak beban CPU pada instans Anda dan, jika perlu, menyesuaikan cara penanganan beban Anda. Untuk informasi selengkapnya, lihat Pantau instans Anda menggunakan CloudWatch.

- Jika beban Anda bervariasi, Anda dapat menaikkan atau menurunkan skala secara otomatis menggunakan Auto Scaling dan Elastic Load Balancing.
- Jika beban terus bertambah, Anda dapat beralih ke tipe instans yang lebih besar. Untuk informasi selengkapnya, lihat Perubahan jenis instans Amazon EC2.

Untuk terhubung ke instans Anda menggunakan IPv6 alamat, periksa hal berikut:

- Subnet Anda harus dikaitkan dengan tabel rute yang memiliki rute untuk IPv6 traffic (`::/0`) ke gateway internet.
- Aturan grup keamanan Anda harus mengizinkan lalu lintas masuk dari IPv6 alamat lokal Anda di port 22.
- Aturan ACL jaringan Anda harus mengizinkan lalu lintas masuk dan keluar IPv6 .
- Jika Anda meluncurkan instans dari AMI yang lebih lama, instans tersebut mungkin tidak dikonfigurasi untuk DHCPv6 (IPv6 alamat tidak dikenali secara otomatis di antarmuka jaringan). Untuk informasi selengkapnya, lihat Mengonfigurasi instans Anda IPv6 di Panduan Pengguna Amazon VPC.
- Komputer lokal Anda harus memiliki IPv6 alamat, dan harus dikonfigurasi untuk digunakan IPv6.

Kesalahan: tidak dapat memuat kunci ... Mengharapkan: KUNCI PRIVAT APA PUN

Jika Anda mencoba untuk terhubung ke instans Anda dan mendapatkan pesan kesalahan, `unable to load key ... Expecting: ANY PRIVATE KEY`, file tempat kunci privat disimpan tidak dikonfigurasi dengan benar. Jika file kunci privat berakhir dengan `.pem`, ia mungkin masih dikonfigurasi dengan salah. Kemungkinan penyebab file kunci privat yang tidak dikonfigurasi dengan benar adalah sertifikat yang hilang.

Jika file kunci privat tidak dikonfigurasi dengan benar, ikuti langkah-langkah berikut ini untuk mengatasi kesalahan

1. Buat pasangan kunci baru. Untuk informasi selengkapnya, lihat Membuat pasangan kunci menggunakan Amazon EC2.

> **Note**
>
> Sebagai gantinya, Anda dapat membuat pasangan kunci baru menggunakan alat pihak ketiga. Untuk informasi selengkapnya, lihat Membuat pasangan kunci menggunakan alat pihak ketiga dan mengimpor kunci publik ke Amazon EC2.

2. Tambahkan pasangan kunci baru ke instans Anda. Untuk informasi selengkapnya, lihat Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance saya?.
3. Hubungkan ke instans Anda menggunakan pasangan kunci baru.

Kesalahan: Kunci pengguna tidak dikenali oleh server

Jika Anda menggunakan SSH untuk terhubung ke instans Anda

- Gunakan `ssh -vvv` untuk mendapatkan informasi debug tiga kali lipat saat menghubungkan:

```
ssh -vvv -i path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Output contoh berikut menunjukkan hal-hal yang mungkin Anda lihat jika mencoba untuk terhubung ke instans menggunakan kunci yang tidak dikenali oleh server:

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
```

```
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Jika Anda menggunakan PuTTY untuk terhubung ke instans Anda

- Verifikasi bahwa file kunci privat (.pem) Anda telah diubah dengan sesuai ke format yang dikenali oleh PuTTY (.ppk). Untuk informasi selengkapnya tentang cara mengubah kunci privat, lihat Connect ke instans Linux Anda menggunakan Putty.

  > **Note**
  >
  > Di PuTTYgen, muat file kunci pribadi Anda dan pilih Simpan Kunci Pribadi daripada Menghasilkan.

- Verifikasi bahwa Anda terhubung dengan nama pengguna yang sesuai untuk AMI Anda. Masukkan nama pengguna di kotak nama Host di jendela Konfigurasi PuTTY.

AMI digunakan untuk meluncurkan instans	Nama pengguna default
Amazon Linux	`ec2-user`
CentOS	`centos` atau `ec2-user`
Debian	`admin`
Fedora	`fedora` atau `ec2-user`
FreeBSD	`ec2-user`

AMI digunakan untuk meluncurkan instans	Nama pengguna default
RHEL	`ec2-user` atau `root`
SEGAR	`ec2-user` atau `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Linux Rocky	`rocky`
Lainnya	Periksa dengan penyedia AMI

- Verifikasi bahwa Anda memiliki aturan grup keamanan masuk untuk mengizinkan lalu lintas masuk ke port yang sesuai. Untuk informasi selengkapnya, lihat Aturan-aturan untuk terhubung ke instans dari komputer Anda.

Kesalahan: Izin ditolak atau koneksi ditutup oleh [instans] port 22

Jika Anda terhubung ke instans Anda menggunakan SSH dan mendapatkan salah satu kesalahan berikut,,`Host key not found in [directory]`,, `Permission denied (publickey)Authentication failed, permission denied`, atau`Connection closed by [instance] port 22`, verifikasi bahwa Anda terhubung dengan nama pengguna yang sesuai untuk AMI Anda dan bahwa Anda telah menentukan kunci pribadi yang tepat (`.pem`)file untuk instans Anda.

Nama pengguna yang sesuai adalah sebagai berikut:

AMI digunakan untuk meluncurkan instans	Nama pengguna default
Amazon Linux	`ec2-user`
CentOS	`centos` atau `ec2-user`
Debian	`admin`
Fedora	`fedora` atau `ec2-user`

AMI digunakan untuk meluncurkan instans	Nama pengguna default
FreeBSD	`ec2-user`
RHEL	`ec2-user` atau `root`
SEGAR	`ec2-user` atau `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Linux Rocky	`rocky`
Lainnya	Periksa dengan penyedia AMI

Misalnya, untuk menggunakan klien SSH agar terhubung ke instans Amazon Linux, gunakan perintah berikut:

```
ssh -i /path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Konfirmasi bahwa Anda menggunakan file kunci privat yang sesuai dengan pasangan kunci, yang Anda pilih saat meluncurkan instans.

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Instans, lalu pilih instans Anda.
3. Pada tab Detail, di bawah Detail instans, verifikasi nilai Nama pasangan kunci.
4. Jika Anda tidak menentukan pasangan kunci saat meluncurkan instans, Anda dapat mengakhiri instans dan meluncurkan instans baru, untuk memastikan bahwa Anda telah menentukan pasangan kunci. Jika ini adalah instans yang Anda gunakan tetapi Anda tidak lagi memiliki file `.pem` untuk pasangan kunci, Anda bisa mengganti pasangan kunci dengan yang baru. Untuk informasi selengkapnya, lihat Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance saya?.

Jika Anda membuat pasangan kunci sendiri, pastikan bahwa pembuat kunci Anda diatur untuk membuat kunci RSA. Kunci DSA tidak diterima.

Jika Anda mendapatkan kesalahan `Permission denied (publickey)` dan tidak ada satu pun di atas yang berlaku (misalnya, Anda dapat terhubung sebelumnya), izin pada direktori beranda instans Anda mungkin telah diubah. Izin untuk /home/*instance-user-name*/.ssh/authorized_keys harus dibatasi untuk pemilik saja.

Untuk memverifikasi izin pada instans Anda

1. Hentikan instans Anda dan lepaskan volume root. Untuk informasi selengkapnya, lihat Hentikan dan mulai instans Amazon EC2.
2. Luncurkan instans sementara di Zona Ketersediaan yang sama dengan instans Anda saat ini (gunakan AMI yang serupa atau sama dengan yang digunakan untuk instans Anda saat ini), dan lampirkan volume root ke instans sementara.
3. Hubungkan ke instans sementara, buat titik pemasangan, dan pasang volume yang Anda lampirkan.
4. Dari instans sementara, periksa izin direktori /home/*instance-user-name*/ dari volume yang dilampirkan. Jika perlu, sesuaikan izin sebagai berikut:

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Copot volume, lepas dari instans sementara, dan lampirkan kembali ke instans asli. Pastikan Anda menentukan nama perangkat yang benar untuk volume root; misalnya, /dev/xvda.
6. Mulai instans Anda. Jika Anda tidak lagi membutuhkan instans sementara, Anda dapat mengakhirinya.

Kesalahan: File kunci privat yang tidak dilindungi

File kunci privat Anda harus dilindungi dari operasi baca dan tulis dari pengguna lain. Jika kunci privat Anda dapat dibaca atau ditulis oleh siapa pun kecuali Anda, SSH akan mengabaikan kunci Anda dan Anda akan melihat pesan peringatan berikut di bawah ini.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Jika Anda melihat pesan serupa saat mencoba masuk ke instans, periksa baris pertama pesan kesalahan untuk memverifikasi bahwa Anda menggunakan kunci publik yang benar untuk instans Anda. Contoh di atas menggunakan kunci privat `.ssh/my_private_key.pem` dengan izin file `0777`, yang memungkinkan siapa pun untuk membaca atau menulis file ini. Tingkat izin ini sangat tidak aman, sehingga SSH mengabaikan kunci ini.

Jika Anda terhubung dari macOS atau Linux, jalankan perintah berikut untuk memperbaiki kesalahan ini, ganti jalur untuk file kunci privat Anda.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Jika Anda terhubung ke instance Linux dari Windows, lakukan langkah-langkah berikut di komputer lokal Anda.

1. Navigasikan ke file .pem Anda.
2. Klik kanan pada file .pem dan pilih Properti.
3. Pilih tab Keamanan.
4. Pilih Lanjutan.
5. Verifikasi bahwa Anda adalah pemilik file. Jika tidak, ubah pemilik ke nama pengguna Anda.
6. Pilih Nonaktifkan warisan dan Hapus semua izin yang diwariskan dari objek ini.
7. Pilih Tambahkan, Pilih pengguna utama, masukkan nama pengguna, lalu pilih OKE.
8. Dari jendela Entri izin, berikan izin Baca dan pilih OKE.
9. Klik Terapkan untuk memastikan semua pengaturan disimpan.
10. Pilih OKE untuk menutup jendela Pengaturan Keamanan Lanjutan.
11. Pilih OKE untuk menutup jendela Properti.
12. Anda harus dapat terhubung ke instance Linux Anda dari Windows menggunakan SSH.

Dari prompt perintah Windows, jalankan perintah berikut.

1. Dari perintah prompt, navigasikan ke jalur lokasi file .pem Anda.
2. Jalankan perintah berikut untuk mengatur ulang dan menghapus izin eksplisit:

```
icacls.exe $path /reset
```

3. Jalankan perintah berikut untuk memberikan izin Baca kepada pengguna saat ini:

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. Jalankan perintah berikut untuk menonaktifkan warisan dan menghapus izin yang diwariskan.

```
icacls.exe $path /inheritance:r
```

5. Anda harus dapat terhubung ke instance Linux Anda dari Windows menggunakan SSH.

Kesalahan: Kunci privat harus dimulai dengan “-----BEGIN RSA PRIVATE KEY-----” dan diakhiri dengan “-----END RSA PRIVATE KEY-----”

Jika Anda menggunakan alat pihak ke tiga, seperti ssh-keygen, untuk membuat pasangan kunci RSA, alat ini menghasilkan kunci privat dalam format kunci OpenSSH. Saat Anda terhubung dengan instans, jika Anda menggunakan kunci privat dalam format OpenSSH untuk mendekripsi kata sandi, Anda akan menerima kesalahan `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Untuk mengatasi kesalahan tersebut, kunci privat harus dalam format PEM. Gunakan perintah berikut untuk membuat kunci privat dalam format PEM:

```
ssh-keygen -m PEM
```

Kesalahan: Verifikasi kunci host gagal

Kesalahan ini terjadi jika ada ketidakcocokan antara kunci host yang disimpan pada instance dalam `known_hosts` file dan pada klien. Misalnya, ketidakcocokan dapat terjadi jika Anda terhubung ke sebuah instance menggunakan satu alamat IP publik, dan kemudian mencoba menghubungkannya lagi menggunakan alamat IP publik yang berbeda. Hal ini dapat terjadi setelah Anda menambahkan atau menghapus alamat IP Elastis, karena hal itu mengubah alamat IP publik dari sebuah instans.

Untuk mengatasi kesalahan ini, mulailah dengan mengonfirmasi bahwa ada perubahan yang diharapkan pada kunci host atau konfigurasi jaringan instance. Sebelum Anda terhubung ke instans, Anda mungkin juga ingin memverifikasi sidik jari host. Setelah Anda terhubung ke instance, Anda dapat menghapus kunci host lama dari `known_hosts` file. Untuk instruksi, lihat dokumentasi untuk distribusi Linux yang digunakan pada instans Anda.

Kesalahan: Server menolak kunci kami atau Tidak tersedia metode autentikasi yang didukung

Jika Anda menggunakan PuTTY untuk terhubung ke instans Anda dan mendapatkan salah satu dari kesalahan berikut, Kesalahan: Server menolak kunci kami atau Kesalahan: Tidak ada metode otentikasi yang didukung, verifikasi bahwa Anda terhubung dengan nama pengguna yang sesuai untuk AMI Anda. Ketik nama pengguna di Nama pengguna di jendela Konfigurasi PuTTY.

Nama pengguna yang sesuai adalah sebagai berikut:

AMI digunakan untuk meluncurkan instans	Nama pengguna default
Amazon Linux	`ec2-user`
CentOS	`centos` atau `ec2-user`
Debian	`admin`
Fedora	`fedora` atau `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` atau `root`
SEGAR	`ec2-user` atau `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Linux Rocky	`rocky`

AMI digunakan untuk meluncurkan instans	Nama pengguna default
Lainnya	Periksa dengan penyedia AMI

Anda juga harus memverifikasi bahwa:

- Anda menggunakan PuTTY versi terbaru. Untuk informasi selengkapnya, lihat halaman web PuTTY.
- File kunci privat (.pem) Anda telah diubah dengan sesuai ke format yang dikenali oleh PuTTY (.ppk). Untuk informasi selengkapnya tentang cara mengubah kunci privat, lihat Connect ke instans Linux Anda menggunakan Putty.

Tidak dapat melakukan ping pada instans

Perintah `ping` adalah tipe lalu lintas ICMP — jika Anda tidak dapat melakukan ping pada instans Anda, pastikan bahwa aturan grup keamanan masuk Anda mengizinkan lalu lintas ICMP untuk pesan `Echo Request` dari semua sumber, atau dari komputer atau instans yang mengeluarkan perintah.

Jika Anda tidak dapat mengeluarkan perintah `ping` dari instans, pastikan bahwa aturan grup keamanan keluar Anda mengizinkan lalu lintas ICMP untuk pesan `Echo Request` ke semua tujuan, atau ke host yang Anda coba ping.

Perintah `Ping` juga dapat diblokir oleh firewall atau waktunya habis karena masalah latensi jaringan atau perangkat keras. Anda harus berkonsultasi dengan jaringan lokal atau administrator sistem untuk bantuan pemecahan masalah lebih lanjut.

Kesalahan: Server menutup koneksi jaringan secara tidak terduga

Jika Anda terhubung ke instans dengan PuTTY dan Anda menerima pesan kesalahan “Server menutup koneksi jaringan secara tidak terduga”, verifikasi bahwa Anda telah mengaktifkan keepalive di halaman Koneksi Konfigurasi PuTTY agar koneksi tidak terputus. Beberapa server memutus koneksi klien saat tidak menerima data apa pun dalam periode waktu tertentu. Atur Detik untuk keepalive menjadi 59 detik.

Jika Anda masih mengalami masalah setelah mengaktifkan keepalive, coba nonaktifkan algoritma Nagle di halaman Koneksi Konfigurasi PuTTY.

Kesalahan: Validasi kunci host gagal untuk EC2 Instance Connect

Jika Anda memutar kunci host instance Anda, kunci host baru tidak secara otomatis diunggah ke database kunci host AWS tepercaya. Hal ini menyebabkan validasi kunci host gagal ketika Anda mencoba untuk terhubung ke instans menggunakan klien berbasis peramban EC2 Instance Connect, dan Anda tidak dapat terhubung ke instans Anda.

Untuk mengatasi kesalahan, Anda harus menjalankan skrip `eic_harvest_hostkeys` pada instans Anda, yang mengunggah kunci host baru Anda ke EC2 Instance Connect. Skrip ini terletak di `/opt/aws/bin/` di instans Amazon Linux 2, dan di `/usr/share/ec2-instance-connect/` pada instans Ubuntu.

Amazon Linux 2

Untuk mengatasi kesalahan kegagalan validasi kunci host pada instans Amazon Linux 2

1. Hubungkan ke instans Anda menggunakan SSH.

   Anda dapat terhubung dengan menggunakan EC2 Instance Connect CLI atau dengan menggunakan key pair SSH yang ditetapkan ke instans Anda saat Anda meluncurkannya dan nama pengguna default AMI yang Anda gunakan untuk meluncurkan instans Anda. Untuk Amazon Linux 2, nama pengguna defaultnya adalah`ec2-user`.

   Misalnya, jika instans Anda diluncurkan menggunakan Amazon Linux 2, nama DNS publik instans Anda adalah `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, dan pasangan kuncinya adalah `my_ec2_private_key.pem`, gunakan perintah berikut untuk SSH ke dalam instans Anda:

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Untuk informasi selengkapnya tentang menghubungkan ke instans Anda, lihat Hubungkan ke instans Linux Anda menggunakan klien SSH.

2. Arahkan ke folder berikut.

   ```
   [ec2-user ~]$ cd /opt/aws/bin/
   ```

3. Jalankan perintah berikut di instans Anda.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Perhatikan bahwa panggilan yang berhasil tidak menghasilkan output.

Anda sekarang dapat menggunakan klien berbasis peramban EC2 Instance Connect untuk terhubung ke instans Anda.

Ubuntu

Untuk mengatasi kesalahan kegagalan validasi kunci host pada instans Ubuntu

1. Hubungkan ke instans Anda menggunakan SSH.

   Anda dapat terhubung dengan menggunakan EC2 Instance Connect CLI atau dengan menggunakan key pair SSH yang ditetapkan ke instans Anda saat Anda meluncurkannya dan nama pengguna default AMI yang Anda gunakan untuk meluncurkan instans Anda. Untuk Ubuntu, nama pengguna default adalah`ubuntu`.

   Misalnya, jika instans Anda diluncurkan menggunakan Ubuntu, nama DNS publik instans Anda adalah `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, dan pasangan kuncinya adalah `my_ec2_private_key.pem`, gunakan perintah berikut untuk SSH ke dalam instans Anda:

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Untuk informasi selengkapnya tentang menghubungkan ke instans Anda, lihat Hubungkan ke instans Linux Anda menggunakan klien SSH.

2. Arahkan ke folder berikut.

   ```
   [ec2-user ~]$ cd /usr/share/ec2-instance-connect/
   ```

3. Jalankan perintah berikut di instans Anda.

   ```
   [ec2-user ~]$ ./eic_harvest_hostkeys
   ```

   Perhatikan bahwa panggilan yang berhasil tidak menghasilkan output.

Anda sekarang dapat menggunakan klien berbasis peramban EC2 Instance Connect untuk terhubung ke instans Anda.

Tidak dapat terhubung ke instans Ubuntu menggunakan EC2 Instance Connect

Jika Anda menggunakan EC2 Instance Connect untuk terhubung ke instans Ubuntu Anda dan mendapatkan kesalahan saat mencoba menghubungkan, Anda dapat menggunakan informasi berikut untuk mencoba memperbaiki masalah.

Kemungkinan penyebab

Paket `ec2-instance-connect` pada instans ini bukanlah versi terbaru.

Solusi

Perbarui paket `ec2-instance-connect` pada instans ke versi terbaru, sebagai berikut:

1. Hubungkan ke instans Anda menggunakan metode selain EC2 Instance Connect.
2. Jalankan perintah berikut pada instans Anda untuk memperbarui paket `ec2-instance-connect` ke versi terbaru.

```
apt update && apt upgrade
```

Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance saya?

Jika Anda kehilangan kunci privat untuk instans yang didukung EBS, Anda dapat memperoleh kembali akses ke instans Anda. Anda harus menghentikan instans, mencopot volume root, dan melampirkannya ke instans lain sebagai volume data, ubah file `authorized_keys` dengan kunci publik baru, memindahkan volume kembali ke instans asli, lalu memulai ulang instans. Untuk informasi tentang peluncuran, penghubungan ke, dan penghentian instans selengkapnya, lihat Perubahan status EC2 instans Amazon.

Prosedur ini hanya didukung untuk instans dengan volume root EBS. Jika instance memiliki volume root penyimpanan instance, Anda tidak dapat menggunakan prosedur ini untuk mendapatkan kembali

akses ke instance Anda; Anda harus memiliki kunci pribadi untuk terhubung ke instance. Untuk menentukan jenis volume root instance Anda, buka konsol Amazon EC2, pilih Instans, pilih instance, pilih tab Penyimpanan, dan di bagian Detail perangkat Root, periksa nilai jenis perangkat Root.

Nilainya antara `EBS` atau.`INSTANCE-STORE`

Selain langkah-langkah berikut, ada cara lain untuk terhubung ke instans Linux Anda jika kehilangan kunci privat Anda. Untuk informasi selengkapnya, lihat Bagaimana cara saya terhubung ke instans Amazon EC2 jika saya kehilangan pasangan kunci SSH setelah peluncuran awal?

Langkah-langkah untuk terhubung ke instans yang didukung EBS dengan pasangan kunci yang berbeda

- Langkah 1: Buat pasangan kunci baru
- Langkah 2: Dapatkan informasi tentang instans asli dan volume root-nya
- Langkah 3: Hentikan instans asli
- Langkah 4: Luncurkan instans sementara
- Langkah 5: Copot volume root dari instans asli dan lampirkan ke instans sementara
- Langkah 6: Tambahkan kunci publik baru ke authorized_keys pada volume asli yang dipasang ke instans sementara
- Langkah 7: Lepaskan dan copot volume asli dari instans sementara, lalu lampirkan kembali ke instans asli
- Langkah 8: Hubungkan ke instans asli menggunakan pasangan kunci baru
- Langkah 9: Bersihkan

Langkah 1: Buat pasangan kunci baru

Buat pasangan kunci baru menggunakan konsol Amazon EC2 atau alat pihak ketiga. Jika Anda ingin nama dari pasangan kunci baru Anda sama persis dengan kunci privat yang hilang, Anda harus menghapus pasangan kunci yang sudah ada terlebih dahulu. Untuk informasi tentang pembuatan pasangan kunci selengkapnya, lihat Membuat pasangan kunci menggunakan Amazon EC2 or Membuat pasangan kunci menggunakan alat pihak ketiga dan mengimpor kunci publik ke Amazon EC2.

Langkah 2: Dapatkan informasi tentang instans asli dan volume root-nya

Catat informasi berikut karena Anda akan membutuhkannya untuk menyelesaikan prosedur ini.

Untuk mendapatkan informasi tentang instans asli Anda

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pilih Instans dalam panel navigasi, lalu pilih instans yang ingin Anda hubungkan. (Kami akan merujuknya sebagai instans asli.)
3. Pada tab Detail, catat ID instans dan ID AMI.
4. Pada tab Jaringan, catat Zona Ketersediaan.
5. Pada tab Penyimpanan, di bawah Nama perangkat root, catat nama perangkat untuk volume root (misalnya, `/dev/xvda`). Lalu, di bawah Perangkat blok, temukan nama perangkat ini dan catat ID volume (misalnya, vol-0a1234b5678c910de).

Langkah 3: Hentikan instans asli

Pilih Status instans, Hentikan instans. Jika opsi ini dinonaktifkan, instance sudah dihentikan atau volume rootnya adalah volume penyimpanan instance.

> **Warning**
>
> Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instance hilang. Untuk menyimpan data ini, buat cadangan ke penyimpanan persisten.

Langkah 4: Luncurkan instans sementara

Untuk meluncurkan instans sementara

1. Di panel navigasi, pilih Instans, lalu pilih Luncurkan instans.
2. Di bagian Nama dan tanda, untuk Nama, masukkan Sementara.
3. Di bagian Gambar Aplikasi dan OS, pilih AMI yang sama dengan yang Anda gunakan untuk meluncurkan instans asli. Jika AMI ini tidak tersedia, Anda dapat membuat AMI yang dapat digunakan dari instans yang dihentikan. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.
4. Di bagian Tipe instans, pertahankan tipe instance default.
5. Di bagian Pasangan kunci, untuk Nama pasangan kunci, pilih pasangan kunci yang ada untuk digunakan atau buat yang baru.

6. Di bagian Pengaturan jaringan, pilih Edit, lalu untuk Subnet, pilih subnet di Zona Ketersediaan yang sama dengan instans asli.
7. Di panel Ringkasan, pilih Luncurkan.

Langkah 5: Copot volume root dari instans asli dan lampirkan ke instans sementara

1. Di panel navigasi, pilih Volume dan pilih volume root untuk instance asli (Anda mencatat ID volumenya di langkah sebelumnya). Pilih Tindakan, Copot volume, lalu pilih Lepaskan. Tunggu status volume menjadi `available`. (Anda mungkin harus memilih ikon Segarkan.)
2. Dengan volume yang masih dipilih, pilih Tindakan, lalu pilih Lampirkan volume. Pilih ID instans dari instans sementara, catat nama perangkat yang ditentukan di bawah Nama perangkat (misalnya, `/dev/sdf`), lalu pilih Lampirkan volume.

> **Note**
>
> Jika Anda meluncurkan instans asli dari AWS Marketplace AMI dan volume berisi AWS Marketplace kode, Anda harus terlebih dahulu menghentikan instans sementara sebelum Anda dapat melampirkan volume.

Langkah 6: Tambahkan kunci publik baru ke **`authorized_keys`** pada volume asli yang dipasang ke instans sementara

1. Luncurkan ke instans sementara.
2. Dari instans sementara, pasang volume yang Anda lampirkan ke instans sehingga Anda dapat mengakses sistem file-nya. Misalnya, jika nama perangkat adalah `/dev/sdf`, gunakan perintah berikut untuk memasang volume sebagai `/mnt/tempvol`.

> **Note**
>
> Nama perangkat mungkin akan dimunculkan secara berbeda pada instans Anda. Misalnya, perangkat yang dipasang sebagai `/dev/sdf` dapat muncul sebagai `/dev/xvdf` pada instans. Beberapa versi Red Hat (atau variannya, seperti CentOS) bahkan dapat menambah huruf tambahan sebanyak 4 karakter, di mana `/dev/sdf` menjadi `/dev/xvdk`.

a. Gunakan perintah lsblk untuk menentukan apakah volume sudah dipartisi atau belum.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
##xvda1 202:1    0    8G  0 part /
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

Di contoh sebelumnya, `/dev/xvda` dan `/dev/xvdf` adalah volume yang sudah dipartisi, dan `/dev/xvdg` yang belum. Jika volume Anda dipartisi, Anda dapat memasang partisi tersebut (`/dev/xvdf1`) alih-alih perangkat mentah (`/dev/xvdf`) pada langkah berikutnya.

b. Buat direktori sementara untuk memasang volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Pasang volume (atau partisi) pada titik pasang sementara, menggunakan nama volume atau nama perangkat yang Anda identifikasi sebelumnya. Perintah yang diperlukan bergantung pada sistem file sistem operasi Anda. Perhatikan bahwa nama perangkat mungkin akan dimunculkan secara berbeda pada instans Anda. Lihat note di Langkah 6 untuk informasi selengkapnya.

- Amazon Linux, Ubuntu, dan Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12, dan RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Jika Anda mendapatkan kesalahan yang menyatakan bahwa sistem file rusak, jalankan perintah berikut untuk menggunakan utilitas fsck guna memeriksa sistem file dan memperbaiki masalah:

```
[ec2-user ~]$ sudo fsck /dev/xvdf1
```

3. Dari instans sementara, gunakan perintah berikut untuk memperbarui `authorized_keys` pada volume yang dipasang dengan kunci publik baru dari `authorized_keys` untuk instans sementara.

> **Important**
>
> Contoh berikut menggunakan nama pengguna Amazon Linux`ec2-user`. Anda mungkin perlu mengganti nama pengguna yang berbeda, seperti `ubuntu` untuk instance Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Jika penyalinan ini berhasil, Anda dapat melanjutkan ke langkah berikutnya.

(Opsional) Kecuali, jika Anda tidak memiliki izin untuk mengedit file di `/mnt/tempvol`, Anda harus memperbarui file menggunakan sudo, lalu memeriksa izin pada file untuk memverifikasi bahwa Anda dapat masuk ke instans asli. Gunakan perintah berikut untuk memeriksa izin pada file.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

Dalam contoh output ini, *222* adalah ID pengguna dan *500* ID grup. Berikutnya, gunakan sudo untuk menjalankan kembali perintah penyalinan yang gagal.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Jalankan lagi akun perintah berikut untuk menentukan apakah izin sudah berubah atau belum.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Jika ID pengguna dan ID grup telah berubah, gunakan perintah berikut untuk memulihkannya.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Langkah 7: Lepaskan dan copot volume asli dari instans sementara, lalu lampirkan kembali ke instans asli

1. Dari instans sementara, lepas volume yang Anda lampirkan ke instans sehingga Anda dapat melampirkannya kembali ke instans asli. Misalnya, gunakan perintah berikut untuk melepaskan volume pada `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Lepaskan volume dari instans sementara (Anda melepasnya pada langkah sebelumnya): Dari konsol Amazon EC2, pilih Volume di panel navigasi, pilih volume root untuk instance asli (Anda mencatat ID volume pada langkah sebelumnya), pilih Tindakan, Lepaskan volume, lalu pilih Lepaskan. Tunggu status volume menjadi `available`. (Anda mungkin harus memilih ikon Segarkan.)
3. Lampirkan kembali volume ke instans asli: Dengan volume yang masih dipilih, pilih Tindakan, Lampirkan Volume. Pilih ID instans dari instance asli, tentukan nama perangkat yang Anda catat sebelumnya di Langkah 2 untuk lampiran volume root asli (`/dev/sda1`atau`/dev/xvda`), lalu pilih Lampirkan volume.

   > **Important**
   >
   > Jika Anda tidak menentukan nama perangkat yang sama dengan lampiran asli, Anda tidak dapat memulai instans asli. Amazon EC2 mengharapkan volume root pada atau. `sda1` `/dev/xvda`

Langkah 8: Hubungkan ke instans asli menggunakan pasangan kunci baru

Pilih instans asli, pilih Status instans, Mulai instans. Setelah instans memasuki status `running`, Anda dapat terhubung menggunakan file kunci privat untuk pasangan kunci baru Anda.

> **Note**
>
> Jika nama pasangan kunci baru Anda dan file kunci privat yang terkait berbeda dari nama pasangan kunci asli, pastikan Anda menentukan nama file kunci privat baru saat terhubung ke instans Anda.

Langkah 9: Bersihkan

(Opsional) Anda dapat mengakhiri instans sementara jika tidak menggunakannya lagi. Pilih instance sementara, dan pilih Instance state, Terminate (delete) instance.

Memecahkan masalah instans Amazon EC2 Linux dengan pemeriksaan status yang gagal

Informasi berikut dapat membantu Anda memecahkan masalah jika instance Linux Anda gagal dalam pemeriksaan status. Pertama-tama, tentukan apakah aplikasi Anda menunjukkan adanya masalah. Jika Anda memverifikasi bahwa instans tidak menjalankan aplikasi Anda seperti yang diharapkan, tinjau informasi pemeriksaan status dan log sistem.

Untuk contoh masalah yang dapat menyebabkan pemeriksaan status gagal, lihat Pemeriksaan status untuk instans Amazon EC2.

Daftar Isi

- Meninjau informasi pemeriksaan status
- Mengambil log sistem
- Memecahkan masalah kesalahan log sistem untuk instance Linux
- Kehabisan memori: hentikan proses
- KESALAHAN: mmu_update gagal (Pembaruan manajemen memori gagal)
- Kesalahan I/O (kegagalan perangkat blok)
- KESALAHAN I/O: bukan disk lokal maupun jarak jauh (Perangkat blok terdistribusi yang rusak)
- request_module: modprobe loop runaway (Melakukan loop modprobe kernel warisan pada versi Linux yang lebih lawas)
- “FATAL: kernel terlalu lawas” dan “fsck: Tidak ada file atau direktori tersebut saat mencoba membuka /dev” (Kernel dan AMI tidak cocok)

- “FATAL: Tidak dapat memuat /lib/modules" atau "BusyBox" (Modul kernel tidak ada)
- KESALAHAN Kernel tidak valid (kernel tidak kompatibel dengan EC2)
- fsck: Tidak ada file atau direktori tersebut saat mencoba membuka... (Sistem file tidak ditemukan)
- Kesalahan umum saat memasang sistem file (kegagalan pemasangan)
- VFS: Tidak dapat memasang fs root pada blok yang tidak diketahui (Sistem file root tidak cocok)
- Kesalahan: Tidak dapat menentukan major/minor jumlah perangkat root... (system/device Ketidakcocokan file root)
- XENBUS: Perangkat tanpa driver...
- ... hari tanpa diperiksa, pemeriksaan paksa (Diperlukan pemeriksaan sistem file)
- fsck mati dengan status keluar... (Perangkat tidak ada)
- Perintah GRUB (grubdom>)
- Memunculkan eth0 antarmuka: eth0 perangkat memiliki alamat MAC yang berbeda dari yang diharapkan, mengabaikan. (Alamat MAC dengan hard-coding)
- Tidak dapat memuat SELinux Kebijakan. Mesin berada dalam mode pemberlakuan. Berhenti sekarang. (SELinux salah konfigurasi)
- XENBUS: Waktu menghubungkan ke perangkat habis (waktu habis Xenbus)

Meninjau informasi pemeriksaan status

Untuk menyelidiki instans yang terganggu menggunakan konsol Amazon EC2

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Pada panel navigasi, pilih Instans, kemudian pilih instans Anda.
3. Pilih tab Status dan alarm untuk melihat hasil individual untuk semua pemeriksaan status Sistem, pemeriksaan status Instans, dan pemeriksaan status EBS Terlampir.

Jika pemeriksaan status gagal, Anda dapat mencoba salah satu opsi berikut:

- Buat alarm untuk memulihkan instance sebagai respons terhadap pemeriksaan status yang gagal. Untuk informasi selengkapnya, lihat Buat alarm yang menghentikan, mengakhiri, melakukan boot ulang, atau memulihkan instans.
- (Pemeriksaan status instans) Jika Anda mengubah jenis instans menjadi instans berbasis Nitro, pemeriksaan status gagal jika Anda bermigrasi dari instance yang tidak memiliki ENA dan NVMe

driver yang diperlukan. Untuk informasi selengkapnya, lihat Kompatibilitas untuk mengubah tipe instans.

- Untuk instance dengan volume root EBS, hentikan dan mulai ulang instance. Untuk informasi selengkapnya, lihat Hentikan dan mulai instans Amazon EC2.
- Untuk instance dengan volume root penyimpanan instance, hentikan instance dan luncurkan instance pengganti. Untuk informasi selengkapnya, lihat Mengakhiri instans Amazon EC2.
- Tunggu hingga Amazon EC2 menyelesaikan masalah.
- Hubungi Dukungan atau posting masalah Anda ke AWS re:post.
- Jika instans Anda berada dalam grup Auto Scaling:
  - (Pemeriksaan status sistem dan pemeriksaan status instans) Secara default, Amazon EC2 Auto Scaling secara otomatis meluncurkan instance pengganti. Untuk informasi selengkapnya, lihat Health memeriksa instans di grup Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling.
  - (Pemeriksaan status EBS terlampir) Anda harus mengonfigurasi Amazon EC2 Auto Scaling untuk secara otomatis meluncurkan instance pengganti. Untuk informasi selengkapnya, lihat Memantau dan mengganti instans Auto Scaling dengan volume Amazon EBS yang terganggu di Panduan Pengguna Amazon EC2 Auto Scaling.
- Mengambil log sistem dan mencari kesalahan. Untuk informasi selengkapnya, lihat Mengambil log sistem.

Mengambil log sistem

Jika pemeriksaan status instans gagal, Anda dapat melakukan boot ulang instans dan mengambil log sistem. Log tersebut mungkin memperlihatkan kesalahan yang dapat membantu Anda memecahkan masalah. Boot ulang akan menghapus informasi yang tidak diperlukan dari log.

Untuk melakukan boot ulang instans dan mengambil log sistem

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, dan pilih instans Anda.
3. Pilih Status instans, Boot ulang instans. Mungkin diperlukan waktu beberapa menit untuk melakukan boot ulang instans Anda.
4. Verifikasi bahwa masalah masih ada. Pada beberapa kasus, boot ulang dapat menyelesaikan masalah.

5. Ketika instans berada dalam status `running`, pilih Tindakan, Memantau dan memecahkan masalah, Dapatkan log sistem.
6. Tinjau log yang muncul di layar, dan gunakan daftar pernyataan kesalahan log sistem yang diketahui di bawah ini untuk memecahkan masalah Anda.
7. Jika masalah belum teratasi, Anda dapat membuat pos masalah Anda ke AWS re:Post.

Memecahkan masalah kesalahan log sistem untuk instance Linux

Untuk instance Linux yang gagal dalam pemeriksaan status instans, seperti pemeriksaan jangkauan instans, verifikasi bahwa Anda mengikuti langkah-langkah di atas untuk mengambil log sistem. Daftar berikut berisi beberapa kesalahan log sistem umum dan tindakan yang disarankan yang dapat Anda ambil guna mengatasi masalah pada setiap kesalahan.

Kesalahan Memori

- Kehabisan memori: hentikan proses
- KESALAHAN: mmu_update gagal (Pembaruan manajemen memori gagal)

Kesalahan Perangkat

- Kesalahan I/O (kegagalan perangkat blok)
- KESALAHAN I/O: bukan disk lokal maupun jarak jauh (Perangkat blok terdistribusi yang rusak)

Kesalahan Kernel

- request_module: modprobe loop runaway (Melakukan loop modprobe kernel warisan pada versi Linux yang lebih lawas)
- “FATAL: kernel terlalu lawas” dan “fsck: Tidak ada file atau direktori tersebut saat mencoba membuka /dev” (Kernel dan AMI tidak cocok)
- “FATAL: Tidak dapat memuat /lib/modules" atau "BusyBox" (Modul kernel tidak ada)
- KESALAHAN Kernel tidak valid (kernel tidak kompatibel dengan EC2)

Kesalahan Sistem File

- fsck: Tidak ada file atau direktori tersebut saat mencoba membuka... (Sistem file tidak ditemukan)

- Kesalahan umum saat memasang sistem file (kegagalan pemasangan)
- VFS: Tidak dapat memasang fs root pada blok yang tidak diketahui (Sistem file root tidak cocok)
- Kesalahan: Tidak dapat menentukan major/minor jumlah perangkat root... (system/device Ketidakcocokan file root)
- XENBUS: Perangkat tanpa driver...
- ... hari tanpa diperiksa, pemeriksaan paksa (Diperlukan pemeriksaan sistem file)
- fsck mati dengan status keluar... (Perangkat tidak ada)

Kesalahan Sistem Operasi

- Perintah GRUB (grubdom>)
- Memunculkan eth0 antarmuka: eth0 perangkat memiliki alamat MAC yang berbeda dari yang diharapkan, mengabaikan. (Alamat MAC dengan hard-coding)
- Tidak dapat memuat SELinux Kebijakan. Mesin berada dalam mode pemberlakuan. Berhenti sekarang. (SELinux salah konfigurasi)
- XENBUS: Waktu menghubungkan ke perangkat habis (waktu habis Xenbus)

Kehabisan memori: hentikan proses

out-of-memoryKesalahan ditunjukkan oleh entri log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

Potensi penyebab

Memori habis

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Lakukan salah satu dari berikut ini:

Untuk tipe instans ini	Lakukan hal berikut
	• Hentikan instans, dan modifikasi instans untuk menggunakan tipe instans yang berbeda, dan mulai lagi instans tersebut. Misalnya, tipe instans yang lebih besar atau instans memori yang dioptimalkan. • Boot ulang instans untuk mengembalikannya ke status tidak terganggu. Masalah mungkin akan terjadi lagi kecuali Anda mengubah tipe instans.
Didukung penyimpanan instans	Lakukan salah satu dari berikut ini: • Akhiri instans dan luncurkan instans baru, dengan menentukan tipe instans yang berbeda. Misalnya, tipe instans yang lebih besar atau instans memori yang dioptimal kan. • Boot ulang instans untuk mengembalikannya ke status tidak terganggu. Masalah mungkin akan terjadi lagi kecuali Anda mengubah tipe instans.

KESALAHAN: mmu_update gagal (Pembaruan manajemen memori gagal)

Kegagalan pembaruan manajemen memori diindikasikan oleh entri log sistem yang serupa dengan yang berikut ini:

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'


root (hd0)

 Filesystem type is ext2fs, using whole disk
```

```
kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Potensi penyebab

Masalah dengan Amazon Linux

Tindakan yang disarankan

Posting masalah Anda ke AWS re:posting atau kontak. Dukungan

Kesalahan I/O (kegagalan perangkat blok)

input/output Kesalahan ditunjukkan oleh entri log sistem yang mirip dengan contoh berikut:

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Potensi penyebab

Jenis instans	Potensi penyebab
Didukung Amazon EBS	Volume Amazon EBS yang gagal
Didukung penyimpanan instans	Drive fisik yang gagal

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Hentikan instans. 2. Lepaskan lampiran volume. 3. Coba pulihkan volume. **Note** Disarankan untuk sering membuat snapshot volume Amazon EBS. Hal ini secara signifikan mengurangi risiko kehilangan data sebagai akibat dari kegagalan. 4. Lampirkan kembali volume ke instans. 5. Mulai instans.
Didukung penyimpanan instans	Akhiri instans dan luncurkan instans baru. **Note** Data tidak dapat dipulihkan. Pulihkan dari cadangan.

Untuk tipe instans ini	Lakukan hal berikut
	Note Disarankan agar menggunakan Amazon S3 atau Amazon EBS untuk pencadangan. Volume penyimpanan instans secara langsung terikat dengan kegagalan host tunggal dan disk tunggal.

KESALAHAN I/O: bukan disk lokal maupun jarak jauh (Perangkat blok terdistribusi yang rusak)

input/output Kesalahan pada perangkat ditunjukkan oleh entri log sistem yang mirip dengan contoh berikut:

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Potensi penyebab

Jenis instans	Potensi penyebab
Didukung Amazon EBS	Volume Amazon EBS yang gagal
Didukung penyimpanan instans	Drive fisik yang gagal

Tindakan yang disarankan

Akhiri instans dan luncurkan instans baru.

Untuk instans yang didukung Amazon EBS, Anda dapat memulihkan data dari snapshot terbaru dengan membuat gambar darinya. Data apa pun yang ditambahkan setelah snapshot tidak dapat dipulihkan.

request_module: modprobe loop runaway (Melakukan loop modprobe kernel warisan pada versi Linux yang lebih lawas)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini. Penggunaan kernel Linux yang tidak stabil atau lawas (misalnya 2.6.16-xenU) dapat menyebabkan kondisi loop yang tidak dapat dihentikan saat dimulai.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan kernel yang lebih baru, yang berbasis GRUB ataupun statis, menggunakan salah satu opsi berikut: Opsi 1: Akhiri instans dan luncurkan instans baru, dengan menentukan parameter `-kernel` dan `-ramdisk`. Opsi 2: 1. Hentikan instans. 2. Modifikasi atribut kernel dan ramdisk untuk menggunakan kernel yang lebih baru. 3. Mulai instans.
Didukung penyimpanan instans	Akhiri instans dan luncurkan instans baru, dengan menentukan parameter `-kernel` dan `-ramdisk`.

“FATAL: kernel terlalu lawas” dan “fsck: Tidak ada file atau direktori tersebut saat mencoba membuka /dev” (Kernel dan AMI tidak cocok)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Potensi penyebab

Kernel dan userland tidak kompatibel

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Hentikan instans. 2. Modifikasi konfigurasi untuk menggunakan kernel yang lebih baru. 3. Mulai instans.
Didukung penyimpanan instans	Gunakan prosedur berikut: 1. Buat AMI yang menggunakan kernel yang lebih baru. 2. Akhiri instans. 3. Mulai instans baru dari AMI yang Anda buat.

“FATAL: Tidak dapat memuat /lib/modules" atau "BusyBox" (Modul kernel tidak ada)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
 directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
 such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Done.
Begin: Running /scripts/init-premount ...
```

```
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Potensi penyebab

Satu atau lebih kondisi berikut dapat menyebabkan masalah ini:

- Ramdisk tidak ada
- Modul yang benar dari ramdisk tidak ada
- Volume root Amazon EBS tidak dilampirkan dengan benar sebagai `/dev/sda1`

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Pilih ramdisk yang sudah benar untuk volume Amazon EBS. 2. Hentikan instans.

Untuk tipe instans ini	Lakukan hal berikut
	3. Lepaskan lampiran volume dan perbaiki. 4. Lampirkan volume ke instans. 5. Mulai instans. 6. Modifikasi AMI untuk menggunakan ramdisk yang telah diperbaiki.
Didukung penyimpanan instans	Gunakan prosedur berikut: 1. Akhiri instans dan luncurkan instans baru dengan ramdisk yang benar. 2. Buat AMI baru dengan ramdisk yang benar.

KESALAHAN Kernel tidak valid (kernel tidak kompatibel dengan EC2)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro
```

```
Error 15: File not found
```

Potensi penyebab

Salah satu atau kedua kondisi berikut dapat menyebabkan masalah ini:

- Kernel yang disediakan tidak didukung oleh GRUB
- Kernel pengganti tidak ada

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Hentikan instans. 2. Ganti dengan kernel yang berfungsi. 3. Instal kernel pengganti. 4. Modifikasi AMI dengan memperbaiki kernel.
Didukung penyimpanan instans	Gunakan prosedur berikut: 1. Akhiri instans dan luncurkan instans baru dengan kernel yang benar. 2. Buat AMI baru dengan kernel yang benar. 3. (Opsional) Carilah bantuan teknis untuk pemulihan data menggunakan Dukungan.

fsck: Tidak ada file atau direktori tersebut saat mencoba membuka... (Sistem file tidak ditemukan)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
```

```
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]

Starting udev: [  OK  ]

Setting hostname localhost:  [  OK  ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]

Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]


*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Potensi penyebab

- Terdapat bug dalam definisi sistem file ramdisk /etc/fstab
- Definisi sistem file salah konfigurasi di /etc/fstab
- Drive tidak ada/gagal

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Hentikan instance, lepaskan volume root, repair/modify /etc/fstab volume, lampirkan volume ke instance, dan mulai instance. 2. Perbaiki ramdisk untuk menyertakan /etc/fstab yang dimodifikasi (jika berlaku). 3. Modifikasi AMI untuk menggunakan ramdisk yang lebih baru. Bidang keenam di fstab menentukan persyaratan ketersediaan pemasangan –nilai bukan nol mengimplikasikan bahwa fsck akan dilakukan pada volume tersebut dan harus berhasil. Penggunaan bidang ini dapat menjadi masalah di Amazon EC2 karena kegagalan biasanya mengakibatkan perintah konsol interaktif yang saat ini tidak tersedia di Amazon EC2. Berhati-hatilah dengan fitur ini dan baca halaman manual Linux untuk fstab.
Didukung penyimpanan instans	Gunakan prosedur berikut: 1. Akhiri instans dan luncurkan instans baru. 2. Lepaskan lampiran volume Amazon EBS yang tidak sesuai dan boot ulang instans. 3. (Opsional) Carilah bantuan teknis untuk pemulihan data menggunakan Dukungan.

Kesalahan umum saat memasang sistem file (kegagalan pemasangan)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Potensi penyebab

Jenis instans	Potensi penyebab
Didukung Amazon EBS	• Volume Amazon EBS yang terlepas lampirannya atau gagal.

Jenis instans	Potensi penyebab
	• Sistem file rusak. • Kombinasi ramdisk dan AMI yang tidak cocok (seperti ramdisk Debian dengan SUSE AMI).
Didukung penyimpanan instans	• Drive yang gagal. • Sistem file yang rusak. • Ramdisk dan kombinasi yang tidak cocok (misalnya ramdisk Debian dengan SUSE AMI).

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Hentikan instans. 2. Lepaskan lampiran volume root. 3. Lampirkan volume root ke instans yang berfungsi yang diketahui. 4. Jalankan pemeriksaan sistem file (fsck -a /dev/...). 5. Perbaiki kesalahan apa pun. 6. Lepaskan lampiran volume dari instans yang berfungsi yang diketahui. 7. Lampirkan volume ke instans yang dihentikan. 8. Mulai instans. 9. Periksa ulang status instans.
Didukung penyimpanan instans	Cobalah salah satu cara berikut ini:

Untuk tipe instans ini	Lakukan hal berikut
	• Mulai instans baru. • (Opsional) Carilah bantuan teknis untuk pemulihan data menggunakan Dukungan.

VFS: Tidak dapat memasang fs root pada blok yang tidak diketahui (Sistem file root tidak cocok)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Potensi penyebab

Jenis instans	Potensi penyebab
Didukung Amazon EBS	• Perangkat tidak terlampir dengan benar. • Perangkat root tidak terpasang pada titik perangkat yang benar. • Sistem file tidak dalam format yang diharapkan. • Penggunaan kernel warisan (seperti 2.6.16-XenU). • Pembaruan kernel terbaru di instans Anda (pembaruan yang salah, atau bug pembaruan)
Didukung penyimpanan instans	Kegagalan perangkat keras.

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Lakukan salah satu dari berikut ini: • Hentikan lalu mulai ulang instans. • Ubah volume root untuk dilampirkan pada titik perangkat yang benar, mungkin/dev/sda1 instead of /dev/sda. • Hentikan dan modifikasi untuk menggunakan kernel modern. • Lihat dokumentasi untuk distribusi Linux Anda guna memeriksa bug pembaruan yang diketahui. Ubah atau instal ulang kernel.
Didukung penyimpanan instans	Akhiri instans dan luncurkan instans baru dengan kernel modern.

Kesalahan: Tidak dapat menentukan major/minor jumlah perangkat root... (system/device Ketidakcocokan file root)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
```

```
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Potensi penyebab

- Driver perangkat blok virtual tidak ada atau salah konfigurasi
- Konflik enumerasi perangkat (sda versus xvda atau sda alih-alih sda1)
- Pilihan yang salah untuk kernel instans

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Hentikan instans. 2. Lepaskan lampiran volume. 3. Perbaiki masalah pemetaan perangkat. 4. Mulai instans. 5. Modifikasi AMI untuk menangani masalah pemetaan perangkat.
Didukung penyimpanan instans	Gunakan prosedur berikut: 1. Buat AMI baru dengan perbaikan yang sesuai (petakan perangkat blok dengan benar). 2. Akhiri instans dan luncurkan instans baru dari AMI yang Anda buat.

XENBUS: Perangkat tanpa driver...

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Potensi penyebab

- Driver perangkat blok virtual tidak ada atau salah konfigurasi
- Konflik enumerasi perangkat (sda versus xvda)
- Pilihan yang salah untuk kernel instans

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Hentikan instans. 2. Lepaskan lampiran volume. 3. Perbaiki masalah pemetaan perangkat. 4. Mulai instans. 5. Modifikasi AMI untuk menangani masalah pemetaan perangkat.
Didukung penyimpanan instans	Gunakan prosedur berikut:

Untuk tipe instans ini	Lakukan hal berikut
	1. Buat AMI dengan perbaikan yang sesuai (petakan perangkat blok dengan benar). 2. Akhiri instans dan luncurkan instans baru menggunakan AMI yang telah Anda buat.

... hari tanpa diperiksa, pemeriksaan paksa (Diperlukan pemeriksaan sistem file)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Potensi penyebab

Waktu pemeriksaan sistem file telah berlalu; pemeriksaan paksa sistem file sedang dilakukan.

Tindakan yang disarankan

- Tunggu hingga pemeriksaan sistem file selesai. Pemeriksaan sistem file dapat memakan waktu yang lama bergantung pada ukuran sistem file root.
- Modifikasi sistem file Anda untuk menghapus pemberlakuan pemeriksaan sistem file (fsck) menggunakan tune2fs atau alat yang sesuai untuk sistem file Anda.

fsck mati dengan status keluar... (Perangkat tidak ada)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
```

```
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
[31mfailed (code 8).[39;49m
```

Potensi penyebab

- Ramdisk mencari drive yang tidak ada
- Pemeriksaan paksa konsistensi sistem file dilakukan
- Drive gagal atau terlepas lampirannya

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Coba salah satu atau beberapa cara berikut untuk menyelesaikan masalah: • Hentikan instans, lampirkan volume ke instans yang sudah ada yang sedang berjalan. • Jalankan pemeriksaan konsistensi secara manual. • Perbaiki ramdisk untuk menyertakan utilitas yang relevan. • Modifikasi parameter penyetelan sistem file untuk menghapus persyaratan konsistensi (tidak disarankan).
Didukung penyimpanan instans	Coba salah satu atau beberapa cara berikut untuk menyelesaikan masalah: • Buat ulang paket ramdisk dengan alat yang benar. • Modifikasi parameter penyetelan sistem file untuk menghapus persyaratan konsistensi (tidak disarankan).

Untuk tipe instans ini	Lakukan hal berikut
	• Akhiri instans dan luncurkan instans baru. • (Opsional) Carilah bantuan teknis untuk pemulihan data menggunakan Dukungan.

Perintah GRUB (grubdom>)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
    GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

       [ Minimal BASH-like line editing is supported.   For

         the   first   word,  TAB  lists  possible  command

         completions.  Anywhere else TAB lists the possible

         completions of a device/filename. ]

grubdom>
```

Potensi penyebab

Jenis instans	Potensi penyebab
Didukung Amazon EBS	• File konfigurasi GRUB tidak ada. • Citra GRUB yang digunakan salah, mengharapkan file konfigurasi GRUB berada di lokasi yang berbeda. • Sistem file yang tidak didukung digunakan untuk menyimpan file konfigurasi GRUB Anda (misalnya mengonversi sistem file root ke tipe yang tidak didukung oleh versi GRUB sebelumnya).
Didukung penyimpanan instans	• File konfigurasi GRUB tidak ada.

Jenis instans	Potensi penyebab
	• Citra GRUB yang digunakan salah, mengharapkan file konfigurasi GRUB berada di lokasi yang berbeda. • Sistem file yang tidak didukung digunakan untuk menyimpan file konfigurasi GRUB Anda (misalnya mengonversi sistem file root ke tipe yang tidak didukung oleh versi GRUB sebelumnya).

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Opsi 1: Modifikasi AMI dan luncurkan ulang instans: 1. Ubah sumber AMI untuk membuat file konfigurasi GRUB di lokasi standar (/boot/grub/menu.lst). 2. Verifikasi bahwa versi GRUB Anda mendukung tipe sistem file yang mendasarinya dan tingkatkan GRUB jika perlu. 3. Pilih citra GRUB yang sesuai, (drive hd0-1st atau hd00 – drive pertama, partisi pertama). 4. Akhiri instans dan luncurkan instans baru menggunakan AMI yang Anda buat. Opsi 2: Perbaiki instans yang sudah ada: 1. Hentikan instans. 2. Lepaskan lampiran sistem file root. 3. Lampirkan sistem file root ke instans yang berfungsi yang diketahui.

Untuk tipe instans ini	Lakukan hal berikut
	4. Pasang sistem file. 5. Buat file konfigurasi GRUB 6. Verifikasi bahwa versi GRUB Anda mendukung tipe sistem file yang mendasari nya dan tingkatkan GRUB jika perlu. 7. Lepaskan lampiran sistem file. 8. Lampirkan ke instans asli. 9. Modifikasi atribut kernel untuk menggunakan citra GRUB yang sesuai (disk pertama atau partisi pertama pada disk pertama). 10. Mulai instans.
Didukung penyimpanan instans	Opsi 1: Modifikasi AMI dan luncurkan ulang instans: 1. Buat AMI baru dengan file konfigurasi GRUB di lokasi standar (/boot/grub/menu.lst). 2. Pilih citra GRUB yang sesuai, (drive hd0-1st atau hd00 – drive pertama, partisi pertama). 3. Verifikasi bahwa versi GRUB Anda mendukung tipe sistem file yang mendasari nya dan tingkatkan GRUB jika perlu. 4. Akhiri instans dan luncurkan instans baru menggunakan AMI yang telah Anda buat. Opsi 2: Akhiri instans dan luncurkan instans baru, dengan menentukan kernel yang benar. **Note** Untuk memulihkan data dari instans yang sudah ada, hubungi Dukungan.

Memunculkan eth0 antarmuka: eth0 perangkat memiliki alamat MAC yang berbeda dari yang diharapkan, mengabaikan. (Alamat MAC dengan hard-coding)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
...
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected,
 ignoring.
[FAILED]

Starting auditd: [  OK  ]
```

Potensi penyebab

Terdapat MAC antarmuka dengan hard-coding dalam konfigurasi AMI

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Lakukan salah satu dari berikut ini: • Modifikasi AMI untuk menghapus hard-codi ng dan meluncurkan ulang instans. • Modifikasi instans untuk menghapus alamat MAC dengan hard-coding. ATAU Gunakan prosedur berikut: 1. Hentikan instans. 2. Lepaskan lampiran volume root.

Untuk tipe instans ini	Lakukan hal berikut
	3. Lampirkan volume ke instans lain dan modifikasi volume untuk menghapus alamat MAC dengan hard-coding. 4. Lampirkan volume ke instans asli. 5. Mulai instans.
Didukung penyimpanan instans	Lakukan salah satu dari berikut ini: • Modifikasi instans untuk menghapus alamat MAC dengan hard-coding. • Akhiri instans dan luncurkan instans baru.

Tidak dapat memuat SELinux Kebijakan. Mesin berada dalam mode pemberlakuan. Berhenti sekarang. (SELinux salah konfigurasi)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Potensi penyebab

SELinux telah diaktifkan karena kesalahan:

- Kernel yang disediakan tidak didukung oleh GRUB
- Kernel pengganti tidak ada

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Gunakan prosedur berikut: 1. Hentikan instans yang gagal.

Untuk tipe instans ini	Lakukan hal berikut
	2. Lepaskan lampiran volume root instans yang gagal. 3. Lampirkan volume root ke instans Linux lain yang sedang berjalan (yang nantinya akan disebut sebagai instans pemulihan). 4. Hubungkan ke instans pemulihan dan pasang volume root dari instans yang gagal. 5. Nonaktifkan SELinux pada volume root yang dipasang. Proses ini bervariasi di seluruh distribusi Linux. Untuk informasi selengkap nya, lihat dokumentasi khusus OS Anda. **Note** Pada beberapa sistem, Anda menonaktifkan SELinux dengan mengatur `SELINUX=disabled` dalam `/mount_point /etc/sysconfig/selinux` file, di mana *mount_point* lokasi yang Anda pasang volume pada instance pemulihan Anda. 6. Copot dan lepaskan lampiran volume root dari instans pemulihan dan lampirkan kembali ke instans asli. 7. Mulai instans.
Didukung penyimpanan instans	Gunakan prosedur berikut: 1. Akhiri instans dan luncurkan instans baru. 2. (Opsional) Carilah bantuan teknis untuk pemulihan data menggunakan Dukungan.

XENBUS: Waktu menghubungkan ke perangkat habis (waktu habis Xenbus)

Kondisi ini diindikasikan oleh log sistem yang mirip dengan yang ditunjukkan di bawah ini.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

Potensi penyebab

- Perangkat blok tidak terhubung ke instans
- Instans ini menggunakan kernel instans lama

Tindakan yang disarankan

Untuk tipe instans ini	Lakukan hal berikut
Didukung Amazon EBS	Lakukan salah satu dari berikut ini: • Modifikasi AMI dan instans untuk menggunakan kernel modern dan luncurkan ulang instans. • Boot ulang instans.
Didukung penyimpanan instans	Lakukan salah satu dari berikut ini: • Akhiri instans. • Modifikasi AMI untuk menggunakan kernel modern, dan luncurkan instans baru menggunakan AMI ini.

Memecahkan masalah booting instans Amazon EC2 Linux dari volume yang salah

Dalam beberapa situasi, volume selain volume yang melekat pada `/dev/xvda` atau `/dev/sda` menjadi volume root dari instance Linux. Hal ini dapat terjadi ketika Anda telah melampirkan volume root dari instans lain, atau volume yang dibuat dari snapshot volume root, ke instans dengan volume root yang sudah ada.

Hal ini disebabkan oleh cara kerja ramdisk awal di Linux. Ramdisk awal di Linux memilih volume yang ditentukan sebagai `/` dalam `/etc/fstab`, dan pada beberapa distribusi, ini ditentukan oleh label yang terlampir ke partisi volume. Secara khusus, Anda menemukan bahwa `/etc/fstab` akan terlihat seperti berikut ini:

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Jika Anda memeriksa label kedua volume tersebut, Anda akan melihat bahwa keduanya berisi label `/`:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

Dalam contoh ini, Anda bisa `/dev/xvdf1` menjadi volume root yang di-boot instance Anda setelah ramdisk awal berjalan, bukan `/dev/xvda1` volume yang ingin Anda boot. Untuk menyelesaikan hal ini, gunakan perintah e2label yang sama untuk mengubah label volume terlampir yang tidak ingin Anda gunakan untuk boot.

Dalam beberapa kasus, penentuan UUID di `/etc/fstab` dapat mengatasi hal ini. Namun, jika kedua volume tersebut berasal dari snapshot yang sama, atau yang sekunder dibuat dari snapshot volume primer, keduanya memiliki UUID yang sama.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

```
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

Untuk mengubah label volume ext4 terlampir

1. Gunakan perintah e2label untuk mengubah label volume agar menjadi sesuatu selain /.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1 old/
   ```

2. Verifikasi bahwa volume tersebut memiliki label baru.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1
   old/
   ```

Untuk mengubah label volume xfs terlampir

- Gunakan perintah xfs_admin untuk mengubah label volume agar menjadi sesuatu selain /.

  ```
  [ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
  writing all SBs
  new label = "old/"
  ```

Setelah mengubah label volume sebagaimana ditunjukkan, Anda dapat melakukan boot ulang instans dan memiliki volume yang tepat yang dipilih oleh ramdisk awal saat instans melakukan boot.

> **Important**
>
> Jika Anda ingin melepaskan lampiran volume dengan label baru dan mengembalikannya ke instans lain untuk digunakan sebagai volume root, Anda harus melakukan prosedur di atas lagi dan mengubah label volume kembali ke nilai aslinya. Jika tidak, instans lain tidak bisa melakukan boot karena ramdisk tidak dapat menemukan volume dengan label /.

Memecahkan masalah saat menghubungkan ke instans Amazon EC2 Windows

Informasi berikut dan kesalahan umum dapat membantu Anda memecahkan masalah saat menghubungkan ke instance Windows Anda.

Masalah koneksi

- Desktop Jarak Jauh tidak dapat terhubung ke komputer jarak jauh
- Kesalahan menggunakan klien RDP macOS
- RDP menampilkan layar hitam, bukan desktop
- Tidak dapat masuk dari jarak jauh ke sebuah instans dengan pengguna yang bukan administrator
- Memecahkan masalah Remote Desktop menggunakan AWS Systems Manager
- Aktifkan Desktop Jarak Jauh pada instans EC2 dengan registri jarak jauh
- Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance Windows?

Desktop Jarak Jauh tidak dapat terhubung ke komputer jarak jauh

Coba hal berikut untuk menyelesaikan masalah yang terkait dengan menghubungkan ke instans Anda:

- Verifikasi bahwa Anda menggunakan nama host DNS publik yang benar. (Di konsol Amazon EC2, pilih instans dan periksa DNS Publik (IPv4) di panel detail.) Jika instans Anda ada di VPC dan Anda tidak melihat nama DNS publik, Anda harus mengaktifkan nama host DNS. Untuk informasi selengkapnya, lihat Atribut DNS untuk VPC Anda di Panduan Pengguna Amazon VPC.
- Verifikasi bahwa instans Anda memiliki IPv4 alamat publik. Jika tidak, Anda dapat mengaitkan alamat IP Elastis dengan instans Anda. Untuk informasi selengkapnya, lihat Alamat Elastic IP.
- Untuk terhubung ke instans Anda menggunakan IPv6 alamat, periksa apakah komputer lokal Anda memiliki IPv6 alamat dan dikonfigurasi untuk digunakan IPv6. Untuk informasi selengkapnya, lihat Mengonfigurasi instans Anda IPv6 di Panduan Pengguna Amazon VPC.
- Verifikasi bahwa grup keamanan Anda memiliki aturan yang memungkinkan akses RDP pada port 3389.
- Jika Anda menyalin kata sandi, tetapi mendapatkan kesalahan `Your credentials did not work`, coba ketik secara manual saat diminta. Ada kemungkinan Anda melewatkan satu karakter atau mengetik karakter spasi tambahan saat Anda menyalin kata sandi.

- Verifikasi bahwa instans telah lulus pemeriksaan status. Untuk informasi selengkapnya, lihat Pemeriksaan status untuk instans Amazon EC2 dan the section called “Pemeriksaan status gagal instance Linux”.
- Verifikasi bahwa tabel rute untuk subnet memiliki rute yang mengirimkan semua lalu lintas yang ditujukan di luar VPC ke gateway internet untuk VPC. Untuk informasi selengkapnya, lihat Membuat tabel rute kustom (Gateway Internet) di Panduan Pengguna Amazon VPC.
- Verifikasi bahwa Windows Firewall, atau perangkat lunak firewall lainnya tidak memblokir lalu lintas RDP ke instans. Sebaiknya Anda menonaktifkan Windows Firewall dan mengendalikan akses ke instans Anda menggunakan aturan grup keamanan. Coba salah satu opsi berikut:
  - Gunakan AWSSupport-TroubleshootRDPuntukdisable the Windows Firewall profiles using SSM Agent. Opsi ini mengharuskan instance dikonfigurasi untuk AWS Systems Manager.
  - Gunakan AWSSupport-ExecuteEC2Rescue.
  - Hentikan instance, lepaskan volume root, dan lampirkan volume ke instance sementara sebagai volume data. Connect ke instance sementara dan bawa volume online. Muat sarang registri dari volume data. Di bawah`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicyStandardProfile`, atur `EnableFirewall` ke 0. Bongkar sarang registri dan kemudian bawa volumenya offline. Lepaskan volume dari instance sementara dan pasang ke instance asli sebagai volume root. Mulai contoh asli.
- Verifikasi bahwa Autentikasi Tingkat Jaringan dinonaktifkan pada instans yang bukan bagian dari domain Direktori Aktif (gunakan AWSSupport-TroubleshootRDP untuk disable NLA).
- Verifikasi bahwa Remote Desktop Service (TermService) Jenis Startup Otomatis dan layanan dimulai (gunakan AWSSupport-TroubleshootRDPuntukenable and start the RDP service).
- Verifikasi bahwa Anda tersambung ke port Remote Desktop Protocol yang benar, yang secara default adalah 3389 (gunakan AWSSupport-TroubleshootRDP untuk read the current RDP port dan change it back to 3389).
- Verifikasi bahwa koneksi Desktop Jarak Jauh diizinkan pada instans Anda (gunakan AWSSupport-TroubleshootRDP ke enable Remote Desktop connections).
- Verifikasi bahwa kata sandi belum kedaluwarsa. Jika kata sandi telah kedaluwarsa, Anda dapat mengatur ulang kata sandi. Untuk informasi selengkapnya, lihat Setel ulang kata sandi administrator Windows untuk instans Windows Amazon EC2.
- Jika Anda mencoba untuk terhubung menggunakan pengguna yang dibuat pada instans dan menerima kesalahan `The user cannot connect to the server due to insufficient`

`access privileges`, verifikasi bahwa Anda memberi pengguna hak untuk masuk secara lokal. Untuk informasi selengkapnya, lihat Memberi Anggota Hak untuk Masuk secara Lokal.

- Jika Anda mencoba lebih dari sesi RDP bersamaan maksimum yang diperbolehkan, sesi Anda akan diakhiri dengan pesan `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` Secara default, Anda mengizinkan dua sesi RDP bersamaan untuk instans Anda.

Kesalahan menggunakan klien RDP macOS

Jika Anda terhubung ke instance Windows Server menggunakan klien Remote Desktop Connection dari situs web Microsoft, Anda mungkin mendapatkan kesalahan berikut:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Unduh aplikasi Microsoft Remote Desktop dari Mac App Store dan gunakan aplikasi untuk terhubung ke instans Anda.

RDP menampilkan layar hitam, bukan desktop

Untuk mengatasi masalah ini, coba hal berikut:

- Periksa output konsol untuk informasi tambahan. Untuk mendapatkan output konsol pada instans Anda menggunakan konsol Amazon EC2, pilih instans, lalu pilih Tindakan, Pantau dan atasi masalah, Dapatkan log sistem.
- Verifikasi bahwa Anda menjalankan versi terbaru klien RDP Anda.
- Coba pengaturan default untuk klien RDP.
- Jika Anda menggunakan Koneksi Desktop Jarak Jauh, coba mulai dengan opsi `/admin` sebagai berikut.

```
mstsc /v:instance /admin
```

- Jika server menjalankan aplikasi layar penuh, server mungkin berhenti merespons. Gunakan Ctrl +Shift+ Esc untuk memulai Windows Task Manager, lalu tutup aplikasi.
- Jika server digunakan secara berlebihan, server mungkin berhenti merespons. Untuk memantau instans menggunakan konsol Amazon EC2, pilih instans, lalu pilih tab Pemantauan. Jika Anda

perlu mengubah tipe instans ke ukuran yang lebih besar, lihat Perubahan jenis instans Amazon EC2.

Tidak dapat masuk dari jarak jauh ke sebuah instans dengan pengguna yang bukan administrator

Jika Anda tidak dapat masuk dari jarak jauh ke instans Windows dengan pengguna yang bukan akun administrator, pastikan bahwa Anda telah memberi pengguna hak untuk masuk secara lokal. Lihat Memberi pengguna atau grup hak untuk masuk secara lokal ke pengendali domain di domain.

Memecahkan masalah Remote Desktop menggunakan AWS Systems Manager

Anda dapat menggunakan AWS Systems Manager untuk memecahkan masalah yang menghubungkan ke instance Windows Anda menggunakan RDP.

AWSSupport-TroubleshootRDP

Dokumen AWSSupport-TroubleshootRDP otomatisasi memungkinkan pengguna untuk memeriksa atau memodifikasi pengaturan umum pada instance target yang dapat memengaruhi koneksi Remote Desktop Protocol (RDP), seperti Port RDP, Network Layer Authentication (NLA), dan profil Windows Firewall. Secara default, dokumen membaca dan mengeluarkan nilai pengaturan ini.

Dokumen AWSSupport-TroubleshootRDP otomatisasi dapat digunakan dengan instans EC2, instans lokal, dan mesin virtual (VMs) yang diaktifkan untuk digunakan dengan AWS Systems Manager (instans terkelola). Selain itu, dokumen otomatisasi juga dapat digunakan dengan instans EC2 pada Windows Server yang tidak diaktifkan untuk digunakan dengan Systems Manager. Untuk informasi tentang mengaktifkan instance untuk digunakan AWS Systems Manager, lihat Node terkelola di AWS Systems Manager Panduan Pengguna.

Untuk memecahkan masalah menggunakan dokumen AWSSupport-TroubleshootRDP

1. Masuk ke Konsol Systems Manager.
2. Verifikasi bahwa Anda berada di Wilayah yang sama dengan instans yang mengalami gangguan.
3. Pilih Dokumen dari panel navigasi kiri.

4. Pada tab Dimiliki oleh Amazon, masukkan `AWSSupport-TroubleshootRDP` di bidang pencarian. Saat dokumen `AWSSupport-TroubleshootRDP` muncul, pilihlah.
5. Pilih Eksekusi otomatisasi.
6. Untuk Mode Eksekusi, pilih Eksekusi sederhana.
7. Untuk parameter Input,InstanceId, aktifkan Tampilkan alat pilih instance interaktif.
8. Pilih instans Amazon EC2 Anda.
9. Tinjau contoh, lalu pilih Eksekusi.
10. Untuk memantau kemajuan eksekusi, pada Status eksekusi, tunggu status berubah dari Tertunda menjadi Berhasil. Perluas Output untuk melihat hasilnya. Untuk melihat output setiap langkah, di Langkah-langkah yang Dieksekusi, pilih item dari ID Langkah.

AWSSupport-TroubleshootRDP contoh

Contoh berikut menunjukkan cara menyelesaikan tugas pemecahan masalah umum menggunakan. AWSSupport-TroubleshootRDP Anda dapat menggunakan AWS CLI start-automation-executionperintah contoh atau tautan yang disediakan ke file Konsol Manajemen AWS.

Example Contoh: Periksa status RDP saat ini

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom" --region region_code
```

AWS Systems Manager konsol:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Contoh: Nonaktifkan Windows Firewall

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=i-1234567890abcdef0, Action=Custom, Firewall=Disable" --
region region_code
```

AWS Systems Manager konsol:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Contoh: Nonaktifkan Autentikasi Tingkat Jaringan

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, NLASettingAction=Disable" --
region region_code
```

AWS Systems Manager konsol:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Contoh: Atur Tipe Startup Layanan RDP ke Otomatis dan mulai layanan RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

AWS Systems Manager konsol:

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Contoh: Pulihkan Port RDP default (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RDPPortAction=Modify" --
region region_code
```

AWS Systems Manager konsol:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Contoh: Izinkan koneksi jarak jauh

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RemoteConnections=Enable" --
region region_code
```

AWS Systems Manager konsol:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport-ExecuteEC2Penyelamatan

Dokumen otomatisasi AWSSupport-ExecuteEC 2Rescue menggunakan EC2Rescue untuk Windows Server untuk secara otomatis memecahkan masalah dan memulihkan konektivitas instans EC2 dan masalah RDP. Untuk informasi selengkapnya, lihat Menjalankan alat EC2 Penyelamatan pada instance yang tidak dapat dijangkau.

Dokumen otomatisasi AWSSupport-ExecuteEC 2Rescue memerlukan penghentian dan restart instance. Otomatisasi System Manager menghentikan instans dan membuat Amazon Machine Image (AMI). Data yang disimpan dalam volume penyimpanan instans hilang. Alamat IP publik berubah jika Anda tidak menggunakan alamat IP Elastis. Untuk informasi selengkapnya, lihat Menjalankan alat EC2 Penyelamatan pada instance yang tidak dapat dijangkau di Panduan Pengguna.AWS Systems Manager

Untuk memecahkan masalah menggunakan dokumen 2Rescue AWSSupport-ExecuteEC

1. Buka konsol System Manager.
2. Verifikasi bahwa Anda berada di Wilayah yang sama dengan instans Amazon EC2 yang mengalami gangguan.
3. Di panel navigasi, pilih Dokumen.
4. Cari dan pilih dokumen `AWSSupport-ExecuteEC2Rescue`, lalu pilih Eksekusi otomatisasi.
5. Untuk Mode Eksekusi, pilih Eksekusi sederhana.

6. Di bagian Parameter masukan, untukUnreachableInstanceId, masukkan ID instans Amazon EC2 dari instans yang tidak dapat dijangkau.
7. (Opsional) UntukLogDestination, masukkan nama bucket Amazon Simple Storage Service (Amazon S3) jika Anda ingin mengumpulkan log sistem operasi untuk memecahkan masalah instans Amazon EC2 Anda. Log secara otomatis diunggah ke bucket yang ditentukan.
8. Pilih Eksekusi.
9. Untuk memantau kemajuan eksekusi, pada Status eksekusi, tunggu status berubah dari Tertunda menjadi Berhasil. Perluas Output untuk melihat hasilnya. Untuk melihat output setiap langkah, di Langkah-langkah yang Dieksekusi, pilih ID Langkah.

Aktifkan Desktop Jarak Jauh pada instans EC2 dengan registri jarak jauh

Jika instans yang tidak dapat dijangkau tidak dikelola oleh AWS Systems Manager Session Manager, maka Anda dapat menggunakan registri jarak jauh untuk mengaktifkan Remote Desktop.

1. Dari konsol EC2, hentikan instans yang tak terjangkau.
2. Lepaskan volume root dari instans tak terjangkau dan lampirkan ke instans terjangkau di Zona Ketersediaan yang sama dengan volume penyimpanan. Jika Anda tidak memiliki instans terjangkau di Zona Ketersediaan yang sama, luncurkan satu instans. Perhatikan nama perangkat volume root pada instans yang tak terjangkau.
3. Pada instans terjangkau, buka Manajemen Disk. Anda dapat melakukannya dengan menjalankan perintah berikut di jendela Prompt Perintah.

   ```
   diskmgmt.msc
   ```
4. Klik kanan volume yang baru dilampirkan, yang berasal dari instans tak terjangkau, lalu pilih Online.
5. Buka Windows Registry Editor. Anda dapat melakukannya dengan menjalankan perintah berikut di jendela Prompt Perintah.

   ```
   regedit
   ```
6. Di Registry Editor, pilih HKEY_LOCAL_MACHINE, lalu pilih File, Muat Hive.
7. Pilih drive dari volume yang terlampir, navigasikan ke `\Windows\System32\config\`, pilih `SYSTEM`, lalu pilih Buka.
8. Untuk Nama Kunci, masukkan nama unik untuk hive dan pilih OKE.

9. Cadangkan hive registri sebelum membuat perubahan pada registri tersebut.

   a. Di pohon konsol Registry Editor, pilih sarang yang Anda muat: HKEY_LOCAL_MACHINE\. *your-key-name*

   b. Pilih File, Ekspor.

   c. Di kotak dialog Ekspor File Registri, pilih lokasi tempat Anda ingin menyimpan salinan cadangan, lalu ketik nama untuk file cadangan di bidang Nama file.

   d. Pilih Simpan.

10. Di Editor Registri, arahkan ke**HKEY_LOCAL_MACHINE*your key name*\ControlSet001\Control\Terminal Server**, dan kemudian, di panel detail, klik dua kali fDeny. TSConnections

11. Di kotak nilai Edit DWORD, masukkan `0` di bidang Data nilai.

12. Pilih OKE.

> **Note**
>
> Jika nilai di bidang Data nilai adalah `1`, instans akan menolak koneksi desktop jarak jauh. Nilai `0` memungkinkan koneksi desktop jarak jauh.

13. Di Registry Editor, pilih HKEY_LOCAL_MACHINE***your-key-name***, lalu pilih File, Unload Hive.

14. Tutup Registry Editor dan Manajemen Disk.

15. Dari konsol EC2, lepaskan volume dari instans terjangkau, dan lampirkan kembali ke instans yang tak terjangkau. Saat melampirkan volume ke instans tak terjangkau, masukkan nama perangkat yang Anda simpan sebelumnya di bidang perangkat.

16. Mulai ulang instans tak terjangkau.

Saya kehilangan kunci privat. Bagaimana saya bisa terhubung ke instance Windows?

Saat Anda terhubung ke instans Windows yang baru diluncurkan, Anda mendekripsi kata sandi untuk akun Administrator menggunakan kunci privat untuk pasangan kunci yang Anda tentukan saat meluncurkan instans.

Jika Anda menghilangkan kata sandi Administrator dan tidak lagi memiliki kunci privat, Anda harus mengatur ulang kata sandi atau membuat sebuah instans baru. Untuk informasi selengkapnya, lihat

Setel ulang kata sandi administrator Windows untuk instans Windows Amazon EC2. Untuk langkah-langkah mengatur ulang kata sandi menggunakan dokumen Systems Manager, lihat Atur ulang kata sandi dan kunci SSH pada instans EC2 di Panduan Pengguna AWS Systems Manager .

Memecahkan masalah awal instans Amazon EC2 Windows

Berikut ini adalah tips pemecahan masalah untuk membantu Anda memecahkan masalah kata sandi dan aktivasi dengan instans Amazon EC2 Windows.

Masalah

- “Kata sandi tidak tersedia”
- “Kata sandi belum tersedia”
- “Tidak dapat mengambil kata sandi Windows”
- “Menunggu layanan metadata”
- “Tidak dapat mengaktifkan Windows”
- “Windows tidak asli (0x80070005)”
- “Tidak ada Server Lisensi Server Terminal yang tersedia untuk memberikan lisensi”
- “Beberapa pengaturan dikelola oleh organisasi Anda”

“Kata sandi tidak tersedia”

Untuk menghubungkan ke instans Windows menggunakan Desktop Jarak Jauh, Anda harus menentukan akun dan kata sandi. Akun dan kata sandi yang diberikan didasarkan pada AMI yang Anda gunakan untuk meluncurkan instans. Anda dapat mengambil kata sandi yang dibuat secara otomatis untuk akun Administrator, atau menggunakan akun dan kata sandi yang digunakan dalam instans asli tempat AMI dibuat.

Anda dapat membuat kata sandi untuk akun Administrator pada instans yang diluncurkan menggunakan AMI Windows kustom. Untuk menghasilkan kata sandi, Anda perlu mengonfigurasi beberapa pengaturan di sistem operasi sebelum AMI dibuat. Untuk informasi selengkapnya, lihat Buat AMI yang didukung Amazon EBS-Backed.

Jika instans Windows Anda tidak dikonfigurasi untuk menghasilkan kata sandi acak, Anda akan menerima pesan berikut saat Anda mengambil kata sandi yang dibuat secara otomatis menggunakan konsol:

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Periksa output konsol pada instans tersebut untuk melihat apakah AMI yang Anda gunakan untuk meluncurkannya dibuat dengan pembuatan kata sandi yang nonaktif. Jika pembuatan kata sandi dinonaktifkan, output konsol berisi hal-hal berikut ini:

```
Ec2SetPassword: Disabled
```

Jika pembuatan kata sandi dinonaktifkan dan Anda tidak ingat kata sandi untuk instans aslinya, Anda dapat menyetel ulang kata sandi untuk instans ini. Untuk informasi selengkapnya, lihat Setel ulang kata sandi administrator Windows untuk instans Windows Amazon EC2.

“Kata sandi belum tersedia”

Untuk menghubungkan ke instans Windows menggunakan Desktop Jarak Jauh, Anda harus menentukan akun dan kata sandi. Akun dan kata sandi yang diberikan didasarkan pada AMI yang Anda gunakan untuk meluncurkan instans. Anda dapat mengambil kata sandi yang dibuat secara otomatis untuk akun Administrator, atau menggunakan akun dan kata sandi yang digunakan dalam instans asli tempat AMI dibuat.

Kata sandi Anda akan tersedia dalam beberapa menit. Jika kata sandi tidak tersedia, Anda akan menerima pesan berikut ketika Anda mengambil kata sandi yang dibuat secara otomatis menggunakan konsol:

```
Password not available yet.
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Jika sudah lebih dari empat menit dan Anda masih tidak bisa mendapatkan kata sandinya, mungkin agen peluncuran untuk instans Anda tidak dikonfigurasi untuk membuat kata sandinya. Verifikasi dengan memeriksa apakah output konsol kosong atau tidak. Untuk informasi selengkapnya, lihat Tidak bisa mendapatkan output konsol.

Juga verifikasi bahwa akun AWS Identity and Access Management (IAM) yang digunakan untuk mengakses Portal Manajemen memiliki `ec2:GetPasswordData` tindakan yang diizinkan. Untuk informasi tentang izin IAM selengkapnya, lihat Apa itu IAM?.

“Tidak dapat mengambil kata sandi Windows”

Untuk mendapatkan kembali kata sandi yang dibuat secara otomatis pada akun Administrator, Anda harus menggunakan kunci privat untuk pasangan kunci yang Anda tentukan saat meluncurkan instans. Jika Anda tidak menentukan pasangan kunci saat meluncurkan instans, Anda akan menerima pesan berikut.

```
Cannot retrieve Windows password
```

Anda dapat menghentikan instans ini dan meluncurkan instans baru menggunakan AMI yang sama, pastikan untuk menentukan pasangan kunci.

“Menunggu layanan metadata”

Sebelum diaktifkan, instans Windows harus memperoleh informasi dari metadata instans miliknya. Secara default, `WaitForMetaDataAvailable` pengaturan memastikan bahwa layanan EC2 Config menunggu metadata instance dapat diakses sebelum melanjutkan proses boot. Untuk informasi selengkapnya, lihat Gunakan metadata instans untuk mengelola instans EC2.

Jika instans gagal dalam uji jangkauan instans, coba langkah berikut untuk menyelesaikan masalah ini.

- Periksa blok CIDR untuk VPC Anda. Instans Windows tidak dapat melakukan boot dengan benar jika diluncurkan ke VPC yang memiliki rentang alamat IP dari `224.0.0.0` hingga `255.255.255.255` (Rentang Alamat IP Kelas D dan Kelas E). Rentang alamat IP ini disimpan, dan tidak boleh ditetapkan ke perangkat host. Sebaiknya Anda membuat VPC dengan blok CIDR dari rentang alamat IP privat (tidak dapat dirutekan secara publik) seperti yang ditentukan dalam RFC 1918.
- Mungkin saja sistem telah dikonfigurasi dengan alamat IP statis. Coba buat antarmuka jaringan dan lampirkan ke instans.
- Untuk mengaktifkan DHCP pada instans Windows yang tidak dapat Anda sambungkan

  1. Hentikan instans yang terpengaruh dan lepaskan volume root-nya.

2. Luncurkan instans sementara di Zona Ketersediaan yang sama dengan instans yang terpengaruh.

> **Warning**
>
> Jika instans sementara Anda didasarkan pada AMI yang sama dengan instans asli, Anda harus menyelesaikan langkah-langkah tambahan atau Anda tidak akan dapat melakukan boot instans asli setelah memulihkan volume root-nya karena tabrakan tanda tangan disk. Atau, pilih AMI yang berbeda untuk instans sementara. Misalnya, jika instance asli menggunakan AWS Windows AMI untuk Windows Server 2016, luncurkan instance sementara menggunakan AWS Windows AMI untuk Windows Server 2019.

3. Lampirkan volume root dari instans yang terpengaruh ke instans sementara ini. Hubungkan ke instans sementara, buka utilitas Manajemen Disk, dan buat drive menjadi online.
4. Dari instans sementara, buka Regedit dan pilih HKEY_LOCAL_MACHINE. Dari menu File, pilih Muat Hive. Pilih drive, buka file `Windows\System32\config\SYSTEM`, dan tentukan nama kunci saat diminta (Anda dapat menggunakan nama apa pun).
5. Pilih kunci yang baru saja Anda muat dan navigasikan ke `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Setiap antarmuka jaringan dicantumkan oleh GUID. Pilih antarmuka jaringan yang benar. Jika DHCP dinonaktifkan dan alamat IP statis ditetapkan, `EnableDHCP` diatur ke 0. Untuk mengaktifkan DHCP, atur `EnableDHCP` ke 1, dan hapus kunci berikut jika ada: `NameServer`, `SubnetMask`, `IPAddress`, dan `DefaultGateway`. Pilih lagi kunci tersebut, dan dari menu File, pilih Bongkar Hive.

> **Note**
>
> Jika Anda memiliki banyak antarmuka jaringan, Anda harus mengidentifikasi antarmuka yang benar untuk mengaktifkan DHCP. Untuk mengidentifikasi antarmuka jaringan yang benar, tinjau nilai kunci berikut `NameServer`, `SubnetMask`, `IPAddress`, dan `DefaultGateway`. Nilai-nilai ini menampilkan konfigurasi statis instans sebelumnya.

6. (Opsional) Jika DHCP sudah diaktifkan, Anda mungkin tidak memiliki rute ke layanan metadata. Memperbarui EC2 Config dapat menyelesaikan masalah ini.

a. Unduh dan instal versi terbaru dari layanan EC2 Config. Untuk informasi selengkapnya tentang menginstal layanan ini, lihat the section called “Instal EC2 Config”.

b. Ekstrak file dari file `.zip` ke direktori `Temp` pada drive yang Anda lampirkan.

c. Buka Regedit dan pilih HKEY_LOCAL_MACHINE. Dari menu File, pilih Muat Hive. Pilih drive, buka file `Windows\System32\config\SOFTWARE`, dan tentukan nama kunci saat diminta (Anda dapat menggunakan nama apa pun).

d. Pilih kunci yang baru saja Anda muat dan navigasikan ke `Microsoft\Windows \CurrentVersion`. Pilih kunci `RunOnce`. (Jika kunci ini tidak ada, klik kanan `CurrentVersion`, arahkan ke Baru, pilih Kunci, dan beri nama kunci `RunOnce`.) Klik kanan, arahkan ke Baru, dan pilih Nilai String. Masukkan`Ec2Install` sebagai nama dan `C:\Temp\Ec2Install.exe -q` sebagai data.

e. Pilih lagi kunci tersebut, dan dari menu File, pilih Bongkar Hive.

7. (Opsional) Jika instans sementara Anda didasarkan pada AMI yang sama dengan instans asli, Anda harus menyelesaikan langkah-langkah berikut atau Anda tidak akan dapat melakukan boot instans asli setelah memulihkan volume root-nya karena tabrakan tanda tangan disk.

> ⚠ Warning
>
> Prosedur berikut menjelaskan cara mengedit Windows Registry menggunakan Registry Editor. Jika Anda tidak terbiasa dengan Windows Registry atau cara membuat perubahan dengan aman menggunakan Registry Editor, lihat Konfigurasi Registry.

a. Buka prompt perintah, ketik regedit.exe, dan tekan Enter.

b. Di Registry Editor, pilih HKEY_LOCAL_MACHINE dari menu konteks (klik kanan), lalu pilih Temukan.

c. Ketik Windows Boot Manager, lalu pilih Temukan Berikutnya.

d. Pilih kunci bernama `11000001`. Kunci ini adalah kelompok dari kunci yang Anda temukan di langkah sebelumnya.

e. Pada panel kanan, pilih `Element`, lalu pilih Ubah dari menu konteks (klik kanan).

f. Temukan tanda tangan disk empat bita pada offset 0x38 dalam data tersebut. Balikkan bita tersebut untuk membuat tanda tangan disk, dan tuliskan. Misalnya, tanda tangan disk yang diwakili oleh data berikut ini adalah `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. Di jendela Command Prompt, jalankan perintah berikut untuk memulai Microsoft DiskPart.

```
diskpart
```

h. Jalankan DiskPart perintah berikut untuk memilih volume. (Anda dapat memverifikasi bahwa nomor disk adalah 1 menggunakan utilitas Manajemen Disk.)

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Jalankan DiskPart perintah berikut untuk mendapatkan tanda tangan disk.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Jika tanda tangan disk yang ditunjukkan pada langkah sebelumnya tidak cocok dengan tanda tangan disk dari BCD yang Anda tulis sebelumnya, gunakan DiskPart perintah berikut untuk mengubah tanda tangan disk sehingga cocok:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Menggunakan utilitas Manajemen Disk, buat drive menjadi offline.

> **Note**
>
> Drive secara otomatis offline jika instans sementara menjalankan sistem operasi yang sama dengan instans yang terpengaruh, jadi Anda tidak perlu membuatnya offline secara manual.

9. Lepaskan volume dari instans sementara. Anda dapat mengakhiri instans sementara jika tidak menggunakannya lagi.

10. Pulihkan volume root dari instans yang terpengaruh dengan melampirkan volume sebagai `/dev/sda1`.
11. Mulai instans yang terpengaruh.

Jika Anda terhubung ke instans, buka peramban Internet dari instans dan masukkan URL berikut untuk server metadata:

```
http://169.254.169.254/latest/meta-data/
```

Jika Anda tidak dapat menghubungi server metadata, coba langkah berikut ini untuk menyelesaikan masalah ini:

- Unduh dan instal versi terbaru dari layanan EC2 Config. Untuk informasi selengkapnya tentang menginstal layanan ini, lihat the section called “Instal EC2 Config”.
- Periksa apakah instance Windows menjalankan driver Red Hat PV. Jika iya, perbarui ke driver Citrix PV. Untuk informasi selengkapnya, lihat the section called “Mutakhirkan driver PV”.
- Verifikasi bahwa firewall IPSec,, dan pengaturan proxy tidak memblokir lalu lintas keluar ke layanan metadata (`169.254.169.254`) atau AWS KMS server (alamat ditentukan dalam `TargetKMSServer` elemen di). `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml`
- Pastikan Anda memiliki rute ke layanan metadata (`169.254.169.254`) menggunakan perintah berikut.

  ```
  route print
  ```

- Periksa masalah jaringan yang mungkin memengaruhi Zona Ketersediaan untuk instans Anda. Buka http://status.aws.amazon.com/.

“Tidak dapat mengaktifkan Windows”

Instans Windows menggunakan AWS KMS aktivasi Windows. Anda dapat menerima pesan ini:`A problem occurred when Windows tried to activate. Error Code 0xC004F074`, jika instans Anda tidak dapat mencapai AWS KMS server. Windows harus diaktifkan setiap 180 hari. EC2Config mencoba menghubungi AWS KMS server sebelum periode aktivasi berakhir untuk memastikan bahwa Windows tetap diaktifkan.

Jika Anda mengalami masalah aktivasi Windows, gunakan prosedur berikut ini untuk menyelesaikan masalah tersebut.

Untuk EC2 Config (Windows Server 2012 R2 AMIs dan sebelumnya)

1. Unduh dan instal versi terbaru dari layanan EC2 Config. Untuk informasi selengkapnya tentang menginstal layanan ini, lihat the section called “Instal EC2 Config”.
2. Masuk ke instans dan buka file berikut: `C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml`.
3. Temukan WindowsActivate plugin Ec2 di `config.xml` file. Ubah statusnya ke Diaktifkan dan simpan perubahan Anda.
4. Di snap-in Layanan Windows, restart layanan EC2 Config atau reboot instance.

Jika langkah ini tidak menyelesaikan masalah aktivasi, ikuti langkah-langkah tambahan berikut.

1. Tetapkan AWS KMS target: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Aktifkan Windows: C:\> slmgr.vbs /ato

Untuk EC2 Peluncuran (Windows Server 2016 AMIs dan yang lebih baru)

1. Dari PowerShell prompt dengan hak administratif, impor modul EC2 Peluncuran:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Panggil fungsi Add-Routes untuk melihat daftar rute baru:

```
PS C:\> Add-Routes
```

3. Panggil ActivationSettings fungsi Set-:

```
PS C:\> Set-Activationsettings
```

4. Kemudian, jalankan script berikut untuk mengaktifkan Windows:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Untuk EC2 Config dan EC2 Launch, jika Anda masih menerima kesalahan aktivasi, verifikasi informasi berikut.

- Verifikasi bahwa Anda memiliki rute ke AWS KMS server. Buka `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` dan temukan elemen `TargetKMSServer`. Jalankan perintah berikut dan periksa apakah alamat untuk AWS KMS server ini terdaftar.

  ```
  route print
  ```

- Verifikasi bahwa kunci AWS KMS klien disetel. Jalankan perintah berikut dan periksa output-nya.

  ```
  C:\Windows\System32\slmgr.vbs /dlv
  ```

  Jika output berisi Error: kunci produk tidak ditemukan, kunci AWS KMS klien tidak disetel. Jika kunci AWS KMS klien tidak disetel, cari kunci klien seperti yang dijelaskan dalam artikel Microsoft ini: aktivasi AWS KMS klien dan kunci produk, lalu jalankan perintah berikut untuk mengatur kunci AWS KMS klien.

  ```
  C:\Windows\System32\slmgr.vbs /ipk client_key
  ```

- Pastikan sistem memiliki waktu dan zona waktu yang benar. Jika Anda menggunakan zona waktu selain UTC, tambahkan kunci registri berikut dan atur 1 untuk memastikan bahwa waktunya sudah benar: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`
- Jika Windows Firewall diaktifkan, nonaktifkan untuk sementara menggunakan perintah berikut.

  ```
  netsh advfirewall set allprofiles state off
  ```

“Windows tidak asli (0x80070005)”

Instans Windows menggunakan AWS KMS aktivasi Windows. Jika sebuah instans tidak dapat menyelesaikan proses aktivasi, instans akan melaporkan bahwa salinan Windows tidak asli.

Coba saran untuk “Tidak dapat mengaktifkan Windows”.

“Tidak ada Server Lisensi Server Terminal yang tersedia untuk memberikan lisensi”

Secara default, Windows Server dilisensikan untuk dua pengguna simultan melalui Desktop Jarak Jauh. Jika Anda perlu memberi lebih dari dua pengguna akses simultan ke instans Windows melalui Desktop Jarak Jauh, Anda dapat membeli lisensi akses klien (CAL) Remote Desktop Services dan menginstal peran Host Sesi Desktop Jarak Jauh dan Server Lisensi Desktop Jarak Jauh.

Periksa masalah berikut:

- Anda telah melebihi jumlah maksimum sesi RDP bersamaan.
- Anda telah menginstal peran Layanan Windows Remote Desktop Services.
- Lisensi telah kedaluwarsa. Jika lisensi telah kedaluwarsa, Anda tidak dapat terhubung ke instans Windows Anda sebagai pengguna. Anda dapat mencoba hal-hal berikut ini:
  - Hubungkan ke instans dari baris perintah menggunakan parameter `/admin`, misalnya:

    ```
    mstsc /v:instance /admin
    ```

    Untuk informasi selengkapnya, lihat artikel Microsoft berikut: Akses Desktop Jarak Jauh Melalui Baris Perintah.
  - Hentikan instans, lepaskan volume Amazon EBS-nya, dan lampirkan ke instans lain di Zona Ketersediaan yang sama untuk memulihkan data Anda.

“Beberapa pengaturan dikelola oleh organisasi Anda”

Instans yang diluncurkan dari Windows Server terbaru AMIs mungkin menampilkan pesan dialog Pembaruan Windows yang menyatakan “Beberapa pengaturan dikelola oleh organisasi Anda.” Pesan ini muncul sebagai akibat dari perubahan di Windows Server dan tidak memengaruhi perilaku Pembaruan Windows atau kemampuan Anda untuk mengelola pengaturan pembaruan.

Untuk menghapus peringatan

1. Buka `gpedit.msc` dan arahkan ke Konfigurasi Komputer, Templat Administratif, Komponen Windows, Pembaruan Windows. Edit Konfigurasi Pembaruan Otomatis, dan atur ke aktif.
2. Di perintah prompt, perbarui kebijakan grup menggunakan gpupdate /force.

3. Tutup dan buka kembali Pengaturan Pembaruan Windows. Anda akan melihat pesan di atas tentang pengaturan yang dikelola oleh organisasi Anda, diikuti dengan “Kami akan mengunduh pembaruan secara otomatis, kecuali pada koneksi terukur (di mana biaya dapat berlaku). Dalam hal ini, kami akan mengunduh pembaruan yang diperlukan secara otomatis agar Windows tetap berjalan dengan lancar”.
4. Kembali ke `gpedit.msc` dan atur kebijakan grup kembali ke tidak dikonfigurasi. Jalankan lagi gpupdate /force.
5. Tutup perintah prompt dan tunggu beberapa menit.
6. Buka kembali Pengaturan Pembaruan Windows. Anda tidak akan melihat pesan “Beberapa pengaturan dikelola oleh organisasi Anda”.

Memecahkan masalah dengan instans Windows Amazon EC2

Berikut ini adalah tips pemecahan masalah untuk membantu Anda memecahkan masalah dengan instans Windows Amazon EC2.

Masalah

- Tidak dapat menghubungkan AWS Systems Manager Sessions Manager ke instans Windows Server 2025
- Volume EBS tidak diinisialisasi di Windows Server 2016 dan 2019
- Lakukan boot instans Windows EC2 ke Directory Service Restore Mode (DSRM)
- Instans kehilangan konektivitas jaringan atau tugas terjadwal tidak berjalan saat diharapkan
- Tidak bisa mendapatkan output konsol
- Windows Server 2012 R2 tidak tersedia di jaringan
- Tabrakan tanda tangan disk

Tidak dapat menghubungkan AWS Systems Manager Sessions Manager ke instans Windows Server 2025

Anda mungkin mengalami masalah saat menghubungkan AWS Systems Manager Sessions Manager ke instans Windows Server 2025. Untuk mengatasi masalah ini, masuk ke instance, lalu navigasikan ke`Settings > Apps > Optional Features`, dan tambahkan`WMIC`. Mulai ulang layanan Agen SSM atau reboot instance, dan Sessions Manager harus terhubung.

Anda juga dapat menggunakan PowerShell perintah berikut untuk melakukan tindakan yang sama:

```
Start-Process -FilePath "$env:SystemRoot\system32\Dism.exe" -ArgumentList @('/
Online', '/Add-Capability', '/CapabilityName:WMIC~~~~') -Wait; Restart-Service -Name
 AmazonSSMAgent
```

Volume EBS tidak diinisialisasi di Windows Server 2016 dan 2019

Instans yang dibuat dari Amazon Machine Images (AMIs) untuk Windows Server 2016 dan 2019 menggunakan agen EC2 Launch v1 untuk berbagai tugas startup, termasuk menginisialisasi volume EBS. Secara default, EC2 Launch v1 tidak menginisialisasi volume sekunder. Namun, Anda dapat mengkonfigurasi EC2 Launch v1 untuk menginisialisasi disk ini secara otomatis, sebagai berikut.

Memetakan huruf drive ke volume

1. Hubungkan ke instans untuk mengonfigurasi dan membuka file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` di editor teks.
2. Tentukan pengaturan volume sebagai berikut:

   ```
   {
   "driveLetterMapping": [
    {
      "volumeName": "sample volume",
      "driveLetter": "H"
    }]
   }
   ```
3. Simpan perubahan Anda dan tutup file.
4. Buka Windows PowerShell dan gunakan perintah berikut untuk menjalankan skrip EC2 Launch v1 yang menginisialisasi disk:

   ```
   PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
   ```

   Untuk menginisialisasi disk setiap kali booting instans, tambahkan bendera `-Schedule` sebagai berikut:

   ```
   PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
   Schedule
   ```

Agen EC2 Launch v1 dapat menjalankan skrip inisialisasi instance seperti `initializeDisks.ps1` paralel dengan skrip. `InitializeInstance.ps1` Jika skrip `InitializeInstance.ps1` melakukan boot ulang instans, mungkin akan mengganggu tugas terjadwal lainnya yang berjalan pada startup instans. Untuk menghindari potensi konflik, sebaiknya Anda menambahkan logika ke skrip `initializeDisks.ps1` untuk memastikan bahwa inisialisasi instans telah selesai terlebih dahulu.

> **Note**
>
> Jika skrip EC2 Peluncuran tidak menginisialisasi volume, pastikan volumenya online. Jika volume offline, jalankan perintah berikut untuk menjadikan semua disk online.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Lakukan boot instans Windows EC2 ke Directory Service Restore Mode (DSRM)

Jika sebuah instans yang menjalankan Microsoft Active Directory mengalami gagal sistem atau masalah kritis lainnya, Anda dapat memecahkan masalah instans dengan melakukan boot ke versi khusus Mode Aman yang disebut Directory Service Restore Mode (DSRM). Di DSRM Anda dapat memperbaiki atau memulihkan Direktori Aktif.

Dukungan driver untuk DSRM

Cara Anda mengaktifkan DSRM dan melakukan boot ke instans bergantung pada driver yang dijalankan instans tersebut. Di konsol EC2, Anda dapat melihat detail versi driver untuk sebuah instans dari Log Sistem. Tabel berikut menunjukkan driver mana yang didukung untuk DSRM.

Versi Driver	DSRM Didukung?	Langkah Berikutnya
Citrix PV 5.9	Tidak	Pulihkan instans dari cadangan. Anda tidak dapat mengaktifkan DSRM.

Versi Driver	DSRM Didukung?	Langkah Berikutnya
AWS PV 7.2.0	Tidak	Meskipun DSRM tidak didukung untuk driver ini, Anda masih dapat melepaskan volume root dari instans, mengambil snapshot volume atau membuat AMI darinya, dan memasangnya ke instans lain di Zona Ketersediaan yang sama dengan volume sekunder. Kemudian, Anda dapat mengaktifkan DSRM (seperti yang dijelaskan di bagian ini).
AWS PV 7.2.2 dan yang lebih baru	Ya	Lepaskan volume root, pasang ke instans lain, dan aktifkan DSRM (seperti yang dijelaskan di bagian ini).
Jaringan yang Ditingkatkan	Ya	Lepaskan volume root, pasang ke instans lain, dan aktifkan DSRM (seperti yang dijelaskan di bagian ini).

Untuk informasi tentang cara mengaktifkan jaringan yang disempurnakan, lihatthe section called “Adaptor Jaringan Elastis (ENA)”. Untuk informasi tentang memutakhirkan driver AWS PV, lihat Memutakhirkan driver PV di instans Windows.

Konfigurasikan sebuah instans untuk melakukan boot ke DSRM

Instans Windows EC2 tidak memiliki konektivitas jaringan sebelum sistem operasi berjalan. Karena alasan ini, Anda tidak dapat menekan tombol F8 pada papan tombol Anda untuk memilih opsi boot. Anda harus menggunakan salah satu dari prosedur berikut untuk melakukan boot instans Server Windows EC2 ke DSRM.

Jika Anda mencurigai bahwa Direktori Aktif telah rusak dan instans masih berjalan, Anda dapat mengonfigurasi instans tersebut untuk boot ke DSRM menggunakan kotak dialog Konfigurasi Sistem atau prompt perintah.

Untuk boot instans online ke DSRM menggunakan kotak dialog Konfigurasi Sistem

1. Di kotak dialog Jalankan, ketik `msconfig` dan tekan Enter.
2. Pilih tab Boot.
3. Di bawah Opsi boot pilih Boot aman.

4. Pilih perbaikan Direktori Aktif, lalu pilih OK. Sistem meminta Anda untuk melakukan boot ulang server.

Untuk melakukan boot instans online ke DSRM menggunakan baris perintah

Dari jendela Prompt Perintah, jalankan perintah berikut:

```
bcdedit /set safeboot dsrepair
```

Jika sebuah instans sedang offline dan tidak dapat dijangkau, Anda harus melepaskan volume root serta memasangnya ke instans lain untuk mengaktifkan mode DSRM.

Untuk melakukan boot instans offline ke DSRM

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Cari dan pilih instans yang terpengaruh. Pilih Status instans, Hentikan instans.
4. Pilih Luncurkan instans dan buat instans sementara di Zona Ketersediaan yang sama dengan instans yang terpengaruh. Pilih tipe instans yang menggunakan versi Windows yang berbeda. Misalnya, jika instans Anda adalah Windows Server 2016, maka pilih instance Windows Server 2019.

   > **Important**
   >
   > Jika Anda tidak membuat instans di Zona Ketersediaan yang sama dengan instans yang terpengaruh, Anda tidak akan dapat melampirkan volume root dari instans yang terpengaruh ke instans baru.

5. Pada panel navigasi, pilih Volume.
6. Cari volume root dari instans yang terpengaruh. Lepaskan volume dan pasang ke instans sementara yang Anda buat sebelumnya. Lampirkan dengan nama perangkat default (xvdf).
7. Gunakan Desktop Jarak Jauh untuk menyambung ke instans sementara, lalu gunakan utilitas Manajemen Disk agar volume tersedia untuk digunakan.
8. Buka prompt perintah dan jalankan perintah berikut. Ganti D dengan huruf drive sebenarnya dari volume sekunder yang baru saja Anda lampirkan:

   ```
   bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
   ```

9. Di Utilitas Manajemen Disk, pilih drive yang Anda pasang sebelumnya, buka menu konteks (klik kanan), dan pilih Offline.
10. Di konsol EC2, lepaskan volume yang terpengaruh dari instans sementara dan pasang kembali ke instans asli Anda dengan nama perangkat `/dev/sda1`. Anda harus menentukan nama perangkat ini untuk menetapkan volume sebagai volume root.
11. Mulai instans.
12. Setelah instans lulus pemeriksaan kondisi di konsol EC2, hubungkan ke instans menggunakan Desktop Jarak Jauh, dan verifikasi bahwa instans melakukan boot ke mode DSRM.
13. (Opsional) Hapus atau hentikan instans sementara yang Anda buat dalam prosedur ini.

Instans kehilangan konektivitas jaringan atau tugas terjadwal tidak berjalan saat diharapkan

Jika Anda memulai ulang instans dan kehilangan konektivitas jaringan, mungkin instans tersebut memiliki waktu yang salah.

Secara default, instans Windows menggunakan Waktu Universal Terkoordinasi (UTC). Jika Anda menyetel waktu pada instans ke zona waktu yang berbeda lalu memulai ulang, waktu tersebut menjadi offset dan instans kehilangan alamat IP-nya untuk sementara. Instans tersebut akhirnya mendapatkan kembali konektivitas jaringan, tetapi ini dapat memakan waktu beberapa jam. Jumlah waktu yang diperlukan instans untuk mendapatkan kembali konektivitas jaringan bergantung pada perbedaan antara UTC dan zona waktu lainnya.

Masalah waktu yang sama ini juga dapat mengakibatkan tugas terjadwal tidak berjalan seperti yang Anda harapkan. Dalam kasus ini, tugas terjadwal tidak berjalan sesuai harapan karena waktu instans salah.

Untuk menggunakan zona waktu selain UTC secara terus menerus, Anda harus menyetelRealTimeIsUniversal kunci registri. Tanpa kunci ini, instans akan menggunakan UTC setelah Anda memulai ulang.

Untuk mengatasi masalah waktu yang menyebabkan hilangnya konektivitas jaringan

1. Pastikan Anda menjalankan driver PV yang direkomendasikan. Untuk informasi selengkapnya, lihat the section called “Mutakhirkan driver PV”.
2. Verifikasi bahwa kunci registri berikut ada dan diatur ke1: HKEY_LOCAL_MACHINE\ SYSTEM\\ Control\\ CurrentControlSet TimeZoneInformation RealTimeIsUniversal

Tidak bisa mendapatkan output konsol

Pada instans Windows, konsol instans menampilkan output dari tugas-tugas yang dilakukan selama proses boot Windows. Jika Windows berhasil melakukan boot, pesan terakhir yang dicatat adalah `Windows is Ready to use`. Anda juga dapat menampilkan pesan log peristiwa di konsol, tetapi fitur ini mungkin tidak diaktifkan secara default tergantung pada versi Windows Anda. Untuk informasi selengkapnya, lihat the section called “Agen peluncuran Windows”.

Untuk mendapatkan output konsol pada instans Anda menggunakan konsol Amazon EC2, pilih instans, lalu pilih Tindakan, Pantau dan atasi masalah, Dapatkan log sistem. Untuk mendapatkan output konsol menggunakan baris perintah, gunakan salah satu perintah berikut: get-console-output(AWS CLI) atau Get-EC2ConsoleOutput(AWS Tools for Windows PowerShell).

Untuk contoh yang menjalankan Windows Server 2012 R2 dan sebelumnya, jika output konsol kosong, itu bisa menunjukkan masalah dengan layanan EC2 Config, seperti file konfigurasi yang salah konfigurasi, atau Windows gagal boot dengan benar. Untuk memperbaiki masalah ini, unduh dan instal EC2 Config versi terbaru. Untuk informasi selengkapnya, lihat the section called “Instal EC2 Config”.

Windows Server 2012 R2 tidak tersedia di jaringan

Untuk informasi tentang pemecahan masalah instans Windows Server 2012 R2 yang tidak tersedia di jaringan, lihat Windows Server 2012 R2 kehilangan konektivitas jaringan dan penyimpanan setelah instance reboot.

Tabrakan tanda tangan disk

Anda dapat memeriksa dan menyelesaikan tabrakan tanda tangan disk menggunakan EC2Rescue untuk Windows Server. Atau, Anda dapat mengatasi masalah tanda tangan disk secara manual dengan melakukan langkah-langkah berikut.

> **Warning**
>
> Prosedur berikut menjelaskan cara mengedit Windows Registry menggunakan Registry Editor. Jika Anda tidak terbiasa dengan Windows Registry atau cara membuat perubahan dengan aman menggunakan Registry Editor, lihat Konfigurasi Registry.

1. Buka prompt perintah, ketik regedit.exe, dan tekan Enter.

2. Di Registry Editor, pilih HKEY_LOCAL_MACHINE dari menu konteks (klik kanan), lalu pilih Temukan.
3. Ketik Windows Boot Manager, lalu pilih Temukan Berikutnya.
4. Pilih kunci bernama `11000001`. Kunci ini adalah kelompok dari kunci yang Anda temukan di langkah sebelumnya.
5. Pada panel kanan, pilih `Element`, lalu pilih Ubah dari menu konteks (klik kanan).
6. Temukan tanda tangan disk empat bita pada offset 0x38 dalam data tersebut. Ini adalah tanda tangan Boot Configuration Database (BCD). Balikkan bita tersebut untuk membuat tanda tangan disk, dan tuliskan. Misalnya, tanda tangan disk yang diwakili oleh data berikut ini adalah `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

7. Di jendela Command Prompt, jalankan perintah berikut untuk memulai Microsoft DiskPart.

```
diskpart
```

8. Jalankan `select disk` DiskPart perintah dan tentukan nomor disk untuk volume dengan tabrakan tanda tangan disk.

> **Tip**
>
> Untuk memeriksa nomor disk pada volume dengan tabrakan tanda tangan disk, gunakan utilitas Manajemen Disk. Buka prompt perintah, ketik `compmgmt.msc`, dan tekan Enter. Pada panel navigasi sebelah kiri, klik dua kali Manajemen Disk. Di utilitas Manajemen Disk, periksa nomor disk untuk volume offline dengan tabrakan tanda tangan disk.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Jalankan DiskPart perintah berikut untuk mendapatkan tanda tangan disk.

```
DISKPART>  uniqueid disk
```

```
Disk ID: 0C764FA8
```

10. Jika tanda tangan disk yang ditunjukkan pada langkah sebelumnya tidak cocok dengan tanda tangan disk yang Anda tulis sebelumnya, gunakan DiskPart perintah berikut untuk mengubah tanda tangan disk agar cocok:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Setel ulang kata sandi administrator Windows untuk instans Windows Amazon EC2

Jika Anda tidak lagi dapat terhubung ke instans Windows Amazon EC2 Anda karena kata sandi administrator Windows hilang atau kedaluwarsa, Anda dapat mengatur ulang kata sandi.

> **Note**
>
> Ada dokumen AWS Systems Manager Otomasi yang secara otomatis menerapkan langkah-langkah manual yang diperlukan untuk mengatur ulang kata sandi administrator lokal. Untuk informasi selengkapnya, lihat Mengatur ulang kata sandi dan kunci SSH pada instans EC2 di Panduan Pengguna.AWS Systems Manager

Metode manual untuk mengatur ulang kata sandi administrator menggunakan EC2 Launch v2, EC2 Config, atau EC2 Launch.

- Untuk semua Windows AMIs yang didukung yang menyertakan agen EC2 Launch v2, gunakan EC2 Launch v2.
- Untuk Windows AMIs sebelum Windows Server 2016, gunakan layanan EC2 Config.
- Untuk Windows Server 2016 dan yang lebih baru AMIs, gunakan layanan EC2 Peluncuran.

Prosedur ini juga menjelaskan cara terhubung ke instans jika Anda kehilangan pasangan kunci yang digunakan untuk membuat instans tersebut. Amazon EC2 menggunakan kunci publik untuk mengenkripsi sebuah data, seperti kata sandi, dan kunci privat untuk mendekripsi data. Kunci publik dan privat dikenal sebagai pasangan kunci. Dengan instans Windows, Anda dapat menggunakan pasangan kunci untuk mendapatkan kata sandi administrator, lalu masuk menggunakan RDP.

> **Note**
>
> Jika Anda telah menonaktifkan akun administrator lokal pada instans dan instans Anda dikonfigurasi untuk Systems Manager, Anda juga dapat mengaktifkan kembali dan mengatur ulang kata sandi administrator lokal Anda dengan menggunakan EC2 Rescue and Run Command. Untuk informasi selengkapnya, lihat Menggunakan EC2 Rescue untuk Windows Server dengan Systems Manager Run Command.

Daftar Isi

- Setel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Launch v2
- Setel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Launch
- Setel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Config

Setel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Launch v2

Jika Anda kehilangan kata sandi administrator Windows dan menggunakan AMI Windows yang didukung yang menyertakan agen EC2 Launch v2, Anda dapat menggunakan EC2 Launch v2 untuk menghasilkan kata sandi baru.

Jika Anda menggunakan AMI Windows Server 2016 atau yang lebih baru yang tidak menyertakan agen EC2 Launch v2, lihatSetel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Launch.

Jika Anda menggunakan AMI Windows Server lebih awal dari Windows Server 2016 yang tidak menyertakan agen EC2 Launch v2, lihatSetel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Config.

> **Note**
>
> Jika Anda telah menonaktifkan akun administrator lokal pada instans dan instans Anda dikonfigurasi untuk Systems Manager, Anda juga dapat mengaktifkan kembali dan mengatur ulang kata sandi administrator lokal Anda dengan menggunakan EC2 Rescue and Run Command. Untuk informasi selengkapnya, lihat Menggunakan EC2 Rescue untuk Windows Server dengan Systems Manager Run Command.

> **Note**
>
> Ada dokumen AWS Systems Manager Otomasi yang secara otomatis menerapkan langkah-langkah manual yang diperlukan untuk mengatur ulang kata sandi administrator lokal. Untuk informasi selengkapnya, lihat Mengatur ulang kata sandi dan kunci SSH pada instans EC2 di Panduan Pengguna.AWS Systems Manager

Untuk mengatur ulang kata sandi administrator Windows Anda menggunakan EC2 Launch v2, Anda perlu melakukan hal berikut:

- Langkah 1: Verifikasi bahwa agen EC2 Launch v2 sedang berjalan
- Langkah 2: Copot volume root dari instans
- Langkah 3: Lampirkan volume ke instans sementara
- Langkah 4: Hapus file .run-once
- Langkah 5: Mulai ulang instans asli

Langkah 1: Verifikasi bahwa agen EC2 Launch v2 sedang berjalan

Sebelum Anda mencoba mengatur ulang kata sandi administrator, verifikasi bahwa agen EC2 Launch v2 diinstal dan dijalankan. Anda menggunakan agen EC2 Launch v2 untuk mengatur ulang kata sandi administrator nanti di bagian ini.

Untuk memverifikasi bahwa agen EC2 Launch v2 sedang berjalan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih instans yang membutuhkan pengaturan ulang kata sandi. Instans ini dirujuk sebagai instans asli di dalam prosedur ini.
3. Pilih Tindakan, Pantau dan pecahkan masalah, Dapatkan log sistem .
4. Temukan entri Peluncuran EC2, misalnya, Launch: EC2 Launch v2 service v2.0.124. Jika Anda melihat entri ini, layanan EC2 Launch v2 sedang berjalan.

   Jika keluaran log sistem kosong, atau jika agen EC2 Launch v2 tidak berjalan, pecahkan masalah instance menggunakan layanan Screenshot Konsol Instans. Untuk informasi selengkapnya, lihat Mengambil tangkapan layar instans yang tidak dapat dijangkau.

Langkah 2: Copot volume root dari instans

Anda tidak dapat menggunakan EC2 Launch v2 untuk mengatur ulang kata sandi administrator jika volume penyimpanan kata sandi dilampirkan ke instance sebagai volume root. Anda harus mencopot volume dari instans asli sebelum dapat melampirkannya ke instans sementara sebagai volume sekunder.

Untuk mencopot volume root dari instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance yang memerlukan pengaturan ulang kata sandi dan pilih Status instans, Stop instance. Setelah status instans berubah menjadi Berhenti, lanjutkan dengan langkah berikutnya.
4. (Opsional) Jika Anda memiliki kunci privat yang Anda tentukan saat meluncurkan instans ini, lanjutkan dengan langkah berikutnya. Jika tidak, gunakan langkah-langkah berikut untuk mengganti instans dengan instans baru yang Anda luncurkan dengan sebuah pasangan kunci baru.
   a. Buatlah pasangan kunci baru menggunakan konsol Amazon EC2. Untuk memberikan nama pasangan kunci baru Anda sama seperti nama kunci privat yang hilang, Anda harus menghapus pasangan kunci yang sudah ada terlebih dahulu.
   b. Pilih instans yang ingin diganti. Catat tipe instans, VPC, subnet, grup keamanan, dan peran IAM dari instans.
   c. Dengan instance yang dipilih, pilih Actions, Image and templates, Create image. Ketikkan nama dan deskripsi untuk gambar dan pilih Buat gambar.
   d. Di panel navigasi, pilih AMIs. Tunggu status gambar berubah menjadi tersedia. Kemudian, pilih gambar dan pilih Launch instance dari AMI.
   e. Lengkapi bidang untuk meluncurkan instance, pastikan untuk memilih jenis instance yang sama, VPC, subnet, grup keamanan, dan peran IAM sebagai instance yang akan diganti, lalu pilih Launch instance.
   f. Saat diminta, pilih key pair yang Anda buat untuk instance baru, lalu pilih Launch instance.
   g. (Opsional) Jika instans asli memiliki alamat IP Elastis terkait, alihkan ke instans baru. Jika instans asli memiliki volume EBS selain volume root, alihkan ke instans baru.
5. Copot volume root dari instans asli dengan cara sebagai berikut:

a. Pilih instance asli dan pilih tab Storage. Perhatikan nama perangkat root di bawah nama perangkat Root. Temukan volume dengan nama perangkat ini di bawah Blokir perangkat, dan catat ID volume.

b. Pada panel navigasi, pilih Volume.

c. Dalam daftar volume, pilih volume yang Anda catat sebagai perangkat root, dan pilih Tindakan, Lepaskan Volume. Setelah status volume berubah menjadi tersedia, lanjutkan ke langkah berikutnya.

6. Jika Anda membuat instance baru untuk menggantikan instans asli Anda, Anda dapat menghentikan instance asli sekarang. Ini tidak lagi dibutuhkan. Untuk sisa prosedur ini, semua referensi ke instance asli berlaku untuk instance baru yang Anda buat.

Langkah 3: Lampirkan volume ke instans sementara

Selanjutnya, luncurkan instans sementara dan lampirkan volume ke instans tersebut sebagai volume sekunder. Ini adalah instans yang Anda gunakan untuk mengubah file konfigurasi.

Untuk meluncurkan sebuah instans sementara dan melampirkan volume

1. Luncurkan instans sementara dengan cara sebagai berikut:

a. Di panel navigasi, pilih Instans, pilih Luncurkan instans, lalu pilih AMI.

> **Important**
>
> Untuk menghindari tabrakan tanda tangan disk, Anda harus memilih AMI untuk versi Windows yang berbeda. Misalnya, jika instans asli menjalankan Windows Server 2019, luncurkan instans sementara menggunakan AMI dasar untuk Windows Server 2016.

b. Abaikan tipe instans default dan pilih Berikutnya: Konfigurasi Detail Instans.

c. Pada halaman Konfigurasi Detail Instans, untuk Subnet, pilih Zona Ketersediaan yang sama dengan instans asli dan pilih Tinjau dan Luncurkan.

> **Important**
>
> Instans sementara harus berada dalam Zona Ketersediaan yang sama dengan instans asli. Jika instans sementara Anda berada dalam Zona Ketersediaan yang berbeda, Anda tidak dapat melampirkan volume root instans asli ke instans tersebut.

d. Di halaman Tinjau Peluncuran Instans, pilih Luncurkan.

e. Jika diminta, buat pasangan kunci baru, unduh ke lokasi yang aman di komputer Anda, lalu pilih Luncurkan Instans.

2. Lampirkan volume ke instans sementara sebagai volume sekunder dengan cara sebagai berikut:

a. Di panel navigasi, pilih Volume, pilih volume yang ingin Anda copot dari instans asli, lalu pilih Tindakan, Lampirkan Volume.

b. Dalam kotak dialog Lampirkan Volume, untuk Instans, mulai untuk mengetikkan nama atau ID dari instans sementara Anda, lalu pilih instans dari daftar.

c. Untuk Perangkat, ketikkan **`xvdf`** (jika belum ada di sana), lalu pilih Lampirkan.

Langkah 4: Hapus file .run-once

Anda sekarang harus menghapus file `.run-once` dari volume offline yang dilampirkan ke instans. Ini mengarahkan EC2 Launch v2 untuk menjalankan semua tugas dengan frekuensi`once`, yang mencakup pengaturan kata sandi administrator. Jalur file di volume sekunder yang Anda lampirkan akan mirip dengan `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

Untuk menghapus file .run-once

1. Buka utilitas Manajemen Disk, dan bawa drive online menggunakan petunjuk ini: Buat volume Amazon EBS tersedia untuk digunakan.
2. Temukan lokasi file `.run-once` di disk yang Anda bawa online.
3. Hapus file .run-once.

> **Important**
>
> Skrip apa pun yang diatur untuk dijalankan sekali akan dipicu oleh tindakan ini.

Langkah 5: Mulai ulang instans asli

Setelah Anda menghapus file `.run-once`, lampirkan ulang volume ke instans asli sebagai volume root dan hubungkan ke instans menggunakan pasangan kuncinya untuk mengambil kata sandi administrator.

1. Lampirkan kembali volume ke instans asli dengan cara sebagai berikut:
   a. Di panel navigasi, pilih Volume, pilih volume yang ingin Anda copot dari instans sementara, lalu pilih Tindakan, Lampirkan Volume.
   b. Dalam kotak dialog Lampirkan Volume, untuk Instans, mulai untuk mengetikkan nama atau ID dari instans asli Anda, lalu pilih instans.
   c. Untuk Perangkat, ketikkan **`/dev/sda1`**.
   d. Pilih Lampirkan. Setelah status volume berubah menjadi `in-use`, lanjutkan ke langkah berikutnya.
2. Di panel navigasi, pilih Instans. Pilih instans asli dan pilih Status instans, Mulai instans. Setelah status instans berubah menjadi `Running`, lanjutkan ke langkah berikutnya.
3. Ambil kata sandi administrator Windows baru Anda menggunakan kunci privat untuk pasangan kunci baru dan hubungkan ke instans. Untuk informasi selengkapnya, lihat Hubungkan ke instans Windows Anda menggunakan RDP.

   > **Important**
   >
   > Instans tersebut mendapatkan alamat IP publik baru setelah Anda menghentikan dan memulainya. Pastikan untuk terhubung ke instans menggunakan nama DNS publiknya saat ini. Untuk informasi selengkapnya, lihat Perubahan status EC2 instans Amazon.

4. (Opsional) Jika Anda tidak menggunakan instans sementara lagi, Anda dapat mengakhirinya. Pilih instans sementara, dan pilih Status instans, Akhiri instans.

Setel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Launch

Jika Anda kehilangan kata sandi administrator Windows dan menggunakan AMI Windows Server 2016 atau yang lebih baru, Anda dapat menggunakan alat EC2 Penyelamatan, yang menggunakan layanan EC2 Peluncuran untuk menghasilkan kata sandi baru.

Jika Anda menggunakan AMI Windows Server 2016 atau yang lebih baru yang tidak menyertakan agen EC2 Launch v2, Anda dapat menggunakan EC2 Launch v2 untuk menghasilkan kata sandi baru.

Jika Anda menggunakan AMI Windows Server versi sebelumnya daripada Windows Server 2016, lihat Setel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Config.

Warning

Ketika Anda menghentikan sebuah instance, data pada volume penyimpanan instans akan hilang. Untuk menyimpan data ini, buat cadangan ke penyimpanan persisten.

Note

Jika Anda telah menonaktifkan akun administrator lokal pada instans dan instans Anda dikonfigurasi untuk Systems Manager, Anda juga dapat mengaktifkan kembali dan mengatur ulang kata sandi administrator lokal Anda dengan menggunakan EC2 Rescue and Run Command. Untuk informasi selengkapnya, lihat Menggunakan EC2 Rescue untuk Windows Server dengan Systems Manager Run Command.

Note

Ada dokumen AWS Systems Manager Otomasi yang secara otomatis menerapkan langkah-langkah manual yang diperlukan untuk mengatur ulang kata sandi administrator lokal. Untuk informasi selengkapnya, lihat Mengatur ulang kata sandi dan kunci SSH pada instans EC2 di Panduan Pengguna.AWS Systems Manager

Untuk mengatur ulang kata sandi administrator Windows Anda menggunakan EC2 Launch, Anda perlu melakukan hal berikut:

- Langkah 1: Copot volume root dari instans
- Langkah 2: Lampirkan volume ke instans sementara
- Langkah 3: Atur ulang kata sandi administrator
- Langkah 4: Mulai ulang instans asli

Langkah 1: Copot volume root dari instans

Anda tidak dapat menggunakan EC2 Launch untuk mengatur ulang kata sandi administrator jika volume penyimpanan kata sandi dilampirkan ke instance sebagai volume root. Anda harus mencopot volume dari instans asli sebelum dapat melampirkannya ke instans sementara sebagai volume sekunder.

Untuk mencopot volume root dari instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance yang memerlukan pengaturan ulang kata sandi dan pilih Status instans, Stop instance. Setelah status instans berubah menjadi Berhenti, lanjutkan dengan langkah berikutnya.
4. (Opsional) Jika Anda memiliki kunci privat yang Anda tentukan saat meluncurkan instans ini, lanjutkan dengan langkah berikutnya. Jika tidak, gunakan langkah-langkah berikut untuk mengganti instans dengan instans baru yang Anda luncurkan dengan sebuah pasangan kunci baru.
   a. Buatlah pasangan kunci baru menggunakan konsol Amazon EC2. Untuk memberikan nama pasangan kunci baru Anda sama seperti nama kunci privat yang hilang, Anda harus menghapus pasangan kunci yang sudah ada terlebih dahulu.
   b. Pilih instans yang ingin diganti. Catat tipe instans, VPC, subnet, grup keamanan, dan peran IAM dari instans.
   c. Dengan instance yang dipilih, pilih Actions, Image and templates, Create image. Ketikkan nama dan deskripsi untuk gambar dan pilih Buat gambar.
   d. Di panel navigasi, pilih AMIs. Tunggu status gambar berubah menjadi tersedia. Kemudian, pilih gambar dan pilih Launch instance dari AMI.
   e. Lengkapi bidang untuk meluncurkan instance, pastikan untuk memilih jenis instance yang sama, VPC, subnet, grup keamanan, dan peran IAM sebagai instance yang akan diganti, lalu pilih Launch instance.
   f. Saat diminta, pilih key pair yang Anda buat untuk instance baru, lalu pilih Launch instance.
   g. (Opsional) Jika instans asli memiliki alamat IP Elastis terkait, alihkan ke instans baru. Jika instans asli memiliki volume EBS selain volume root, alihkan ke instans baru.
5. Copot volume root dari instans asli dengan cara sebagai berikut:

a. Pilih instance asli dan pilih tab Storage. Perhatikan nama perangkat root di bawah nama perangkat Root. Temukan volume dengan nama perangkat ini di bawah Blokir perangkat, dan catat ID volume.

b. Pada panel navigasi, pilih Volume.

c. Dalam daftar volume, pilih volume yang Anda catat sebagai perangkat root, dan pilih Tindakan, Lepaskan Volume. Setelah status volume berubah menjadi tersedia, lanjutkan ke langkah berikutnya.

6. Jika Anda membuat instance baru untuk menggantikan instans asli Anda, Anda dapat menghentikan instance asli sekarang. Ini tidak lagi dibutuhkan. Untuk sisa prosedur ini, semua referensi ke instance asli berlaku untuk instance baru yang Anda buat.

Langkah 2: Lampirkan volume ke instans sementara

Selanjutnya, luncurkan instans sementara dan lampirkan volume ke instans tersebut sebagai volume sekunder. Ini adalah contoh yang Anda gunakan untuk menjalankan EC2 Launch.

Untuk meluncurkan sebuah instans sementara dan melampirkan volume

1. Luncurkan instans sementara dengan cara sebagai berikut:

a. Di panel navigasi, pilih Instans, pilih Luncurkan instans, lalu pilih AMI.

> **Important**
>
> Untuk menghindari tabrakan tanda tangan disk, Anda harus memilih AMI untuk versi Windows yang berbeda. Misalnya, jika instans asli menjalankan Windows Server 2019, luncurkan instans sementara menggunakan AMI dasar untuk Windows Server 2016.

b. Abaikan tipe instans default dan pilih Berikutnya: Konfigurasi Detail Instans.

c. Pada halaman Konfigurasi Detail Instans, untuk Subnet, pilih Zona Ketersediaan yang sama dengan instans asli dan pilih Tinjau dan Luncurkan.

> **Important**
>
> Instans sementara harus berada dalam Zona Ketersediaan yang sama dengan instans asli. Jika instans sementara Anda berada dalam Zona Ketersediaan yang berbeda, Anda tidak dapat melampirkan volume root instans asli ke instans tersebut.

d. Di halaman Tinjau Peluncuran Instans, pilih Luncurkan.

e. Jika diminta, buat pasangan kunci baru, unduh ke lokasi yang aman di komputer Anda, lalu pilih Luncurkan Instans.

2. Lampirkan volume ke instans sementara sebagai volume sekunder dengan cara sebagai berikut:

a. Di panel navigasi, pilih Volume, pilih volume yang ingin Anda copot dari instans asli, lalu pilih Tindakan, Lampirkan Volume.

b. Dalam kotak dialog Lampirkan Volume, untuk Instans, mulai untuk mengetikkan nama atau ID dari instans sementara Anda, lalu pilih instans dari daftar.

c. Untuk Perangkat, ketikkan **`xvdf`** (jika belum ada di sana), lalu pilih Lampirkan.

Langkah 3: Atur ulang kata sandi administrator

Selanjutnya, sambungkan ke instance sementara dan gunakan EC2 Luncurkan untuk mengatur ulang kata sandi administrator.

Untuk mengatur ulang kata sandi administrator

1. Connect ke instance sementara dan gunakan alat EC2 Rescue for Windows Server pada instance untuk mengatur ulang kata sandi administrator sebagai berikut:

a. Unduh file zip EC2Rescue for Windows Server, ekstrak isinya, dan jalankan EC2Rescue.exe.

b. Pada layar Perjanjian Lisensi, baca perjanjian lisensi, dan jika Anda menerima persyaratan, pilih Saya setuju.

c. Pada layar Selamat Datang untuk EC2 Penyelamatan untuk Windows Server, pilih Berikutnya.

d. Pada layar Pilih mode, pilih Instans offline.

e. Pada layar Pilih disk, pilih perangkat xvdf, lalu pilih Berikutnya.

f. Konfirmasi pilihan disk dan pilih Ya.

g. Setelah volume dimuat, pilih OKE.

h. Pada layar Pilih Opsi Instans Offline, pilih Diagnosis dan Penyelamatan.

i. Pada layar Ringkasan, tinjau informasi dan pilih Berikutnya.

j. Pada layar Kemungkinan masalah yang Terdeteksi, pilih Atur Ulang Kata Sandi Administrator, lalu pilih Berikutnya.

k. Pada layar Konfirmasi, pilih Selamatkan, OKE.

l. Pada layar Selesai, pilih Akir.

m. Tutup alat EC2Rescue for Windows Server, putuskan sambungan dari instans sementara, lalu kembali ke konsol Amazon EC2.

2. Copot volume (`xvdf`) sekunder dari instans asli seperti berikut ini:

a. Pada panel navigasi, pilih Instans dan pilih instans sementara.

b. Pada tab Penyimpanan untuk instans sementara, catat ID dari volume EBS yang terdaftar sebagai xvdf.

c. Pada panel navigasi, pilih Volume.

d. Dalam daftar volume, pilih volume yang dicatat di langkah sebelumnya, lalu pilih Tindakan, Copot Volume. Setelah status volume berubah menjadi tersedia, lanjutkan ke langkah berikutnya.

Langkah 4: Mulai ulang instans asli

Setelah Anda mengatur ulang kata sandi administrator menggunakan EC2 Launch, pasang kembali volume ke instance asli sebagai volume root dan sambungkan ke instance menggunakan key pair untuk mengambil kata sandi administrator.

Untuk memulai ulang instans asli

1. Lampirkan kembali volume ke instans asli dengan cara sebagai berikut:

a. Di panel navigasi, pilih Volume, pilih volume yang ingin Anda copot dari instans sementara, lalu pilih Tindakan, Lampirkan Volume.

b. Dalam kotak dialog Lampirkan Volume, untuk Instans, mulai untuk mengetikkan nama atau ID dari instans asli Anda, lalu pilih instans.

c. Untuk Perangkat, ketikkan **`/dev/sda1`**.

d. Pilih Lampirkan. Setelah status volume berubah menjadi `in-use`, lanjutkan ke langkah berikutnya.

2. Di panel navigasi, pilih Instans. Pilih instans asli dan pilih Status instans, Mulai instans. Setelah status instans berubah menjadi `Running`, lanjutkan ke langkah berikutnya.
3. Ambil kata sandi administrator Windows baru Anda menggunakan kunci privat untuk pasangan kunci baru dan hubungkan ke instans. Untuk informasi selengkapnya, lihat Hubungkan ke instans Windows Anda menggunakan RDP.
4. (Opsional) Jika Anda tidak menggunakan instans sementara lagi, Anda dapat mengakhirinya. Pilih instans sementara, dan pilih Status instans, Akhiri instans.

Setel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Config

Jika Anda kehilangan kata sandi administrator Windows dan menggunakan AMI Windows sebelum Windows Server 2016, Anda dapat menggunakan agen EC2 Config untuk menghasilkan kata sandi baru.

Jika Anda menggunakan AMI Windows Server 2016 atau yang lebih baru, lihat Setel ulang kata sandi admin Windows untuk instans EC2 menggunakan EC2 Launch atau, Anda dapat menggunakan alat EC2 Penyelamatan, yang menggunakan layanan EC2 Peluncuran untuk menghasilkan kata sandi baru.

> **Note**
>
> Jika Anda telah menonaktifkan akun administrator lokal pada instans dan instans Anda dikonfigurasi untuk Systems Manager, Anda juga dapat mengaktifkan kembali dan mengatur ulang kata sandi administrator lokal Anda dengan menggunakan EC2 Rescue and Run Command. Untuk informasi selengkapnya, lihat Menggunakan EC2 Rescue untuk Windows Server dengan Systems Manager Run Command.

> **Note**
>
> Ada dokumen AWS Systems Manager Otomasi yang secara otomatis menerapkan langkah-langkah manual yang diperlukan untuk mengatur ulang kata sandi administrator lokal. Untuk

informasi selengkapnya, lihat Mengatur ulang kata sandi dan kunci SSH pada instans EC2 di Panduan Pengguna.AWS Systems Manager

Untuk mengatur ulang kata sandi administrator Windows Anda menggunakan EC2 Config, Anda perlu melakukan hal berikut:

- Langkah 1: Verifikasi bahwa layanan EC2 Config sedang berjalan
- Langkah 2: Copot volume root dari instans
- Langkah 3: Lampirkan volume ke instans sementara
- Langkah 4: Ubah file konfigurasi
- Langkah 5: Mulai ulang instans asli

Langkah 1: Verifikasi bahwa layanan EC2 Config sedang berjalan

Sebelum Anda mencoba mengatur ulang kata sandi administrator, verifikasi bahwa layanan EC2 Config diinstal dan dijalankan. Anda menggunakan layanan EC2 Config untuk mengatur ulang kata sandi administrator nanti di bagian ini.

Untuk memverifikasi bahwa layanan EC2 Config sedang berjalan

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans, lalu pilih instans yang membutuhkan pengaturan ulang kata sandi. Instans ini dirujuk sebagai instans asli di dalam prosedur ini.
3. Pilih Actions, Monitor and troubleshoot, Get system log.
4. Temukan entri EC2 Agent, misalnya EC2 Agent: Ec2Config service v3.18.1118. Jika Anda melihat entri ini, layanan EC2 Config sedang berjalan.

   Jika keluaran log sistem kosong, atau jika layanan EC2 Config tidak berjalan, pecahkan masalah instance menggunakan layanan Screenshot Konsol Instans. Untuk informasi selengkapnya, lihat Mengambil tangkapan layar instans yang tidak dapat dijangkau.

Langkah 2: Copot volume root dari instans

Anda tidak dapat menggunakan EC2 Config untuk mengatur ulang kata sandi administrator jika volume penyimpanan kata sandi dilampirkan ke instance sebagai volume root. Anda harus mencopot

volume dari instans asli sebelum dapat melampirkannya ke instans sementara sebagai volume sekunder.

Untuk mencopot volume root dari instans

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.
3. Pilih instance yang memerlukan pengaturan ulang kata sandi dan pilih Status instans, Stop instance. Setelah status instans berubah menjadi Berhenti, lanjutkan dengan langkah berikutnya.
4. (Opsional) Jika Anda memiliki kunci privat yang Anda tentukan saat meluncurkan instans ini, lanjutkan dengan langkah berikutnya. Jika tidak, gunakan langkah-langkah berikut untuk mengganti instans dengan instans baru yang Anda luncurkan dengan sebuah pasangan kunci baru.

    a. Buatlah pasangan kunci baru menggunakan konsol Amazon EC2. Untuk memberikan nama pasangan kunci baru Anda sama seperti nama kunci privat yang hilang, Anda harus menghapus pasangan kunci yang sudah ada terlebih dahulu.

    b. Pilih instans yang ingin diganti. Catat tipe instans, VPC, subnet, grup keamanan, dan peran IAM dari instans.

    c. Dengan instance yang dipilih, pilih Actions, Image and templates, Create image. Ketikkan nama dan deskripsi untuk gambar dan pilih Buat gambar.

    d. Di panel navigasi, pilih AMIs. Tunggu status gambar berubah menjadi tersedia. Kemudian, pilih gambar dan pilih Launch instance dari AMI.

    e. Lengkapi bidang untuk meluncurkan instance, pastikan untuk memilih jenis instance yang sama, VPC, subnet, grup keamanan, dan peran IAM sebagai instance yang akan diganti, lalu pilih Launch instance.

    f. Saat diminta, pilih key pair yang Anda buat untuk instance baru, lalu pilih Launch instance.

    g. (Opsional) Jika instans asli memiliki alamat IP Elastis terkait, alihkan ke instans baru. Jika instans asli memiliki volume EBS selain volume root, alihkan ke instans baru.

5. Copot volume root dari instans asli dengan cara sebagai berikut:

    a. Pilih instance asli dan pilih tab Storage. Perhatikan nama perangkat root di bawah nama perangkat Root. Temukan volume dengan nama perangkat ini di bawah Blokir perangkat, dan catat ID volume.

    b. Pada panel navigasi, pilih Volume.

c. Dalam daftar volume, pilih volume yang Anda catat sebagai perangkat root, dan pilih Tindakan, Lepaskan Volume. Setelah status volume berubah menjadi tersedia, lanjutkan ke langkah berikutnya.

6. Jika Anda membuat instance baru untuk menggantikan instans asli Anda, Anda dapat menghentikan instance asli sekarang. Ini tidak lagi dibutuhkan. Untuk sisa prosedur ini, semua referensi ke instance asli berlaku untuk instance baru yang Anda buat.

Langkah 3: Lampirkan volume ke instans sementara

Selanjutnya, luncurkan instans sementara dan lampirkan volume ke instans tersebut sebagai volume sekunder. Ini adalah instans yang Anda gunakan untuk mengubah file konfigurasi.

Untuk meluncurkan sebuah instans sementara dan melampirkan volume

1. Luncurkan instans sementara dengan cara sebagai berikut:

   a. Di panel navigasi, pilih Instans, pilih Luncurkan instans, lalu pilih AMI.

   > **Important**
   >
   > Untuk menghindari tabrakan tanda tangan disk, Anda harus memilih AMI untuk versi Windows yang berbeda. Misalnya, jika instans asli menjalankan Windows Server 2019, luncurkan instans sementara menggunakan AMI dasar untuk Windows Server 2016.

   b. Abaikan tipe instans default dan pilih Berikutnya: Konfigurasi Detail Instans.

   c. Pada halaman Konfigurasi Detail Instans, untuk Subnet, pilih Zona Ketersediaan yang sama dengan instans asli dan pilih Tinjau dan Luncurkan.

   > **Important**
   >
   > Instans sementara harus berada dalam Zona Ketersediaan yang sama dengan instans asli. Jika instans sementara Anda berada dalam Zona Ketersediaan yang berbeda, Anda tidak dapat melampirkan volume root instans asli ke instans tersebut.

   d. Di halaman Tinjau Peluncuran Instans, pilih Luncurkan.

   e. Jika diminta, buat pasangan kunci baru, unduh ke lokasi yang aman di komputer Anda, lalu pilih Luncurkan Instans.

2. Lampirkan volume ke instans sementara sebagai volume sekunder dengan cara sebagai berikut:

   a. Di panel navigasi, pilih Volume, pilih volume yang ingin Anda copot dari instans asli, lalu pilih Tindakan, Lampirkan Volume.

   b. Dalam kotak dialog Lampirkan Volume, untuk Instans, mulai untuk mengetikkan nama atau ID dari instans sementara Anda, lalu pilih instans dari daftar.

   c. Untuk Perangkat, ketikkan **`xvdf`** (jika belum ada di sana), lalu pilih Lampirkan.

Langkah 4: Ubah file konfigurasi

Setelah Anda melampirkan volume ke instans sementara sebagai volume sekunder, ubah plugin `Ec2SetPassword` di file konfigurasi.

Untuk mengubah file konfigurasi

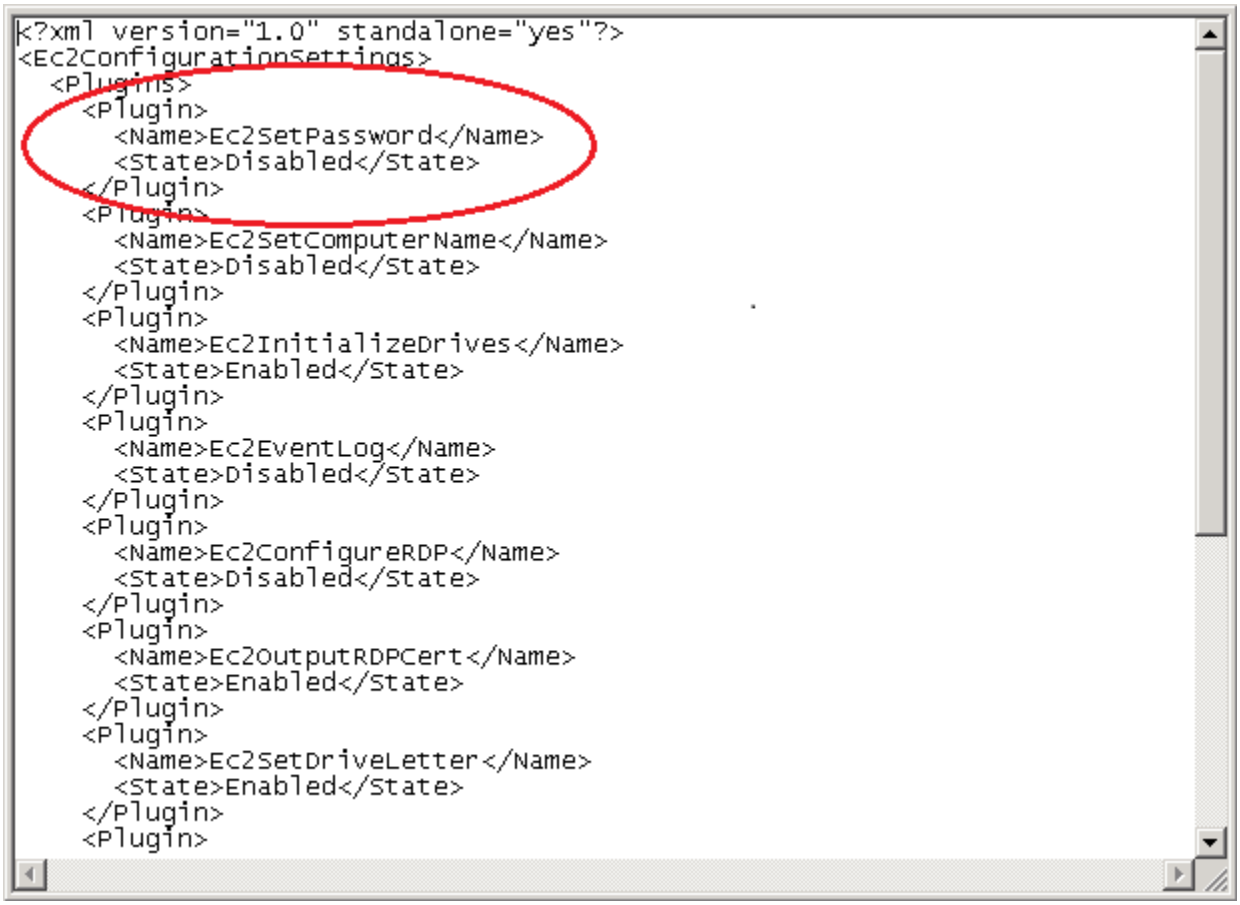
1. Dari instans sementara, ubah file konfigurasi pada volume sekunder dengan cara seperti berikut:

   a. Luncurkan dan hubungkan ke instans sementara.

   b. Gunakan petunjuk berikut untuk membawa drive online: Buat volume Amazon EBS tersedia untuk digunakan.

   c. Lakukan navigasi pada volume sekunder, dan buka `\Program Files\Amazon \Ec2ConfigService\Settings\config.xml` menggunakan editor teks, seperti Notepad.

   d. Pada bagian atas file, temukan plugin dengan nama `Ec2SetPassword`, seperti yang ditunjukkan dalam screenshot. Ubah status dari `Disabled` ke `Enabled`, lalu simpan file.



2. Setelah mengubah file konfigurasi, copot volume sekunder dari instans sementara dengan cara seperti berikut:

   a. Menggunakan utitlitas Manajemen Disk, yang membuat volume menjadi offline.

   b. Putuskan sambungan dari instans sementara lalu kembali ke konsol Amazon EC2.

   c. Dalam panel navigasi, pilih Volume, pilih volume, lalu pilih Tindakan, Copot Volume. Setelah status volume berubah menjadi tersedia, lanjutkan dengan langkah berikutnya.

Langkah 5: Mulai ulang instans asli

Setelah Anda mengubah file konfigurasi, lampirkan ulang volume ke instans asli sebagai volume root dan hubungkan ke instans menggunakan pasangan kuncinya untuk mengambil kata sandi administrator.

1. Lampirkan kembali volume ke instans asli dengan cara sebagai berikut:

   a. Di panel navigasi, pilih Volume, pilih volume yang ingin Anda copot dari instans sementara, lalu pilih Tindakan, Lampirkan Volume.

b. Dalam kotak dialog Lampirkan Volume, untuk Instans, mulai untuk mengetikkan nama atau ID dari instans asli Anda, lalu pilih instans.

c. Untuk Perangkat, ketikkan **`/dev/sda1`**.

d. Pilih Lampirkan. Setelah status volume berubah menjadi `in-use`, lanjutkan ke langkah berikutnya.

2. Di panel navigasi, pilih Instans. Pilih instans asli dan pilih Status instans, Mulai instans. Setelah status instans berubah menjadi `Running`, lanjutkan ke langkah berikutnya.
3. Ambil kata sandi administrator Windows baru Anda menggunakan kunci privat untuk pasangan kunci baru dan hubungkan ke instans. Untuk informasi selengkapnya, lihat Hubungkan ke instans Windows Anda menggunakan RDP.

> **Important**
>
> Instans tersebut mendapatkan alamat IP publik baru setelah Anda menghentikan dan memulainya. Pastikan untuk terhubung ke instans menggunakan nama DNS publiknya saat ini. Untuk informasi selengkapnya, lihat Perubahan status EC2 instans Amazon.

4. (Opsional) Jika Anda tidak menggunakan instans sementara lagi, Anda dapat mengakhirinya. Pilih instans sementara, dan pilih Status instans, Akhiri instans.

Memecahkan masalah Sysprep dengan instans Windows Amazon EC2

Jika Anda mengalami masalah atau menerima pesan kesalahan selama persiapan gambar, tinjau log berikut ini. Lokasi log bervariasi tergantung pada apakah Anda menjalankan EC2 Config, EC2 Launch v1, atau Launch v2 dengan EC2 Sysprep.

- `%WINDIR%\Panther\Unattendgc`(EC2Config, EC2 Luncurkan v1, dan EC2 Luncurkan v2)
- `%WINDIR%\System32\Sysprep\Panther`(EC2Config, EC2 Luncurkan v1, dan EC2 Luncurkan v2)
- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt`(EC2Hanya Config)
- `C:\ProgramData\Amazon\Ec2Config\Logs`(EC2Hanya Config)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log`(Hanya EC2 Luncurkan v1)

- `%ProgramData%\Amazon\EC2Launch\log\agent.log`(Hanya EC2 Luncurkan v2)

Jika Anda menerima pesan kesalahan selama persiapan gambar dengan Sysprep, OS mungkin tidak dapat dijangkau. Untuk meninjau file log, Anda harus menghentikan instans, melampirkan volume root-nya ke instans sehat lainnya sebagai volume sekunder, lalu meninjau log yang disebutkan sebelumnya di volume sekunder. Untuk informasi selengkapnya tentang tujuan file log berdasarkan nama, lihat File Log Terkait Penataan Windows di dokumentasi Microsoft.

Jika Anda menemukan kesalahan di file log Unattendgc, gunakan Alat Pencarian Kesalahan Microsoft untuk mendapatkan detail selengkapnya tentang kesalahan tersebut. Masalah berikut yang dilaporkan di file log Unattendgc biasanya disebabkan oleh satu atau beberapa profil pengguna yang rusak pada instans:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Ada dua opsi untuk menyelesaikan masalah ini:

Opsi 1

Gunakan Regedit pada instans untuk mencari kunci berikut. Verifikasi bahwa tidak ada kunci registri profil untuk pengguna yang dihapus.

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\`

Opsi 2

1. Edit file yang relevan, sebagai berikut:
   - Windows Server 2012 R2 dan sebelumnya - Edit file `C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml` jawaban EC2 Config ().
   - Windows Server 2016 dan 2019 - Edit file jawaban unattend.xml (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).
   - Windows Server 2022 - Edit file jawaban unattend.xml (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).
2. Ubah `<CopyProfile>true</CopyProfile>` ke `<CopyProfile>false</CopyProfile>`.
3. Jalankan lagi Syspre. Perhatikan bahwa perubahan konfigurasi ini akan menghapus profil pengguna administrator bawaan setelah Sysprep selesai.

Memecahkan masalah instans Amazon EC2 Linux yang terganggu menggunakan Rescue EC2

EC2Rescue untuk Linux adalah alat sumber terbuka yang dapat dijalankan pada instans Amazon EC2 Linux untuk mendiagnosis, memecahkan masalah, dan memperbaiki masalah umum menggunakan pustaka lebih dari 100 modul. easy-to-use Modul adalah file YAMG yang berisi skrip BASH atau Python dan metadata yang diperlukan.

Beberapa kasus penggunaan umum untuk instance EC2 Rescue for Linux meliputi:

- Mengumpulkan log syslog dan manajer paket
- Mengumpulkan data pemanfaatan sumber daya
- Mendiagnosis dan memulihkan parameter kernel bermasalah yang diketahui dan masalah umum OpenSSH

> **Note**
>
> Runbook `AWSSupport-TroubleshootSSH` AWS Systems Manager Otomasi menginstal EC2 Rescue untuk Linux dan kemudian menggunakan alat untuk memeriksa atau mencoba memperbaiki masalah umum yang mencegah koneksi SSH ke instance Linux. Untuk informasi selengkapnya, lihat AWSSupport-TroubleshootSSH.

Jika Anda menggunakan instance Windows, lihatthe section called “EC2Rescue untuk instance Windows”.

Topik

- Instal EC2Rescue pada instans Amazon EC2 Linux
- Jalankan perintah EC2Rescue pada instans Amazon EC2 Linux
- Mengembangkan modul EC2Rescue untuk instans Amazon EC2 Linux

Instal EC2Rescue pada instans Amazon EC2 Linux

Alat EC2Rescue untuk Linux dapat diinstal pada instans Amazon EC2 Linux yang memenuhi prasyarat berikut.

Prasyarat

- Sistem operasi yang didukung:
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7+
  - Ubuntu 16.04+
- Persyaratan perangkat lunak:
  - Python 2.7.9+ atau 3.2+

Instal EC2 Rescue

`AWSSupport-TroubleshootSSH`Runbook menginstal EC2 Rescue untuk Linux dan kemudian menggunakan alat untuk memeriksa atau mencoba memperbaiki masalah umum yang mencegah koneksi jarak jauh ke mesin Linux melalui SSH. Untuk informasi lebih lanjut, dan untuk menjalankan otomatisasi ini, lihat Dukungan-TroubleshootSSH.

Jika sistem Anda memiliki versi Python yang diperlukan, Anda dapat menginstal build standar. Jika tidak, Anda dapat menginstal paket build, yang menyertakan salinan minimal Python.

Untuk menginstal build standar

1. Dari instance Linux yang berfungsi, unduh alat EC2Rescue for Linux:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
   ```

2. (Opsional) Verifikasi tanda tangan file instalasi EC2 Rescue for Linux. Untuk informasi selengkapnya, lihat (Opsional) Verifikasi tanda tangan EC2 Rescue untuk Linux.
3. Unduh file sha256 hash:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
   ```

4. Verifikasi integritas tarball:

   ```
   sha256sum -c ec2rl.tgz.sha256
   ```

5. Buka kemasan tarball:

```
tar -xzvf ec2rl.tgz
```

6. Verifikasi instalasi dengan mencantumkan file bantuan:

```
cd ec2rl-<version_number>
./ec2rl help
```

Untuk menginstal paket build

Untuk tautan ke unduhan dan daftar batasan, lihat EC2Rescue for Linux di github.

(Opsional) Verifikasi tanda tangan EC2 Rescue untuk Linux

Berikut ini adalah proses yang direkomendasikan untuk memverifikasi validitas paket EC2 Rescue for Linux untuk sistem operasi berbasis Linux.

Saat Anda mengunduh aplikasi dari internet, kami menyarankan Anda untuk mengautentikasi identitas penerbit perangkat lunak dan memeriksa apakah aplikasi tersebut belum diubah atau rusak setelah diterbitkan. Hal ini akan melindungi Anda agar tidak menginstal versi aplikasi yang berisi virus atau kode berbahaya lainnya.

Jika, setelah menjalankan langkah-langkah dalam topik ini, Anda menentukan bahwa perangkat lunak untuk EC2 Rescue for Linux diubah atau rusak, jangan jalankan file instalasi. Alih-alih, hubungi Amazon Web Services.

EC2Rescue untuk file Linux untuk sistem operasi berbasis Linux ditandatangani menggunakan GnuPG, implementasi open-source dari standar Pretty Good Privacy (OpenPGP) untuk tanda tangan digital yang aman. GnuPG (juga dikenal sebagai GPG) menyediakan otentikasi dan pemeriksaan integritas melalui tanda tangan digital. AWS menerbitkan kunci publik dan tanda tangan yang dapat Anda gunakan untuk memverifikasi paket EC2 Rescue for Linux yang diunduh. Untuk informasi lebih lanjut tentang PGP dan GnuPG (GPG), lihat https://www.gnupg.org/.

Langkah pertamanya adalah membangun kepercayaan dengan penerbit perangkat lunak. Unduh kunci publik dari penerbit perangkat lunak, periksa apakah pemilik kunci publik adalah benar-benar pemiliknya, lalu tambahkan kunci publik ke dalam keyring Anda. Keyring adalah kumpulan kunci publik yang diketahui. Setelah menetapkan autentikasi kunci publik, Anda dapat menggunakannya untuk memverifikasi tanda tangan aplikasi.

Tugas

- Autentikasi dan impor kunci publik
- Memverifikasi tanda tangan paket

Autentikasi dan impor kunci publik

Langkah selanjutnya dalam proses ini adalah mengautentikasi kunci publik EC2 Rescue for Linux dan menambahkannya sebagai kunci tepercaya di keyring GPG Anda.

Untuk mengautentikasi dan mengimpor kunci publik EC2 Rescue for Linux

1. Pada prompt perintah, gunakan perintah berikut untuk mendapatkan salinan kunci publik build GPG kami:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
   ```

2. Pada prompt perintah di direktori tempat Anda menyimpan`ec2rl.key`, gunakan perintah berikut untuk mengimpor kunci publik EC2 Rescue for Linux ke keyring Anda:

   ```
   gpg2 --import ec2rl.key
   ```

   Perintah tersebut akan mengembalikan hasil yang serupa dengan berikut ini:

   ```
   gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
   gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
    imported
   gpg: Total number processed: 1
   gpg:               imported: 1  (RSA: 1)
   ```

   > **Tip**
   >
   > Jika Anda melihat kesalahan yang menyatakan bahwa perintah tidak dapat ditemukan, instal utilitas GnuPG `apt-get install gnupg2` dengan (Linux berbasis Debian) `yum install gnupg2` atau (Linux berbasis Red Hat).

Memverifikasi tanda tangan paket

Setelah Anda menginstal alat GPG, mengautentikasi dan mengimpor kunci publik EC2 Rescue for Linux, dan memverifikasi bahwa kunci publik EC2 Rescue for Linux dipercaya, Anda siap untuk memverifikasi tanda tangan skrip instalasi EC2 Rescue for Linux.

Untuk memverifikasi tanda tangan skrip instalasi EC2 Rescue for Linux

1. Pada prompt perintah, jalankan perintah berikut untuk mengunduh file tanda tangan untuk skrip instalasi:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Verifikasi tanda tangan dengan menjalankan perintah berikut pada prompt perintah di direktori tempat Anda menyimpan `ec2rl.tgz.sig` dan file instalasi EC2 Rescue for Linux. Kedua file tersebut harus ada.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

   Output-nya akan terlihat seperti berikut ini:

   ```
   gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
   gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
        Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
   ```

   Jika output berisi frasa`Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, itu berarti tanda tangan telah berhasil diverifikasi, dan Anda dapat melanjutkan untuk menjalankan skrip instalasi EC2 Rescue for Linux.

   Jika output berisi frasa `BAD signature`, periksa apakah Anda melakukan prosedur dengan benar. Jika Anda terus mendapatkan respons ini, hubungi Amazon Web Services dan jangan menjalankan file instalasi yang Anda unduh sebelumnya.

Berikut ini adalah informasi peringatan yang mungkin Anda lihat:

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner.Ini mengacu pada tingkat kepercayaan pribadi Anda dalam keyakinan Anda bahwa Anda memiliki kunci publik otentik untuk EC2 Penyelamatan untuk Linux. Idealnya, Anda harus mendatangi kantor Amazon Web Services dan menerima kunci secara langsung. Namun, kemungkinan besar Anda akan mengunduhnya dari situs web. Dalam hal ini, situs web yang dimaksud adalah situs web Amazon Web Services .
- gpg2: no ultimately trusted keys found. Ini berarti bahwa kunci tersebut tidak "benar-benar tepercaya" oleh Anda (atau orang lain yang Anda percayai).

Untuk informasi lebih lanjut, lihat https://www.gnupg.org/.

Jalankan perintah EC2Rescue pada instans Amazon EC2 Linux

EC2Penyelamatan adalah alat baris perintah. Setelah Anda menginstal EC2 Rescue pada instance Linux Anda, Anda bisa mendapatkan bantuan umum tentang cara menggunakan alat dengan menjalankannya `./ec2rl help`. Anda dapat melihat modul yang tersedia dengan menjalankan `./ec2rl list`, dan Anda bisa mendapatkan bantuan pada modul tertentu dengan menjalankan `./ec2rl help` *`module_name`*.

Berikut ini adalah tugas umum yang dapat Anda lakukan untuk mulai menggunakan alat ini.

Tugas

- Jalankan modul EC2 Rescue
- Unggah hasil modul EC2 Rescue
- Membuat cadangan instans Amazon EC2 Linux

Jalankan modul EC2 Rescue

Untuk menjalankan semua modul EC2 Rescue

Gunakan ./ec2rl run perintah tanpa menentukan parameter tambahan apa pun. Beberapa modul memerlukan akses root. Jika Anda bukan pengguna root, gunakan sudo saat Anda menjalankan perintah.

```
./ec2rl run
```

Untuk menjalankan modul EC2 Rescue tertentu

Gunakan ./ec2rl run perintah dan untuk`--only-modules`, tentukan nama modul yang akan dijalankan. Beberapa modul memerlukan argumen untuk menggunakannya.

```
./ec2rl run --only-modules=module_name --arguments
```

Misalnya, untuk menjalankan dig modul untuk query `amazon.com` domain, gunakan perintah berikut.

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Untuk melihat hasil dari modul EC2 Rescue

Jalankan modul lalu lihat file log di`cat /var/tmp/ec2rl/logfile_location`. Misalnya, file log untuk dig modul dapat ditemukan di lokasi berikut:

```
cat /var/tmp/ec2rl/timestamp/mod_out/run/dig.log
```

Unggah hasil modul EC2 Rescue

Jika Dukungan telah meminta hasil untuk modul EC2 Penyelamatan, Anda dapat mengunggah file log menggunakan alat EC2 Penyelamatan. Anda dapat mengunggah hasilnya ke lokasi yang disediakan oleh Dukungan atau ke bucket Amazon S3 yang Anda miliki.

Untuk mengunggah hasil ke lokasi yang disediakan oleh Dukungan

Gunakan perintah ./ec2rl upload. Untuk`--upload-directory`, tentukan lokasi file log. Untuk`--support-url`, tentukan URL yang disediakan oleh Dukungan.

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --support-
url="url_provided_by_aws_support"
```

Untuk mengunggah hasil ke bucket Amazon S3

Gunakan perintah ./ec2rl upload. Untuk`--upload-directory`, tentukan lokasi file log. Untuk`--presigned-url`, tentukan URL yang telah ditetapkan sebelumnya untuk bucket S3. Untuk informasi selengkapnya tentang membuat pra-ditandatangani URLs untuk Amazon S3, lihat Mengunggah Objek Menggunakan Pra-Tanda Tangan. URLs

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --presigned-
url="presigned_s3_url"
```

Membuat cadangan instans Amazon EC2 Linux

Anda dapat menggunakan EC2 Rescue untuk mencadangkan instance Linux Anda dengan membuat AMI atau dengan membuat snapshot dari volume terlampirnya.

Untuk membuat AMI

Gunakan `./ec2rl run` perintah dan untuk `--backup`, tentukan`ami`.

```
./ec2rl run --backup=ami
```

Untuk membuat snapshot multi-volume dari semua volume terlampir

Gunakan `./ec2rl run` perintah dan untuk `--backup`, tentukan`allvolumes`.

```
./ec2rl run --backup=allvolumes
```

Untuk membuat snapshot dari volume terlampir tertentu

Gunakan `./ec2rl run` perintah dan untuk `--backup`, tentukan ID volume yang akan dicadangkan.

```
./ec2rl run --backup=vol-01234567890abcdef
```

Mengembangkan modul EC2Rescue untuk instans Amazon EC2 Linux

Modul ditulis dalam YAML, yaitu standar serialisasi data. File YAML pada sebuah modul terdiri atas satu dokumen yang mewakili modul dan atributnya.

Menambahkan atribut modul

Tabel berikut menjelaskan atribut modul yang tersedia.

Atribut	Deskripsi
nama	Nama modul. Nama harus berisi 18 karakter atau kurang.
version	Nomor versi modul.

Atribut	Deskripsi
title	Judul singkat dan deskriptif untuk modul. Panjang judul harus berisi 50 karakter atau kurang.

helptext	Deskripsi modul yang lebih panjang. Setiap baris harus berisi 75 karakter atau kurang. Jika modul menggunakan argumen, yang bersifat wajib atau opsional, sertakan argumen tersebut dalam nilai teks bantuan.
	
	Misalnya:
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

placement	Tahap ketika modul harus dijalankan. Nilai yang didukung: • prediagnostic • run • postdiagnostic

Atribut	Deskripsi
language	Bahasa yang digunakan untuk menuliskan kode modul. Nilai yang didukung: • bash • python **Note** Kode Python harus kompatibel dengan Python 2.7.9+ maupun Python 3.2+.
remediation	Menunjukkan apakah modul mendukung remediasi. Nilai yang didukung adalah `True` atau `False`. Secara default, modul menjadi `False` jika hal ini tidak ada, sehingga membuatnya menjadi atribut opsional untuk modul yang tidak mendukung remediasi.
content	Keseluruhan kode skrip.
constraint	Nama objek yang berisi nilai kendala.
domain	Penjelasan tentang cara modul dikelompokkan atau diklasifikasikan. Rangkaian modul yang disertakan menggunakan domain berikut: • application • net • os • performance

Atribut	Deskripsi
class	Penjelasan tentang tipe tugas yang dilakukan oleh modul. Rangkaian modul yang disertakan menggunakan domain berikut: • collect (mengambil output dari program) • diagnose (lulus/gagal berdasarkan serangkai an kriteria) • gather (menyalin file dan menulis ke file tertentu)
distro	Daftar distribusi Linux yang didukung oleh modul ini. Rangkaian modul yang disertakan menggunakan distribusi berikut: • alami (Amazon Linux) • rhel • ubuntu • suse
diperlukan	Argumen wajib yang digunakan oleh modul dari opsi CLI.
optional	Argumen opsional yang dapat digunakan oleh modul.
software	Perangkat lunak yang dapat dieksekusi yang digunakan di dalam modul. Atribut ini ditujukan untuk menentukan perangkat lunak yang tidak terinstal secara default. Logika EC2 Rescue for Linux memastikan bahwa program-program ini hadir dan dapat dieksekusi sebelum menjalank an modul.

Atribut	Deskripsi
package	Paket perangkat lunak sumber untuk file yang dapat dieksekusi. Atribut ini ditujukan untuk memberikan detail tambahan pada paket dengan perangkat lunak, termasuk URL untuk mengunduh atau mendapatkan informasi lebih lanjut.
sudo	Mengindikasikan apakah akses root diperlukan untuk menjalankan modul. Anda tidak perlu menerapkan pengecekan sudo dalam skrip modul. Jika nilainya benar, maka logika EC2 Rescue for Linux hanya menjalankan modul ketika pengguna yang mengeksekusi memiliki akses root.
perfimpact	Mengindikasikan apakah modul dapat menimbulkan dampak performa yang signifikan terhadap lingkungan tempat modul dijalankan. Jika nilainya benar dan argumen `--perfimpact=true` tidak ada, modul akan dilewati.
parallelexclusive	Menentukan program yang membutuhkan eksklusivitas bersama. Misalnya, semua modul yang menentukan proses "bpf" dijalankan secara bersambung.

Menambahkan variabel lingkungan

Tabel berikut menjelaskan variabel lingkungan yang tersedia.

Variabel Lingkungan	Deskripsi
EC2RL_CALLPATH	Path ke ec2rl.py. Path ini dapat digunakan untuk menemukan direktori lib dan menggunakan modul Python yang bervendor.
EC2RL_WORKDIR	Direktori tmp utama untuk alat diagnostik. Nilai default: /var/tmp/ec2rl .
EC2RL_RUNDIR	Direktori tempat semua output disimpan. Nilai default: /var/tmp/ec2rl/<date&timestamp> .
EC2RL_GATHEREDDIR	Direktori root untuk menempatkan data modul yang dikumpulkan. Nilai default:/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/ .
EC2RL_NET_DRIVER	Driver yang digunakan untuk antarmuka jaringan non-virtual pertama yang diurutkan menurut abjad pada instans. Contoh: • xen_netfront • ixgbevf • ena
EC2RL_SUDO	Benar jika EC2 Rescue untuk Linux berjalan sebagai root; jika tidak, false.
EC2RL_VIRT_TYPE	Tipe virtualisasi seperti yang disediakan oleh metadata instans. Contoh:

Variabel Lingkungan	Deskripsi
	• default-hvm • default-paravirtual
`EC2RL_INTERFACES`	Daftar antarmuka yang disebutkan pada sistem. Nilai tersebut adalah string yang berisi nama, seperti `eth0`, `eth1`, dan lain-lain. Ini dibuat melalui `functions.bash` dan hanya tersedia untuk modul yang bersumber darinya.

Menggunakan sintaks YAML

Hal-hal berikut ini harus diperhatikan saat menyusun file YAML modul Anda:

- Tiga tanda hubung (`---`) menunjukkan awal yang jelas dari suatu dokumen.
- Tanda `!ec2rlcore.module.Module` memberi tahu pengurai YAML konstruktor mana yang akan dipanggil saat membuat objek dari aliran data. Anda dapat menemukan konstruktor di dalam file `module.py`.
- Tanda `!!str` memberi tahu pengurai YAML untuk tidak mencoba menentukan tipe data, dan sebagai gantinya menginterpretasikan konten sebagai literal string.
- Simbol garis lurus (`|`) memberi tahu pengurai YAML bahwa nilainya adalah skalar gaya literal. Dalam hal ini, pengurai menyertakan semua spasi. Ini penting untuk modul karena indentasi dan karakter baris baru disimpan.
- Indentasi standar YAML adalah dua spasi, yang dapat dilihat pada contoh berikut. Pastikan Anda mempertahankan indentasi standar (misalnya, empat spasi untuk Python) untuk skrip Anda dan kemudian menunjukkan seluruh konten dua spasi di dalam file modul.

Contoh modul

Contoh satu (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
```

```
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Memecahkan masalah instans Windows Amazon EC2 yang terganggu menggunakan Rescue EC2

EC2Rescue untuk Windows Server adalah easy-to-use alat yang Anda jalankan pada instans Amazon EC2 Windows Server untuk mendiagnosis dan memecahkan masalah yang mungkin terjadi. Ini berguna untuk mengumpulkan file log dan memecahkan masalah, juga mencari kemungkinan area yang menjadi permasalahan secara proaktif. Ini juga dapat memeriksa volume root Amazon EBS dari instans lain dan mengumpulkan log yang relevan untuk memecahkan masalah instans Windows Server menggunakan volume tersebut. Berikut ini adalah beberapa masalah umum yang dapat diatasi oleh EC2 Rescue:

- Masalah konektivitas instans karena firewall, Remote Desktop Protocol (RDP), atau konfigurasi antarmuka jaringan
- Masalah boot sistem operasi karena kesalahan berhenti, loop boot, atau registri rusak
- Masalah yang mungkin memerlukan analisis log lanjutan dan pemecahan masalah

EC2Rescue untuk Windows Server memiliki dua modul berbeda:

- Modul pengumpul data yang mengumpulkan data dari semua sumber yang berbeda
- Modul analyzer yang mem-parsing data yang dikumpulkan terhadap serangkaian aturan yang telah ditetapkan untuk mengidentifikasi masalah dan memberikan saran

Alat EC2Rescue untuk Windows Server hanya berjalan pada instans Amazon EC2 yang menjalankan Windows Server 2012 dan yang lebih baru. Saat dimulai, alat akan memeriksa apakah ia beroperasi di instans Amazon EC2 atau bukan.

> **Note**
>
> Runbook `AWSSupport-ExecuteEC2Rescue` AWS Systems Manager Otomasi menggunakan alat EC2Rescue untuk memecahkan masalah dan, jika memungkinkan, memperbaiki masalah konektivitas umum dengan instans EC2 yang ditentukan. Untuk informasi selengkapnya, dan untuk menjalankan otomatisasi ini, lihat > AWSSupport-ExecuteEC 2Rescue.

Jika Anda menggunakan instance Linux, lihatthe section called “EC2Penyelamatan untuk instance Linux”.

Topik

- Memecahkan masalah instans Windows yang rusak dengan GUI Penyelamatan EC2
- Memecahkan masalah instance Windows yang rusak dengan Rescue EC2 CLI
- Memecahkan masalah instans Windows yang rusak dengan EC2 Rescue and Systems Manager

Memecahkan masalah instans Windows yang rusak dengan GUI Penyelamatan EC2

EC2Rescue untuk Windows Server dapat melakukan analisis berikut pada instance offline:

Opsi	Deskripsi

Diagnosis dan Penyelamatan	EC2Rescue untuk Windows Server dapat mendeteksi dan mengatasi masalah dengan pengaturan layanan berikut:
	• Waktu Sistem
	  • RealTimeisUniversal - Mendeteksi apakah kunci registri `RealTimeisUniversal` diaktifkan. Jika dinonaktifkan, waktu sistem Windows menyimpang saat zona waktu disetel ke nilai selain UTC.
	• Windows Firewall
	  • Jaringan domain - Mendeteksi apakah profil Windows Firewall ini diaktifkan atau dinonaktifkan.
	  • Jaringan pribadi - Mendeteksi apakah profil Windows Firewall ini diaktifkan atau dinonaktifkan.

Opsi	Deskripsi

	• Jaringan tamu atau publik - Mendeteksi apakah profil Windows Firewall ini diaktifkan atau dinonaktifkan.
	
	• Desktop Jarak Jauh
	  • Mulai Layanan - Mendeteksi apakah layanan Desktop Jarak Jauh diaktifkan.
	  • Koneksi Desktop Jarak Jauh - Mendeteksi apakah fitur ini diaktifkan.
	  • Port TCP - Mendeteksi port mana yang mendengarkan layanan Desktop Jarak Jauh.
	
	• EC2Config (Windows Server 2012 R2 dan sebelumnya)
	  • Instalasi - Mendeteksi versi EC2 Config mana yang diinstal.
	  • Service Start - Mendeteksi apakah layanan EC2 Config diaktifkan.
	  • Ec2 SetPassword - Menghasilkan kata sandi administrator baru.
	  • HandleUserDataEc2 - Memungkinkan Anda menjalankan skrip data pengguna pada boot berikutnya dari instance.
	
	• EC2Peluncuran (Windows Server 2016 dan yang lebih baru)
	  • Instalasi - Mendeteksi versi EC2 Peluncuran mana yang diinstal.
	  • Ec2 SetPassword - Menghasilkan kata sandi administrator baru.

Opsi	Deskripsi

	• Antarmuka Jaringan
	  • Startup Layanan DHCP - Mendeteksi apakah layanan DHCP diaktifkan atau dinonaktifkan.
	  • Detail ethernet - Menampilkan informasi tentang versi driver jaringan, jika terdeteksi.
	  • DHCP di Ethernet - Mendeteksi apakah DHCP diaktifkan atau dinonaktifkan.
	• Status tanda tangan disk
	  • Tanda tangan pada disk dan Tanda tangan pada Boot Configuration Database (BCD) - Mendeteksi apakah tanda tangan disk dan tanda tangan BCD sama atau tidak. Jika nilainya berbeda, EC2 Rescue mencoba menimpa tanda tangan disk dengan tanda tangan pada BCD.

Pulihkan	Lakukan salah satu tindakan berikut: • Konfigurasi Baik yang Terakhir Diketahui - Berupaya melakukan boot instans ke status terakhir yang diketahui dapat melakukan boot. • Pulihkan registri dari cadangan - Memulihkan registri dari `\Windows\System32\config\RegBack` .
Menangkap Log	Memungkinkan Anda untuk menangkap log pada instans untuk analisis.

EC2Rescue untuk Windows Server dapat mengumpulkan data berikut dari instans aktif dan offline:

Item	Deskripsi
Log Peristiwa	Mengumpulkan log peristiwa aplikasi, sistem, dan EC2 Config.
Registri	Mengumpulkan hive `SYSTEM` dan `SOFTWARE`.
Log Pembaruan Windows	Mengumpulkan file log yang dihasilkan oleh Pembaruan Windows. **Note** Di Windows Server 2016 dan versi yang lebih baru, log dikumpulkan dalam format Pelacakan Peristiwa untuk Windows (ETW).
Log Sysprep	Mengumpulkan file log yang dihasilkan oleh alat Windows System Preparation.
Log Pengaturan Driver	Mengumpulkan log Windows SetupAPI (`setupapi.dev.log` dan `setupapi.setup.log`).
Konfigurasi Boot	Mengumpulkan hive `HKEY_LOCAL_MACHINE\BCD00000000`.
Dump Memori	Mengumpulkan file dump memori yang ada pada instans.
EC2Berkas Config	Mengumpulkan file log yang dihasilkan oleh layanan EC2 Config.
EC2Luncurkan File	Mengumpulkan file log yang dihasilkan oleh skrip EC2 Launch.
File Agen SSM	Mengumpulkan file log yang dihasilkan oleh Agen SSM dan log Patch Manager.

Item	Deskripsi
File Elastis GPUs EC2	Mengumpulkan log peristiwa yang terkait dengan elastis GPUs.
ECS	Kumpulkan log terkait ke Amazon ECS.
CloudEndure	Mengumpulkan file log yang terkait dengan CloudEndure Agen.
AWS Agen Replikasi untuk File Log MGN atau DRS	Mengumpulkan file log yang terkait dengan AWS Application Migration Service atau AWS Elastic Disaster Recovery.

EC2Rescue untuk Windows Server dapat mengumpulkan data tambahan berikut dari instans aktif:

Item	Deskripsi
Informasi Sistem	Mengumpulkan. MSInfo32
Hasil Kebijakan Grup	Mengumpulkan laporan Kebijakan Grup.

Analisis instans offline

Opsi Instans Offline berguna untuk mendebug permasalahan booting dengan instans Windows.

Untuk melakukan tindakan pada instans offline

1. Dari instance Windows Server yang berfungsi, unduh alat EC2Rescue for Windows Server dan ekstrak file.

   Anda dapat menjalankan PowerShell perintah berikut untuk mengunduh EC2 Rescue tanpa mengubah Internet Explorer Enhanced Security Configuration (ESC) Anda:

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

Perintah ini akan mengunduh file EC2 Rescue.zip ke desktop pengguna yang saat ini masuk.

> **Note**
>
> Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016 atau yang lebih lama, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

2. Hentikan instans yang bermasalah, jika belum dihentikan.
3. Lepaskan volume root EBS dari instance yang salah dan lampirkan volume ke instance Windows yang berfungsi yang telah menginstal EC2 Rescue for Windows Server.
4. Jalankan alat EC2 Rescue for Windows Server pada instance kerja dan pilih Instans Offline.
5. Pilih disk volume yang baru dipasang dan pilih Berikutnya.
6. Konfirmasi pilihan disk dan pilih Ya.
7. Pilih opsi instans offline untuk dijalankan dan pilih Berikutnya.

Alat EC2 Rescue for Windows Server memindai volume dan mengumpulkan informasi pemecahan masalah berdasarkan file log yang dipilih.

Mengumpulkan data dari instans yang aktif

Anda dapat mengumpulkan log dan data lain dari instans yang aktif.

Untuk mengumpulkan data dari instans yang aktif

1. Hubungkan ke instans Anda.
2. Unduh alat EC2Rescue for Windows Server ke instance Windows Anda dan ekstrak file.

   Anda dapat menjalankan PowerShell perintah berikut untuk mengunduh EC2 Rescue tanpa mengubah Internet Explorer Enhanced Security Configuration (ESC) Anda:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Perintah ini akan mengunduh file EC2 Rescue.zip ke desktop pengguna yang saat ini masuk.

> **Note**
>
> Jika Anda menerima kesalahan saat mengunduh file, dan Anda menggunakan Windows Server 2016 atau yang lebih lama, TLS 1.2 mungkin perlu diaktifkan untuk PowerShell terminal Anda. Anda dapat mengaktifkan TLS 1.2 untuk PowerShell sesi saat ini dengan perintah berikut dan kemudian coba lagi:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

3. Buka aplikasi EC2 Rescue for Windows Server dan terima perjanjian lisensi.
4. Pilih Berikutnya, Instans saat ini, Tangkap log.
5. Pilih item data yang akan dikumpulkan dan pilih Kumpulkan.... Baca peringatan dan pilih Ya untuk melanjutkan.
6. Pilih nama file dan lokasi untuk file ZIP, lalu pilih Simpan.
7. Setelah EC2 Rescue untuk Windows Server selesai, pilih Open Connecting Folder untuk melihat file ZIP.
8. Pilih Selesai.

Memecahkan masalah instance Windows yang rusak dengan Rescue EC2 CLI

Antarmuka baris perintah EC2 Rescue for Windows Server (CLI) memungkinkan Anda menjalankan plugin EC2 Rescue for Windows Server (disebut sebagai “tindakan”) secara terprogram.

Alat EC2 Penyelamatan untuk Windows Server memiliki dua mode eksekusi:

- /online —Ini memungkinkan Anda untuk mengambil tindakan pada contoh bahwa EC2 Rescue untuk Windows Server diinstal pada, seperti mengumpulkan file log.

- /offline: <device_id>—Ini memungkinkan Anda untuk mengambil tindakan pada volume root offline yang dilampirkan ke instance Windows Amazon EC2 terpisah, di mana Anda telah EC2 menginstal Rescue untuk Windows Server.

Unduh alat EC2Rescue for Windows Server EC2 EC2 untuk Windows Server ke instance Windows Anda dan ekstrak file. Anda dapat melihat file bantuan menggunakan perintah berikut:

```
EC2RescueCmd.exe /help
```

EC2Rescue untuk Windows Server dapat melakukan tindakan berikut pada instans Windows Amazon EC2:

- Tindakan pengumpulan
- Tindakan penyelamatan
- Tindakan pemulihan

Tindakan pengumpulan

> **Note**
>
> Anda dapat mengumpulkan semua log, seluruh grup log, atau satu log individu di dalam sebuah grup.

EC2Rescue untuk Windows Server dapat mengumpulkan data berikut dari instans aktif dan offline.

Grup log	Log yang tersedia	Deskripsi
`all`		Kumpulkan semua log yang tersedia.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Mengumpulkan log peristiwa aplikasi, sistem, dan EC2 Config.

Grup log	Log yang tersedia	Deskripsi
`memory-dump`	• `'Memory Dump File'` • `'Mini Dump Files'`	Mengumpulkan file pembuangan memori yang ada pada instans.
`ec2config`	• `'Log Files'` • `'Configuration Files'`	Mengumpulkan file log yang dihasilkan oleh layanan EC2 Config.
`ec2launch`	• `'Logs'` • `'Config'`	Mengumpulkan file log yang dihasilkan oleh skrip EC2 Launch.
`ssm-agent`	• `'Log Files'` • `'Patch Baseline Logs'` • `'InstanceData'`	Mengumpulkan file log yang dihasilkan oleh SSM Agent dan log Patch Manager.
`sysprep`	`'Log Files'`	Mengumpulkan file log yang dihasilkan oleh alat Windows System Preparation.
`driver-setup`	• `'SetupAPI Log Files'` • `'DPInst Log File'` • `'AWS PV Setup Log File'`	Mengumpulkan log Windows SetupAPI (`setupapi.dev.log` dan `setupapi.setup.log`).
`registry`	• `'SYSTEM'` • `'SOFTWARE'` • `'BCD'`	Mengumpulkan hive `SYSTEM` dan `SOFTWARE`.
`egpu`	• `'Event Log'` • `'System Files'`	Mengumpulkan log peristiwa yang terkait dengan elastis GPUs.

Grup log	Log yang tersedia	Deskripsi
`boot-config`	`'BCDEDIT Output'`	Mengumpulkan hive `HKEY_LOCAL_MACHINE \BCD00000000` .
`windows-update`	`'Log Files'`	Mengumpulkan file log yang dihasilkan oleh Windows Update. **Note** Di Windows Server 2016 dan lebih baru, log dikumpulkan dalam format Pelacakan Peristiwa untuk Windows (ETW).
`cloudendure`	• `'Migrate Script Logs'` • `'Driver Logs'` • `'CloudEndure File List'`	Mengumpulkan file log yang terkait dengan CloudEndure Agen.

EC2Rescue untuk Windows Server dapat mengumpulkan data tambahan berikut dari instans aktif.

Grup log	Log yang tersedia	Deskripsi
`system-info`	`'MSInfo32 Output'`	Kumpulkan `MSInfo32`.
`gpresult`	`'GPResult Output'`	Mengumpulkan laporan Kebijakan Grup.

Berikut ini adalah opsi yang tersedia:

- /output:<outputFilePath> - Lokasi jalur file tujuan yang diperlukan untuk menyimpan file log yang dikumpulkan dalam format zip.
- /no-offline - Atribut opsional yang digunakan dalam mode offline. Tidak menetapkan volume secara offline setelah menyelesaikan tindakan.
- /no-fix-signature- Atribut opsional yang digunakan dalam mode offline. Tidak memperbaiki kemungkinan tabrakan tanda tangan disk setelah menyelesaikan tindakan.

Contoh

Berikut ini adalah contoh menggunakan EC2 Rescue for Windows Server CLI.

Contoh mode online

Kumpulkan semua log yang tersedia:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Hanya mengumpulkan grup log tertentu:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Kumpulkan log individu di dalam grup log:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Contoh mode offline

Kumpulkan semua log yang tersedia dari volume EBS. Volume ditentukan oleh nilai device_id.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Hanya kumpulkan grup log tertentu:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Tindakan penyelamatan

EC2Rescue untuk Windows Server dapat mendeteksi dan mengatasi masalah dengan pengaturan layanan berikut:

Grup layanan	Tindakan yang tersedia	Deskripsi
`all`		
`system-time`	`'RealTimeIsUniversal'`	Waktu Sistem • RealTimeisUniversal - Mendeteksi apakah kunci registri `RealTimeisUniversal` diaktifkan. Jika dinonaktifkan, waktu sistem Windows menyimpang saat zona waktu disetel ke nilai selain UTC.
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Windows Firewall • Jaringan domain - Mendeteksi apakah profil Windows Firewall ini diaktifkan atau dinonaktifkan. • Jaringan pribadi - Mendeteksi apakah profil Windows Firewall ini diaktifkan atau dinonaktifkan. • Jaringan tamu atau publik - Mendeteksi apakah profil Windows Firewall ini diaktifkan atau dinonaktifkan.

Grup layanan	Tindakan yang tersedia	Deskripsi
rdp	• 'Service Start' • 'Remote Desktop Connections' • 'TCP Port'	Desktop Jarak Jauh • Mulai Layanan - Mendeteksi apakah layanan Desktop Jarak Jauh diaktifkan. • Koneksi Desktop Jarak Jauh - Mendeteksi apakah fitur ini diaktifkan. • Port TCP - Mendeteksi port mana yang mendengarkan layanan Desktop Jarak Jauh.
ec2config	• 'Service Start' • 'Ec2SetPassword' • 'Ec2HandleUserData'	EC2Config • Service Start - Mendeteksi apakah layanan EC2 Config diaktifkan. • Ec2 SetPassword - Menghasilkan kata sandi administrator baru. • HandleUserDataEc2 - Memungkinkan Anda menjalankan skrip data pengguna pada boot berikutnya dari instance.
ec2launch	'Reset Administrator Password'	Buat kata sandi administrator Windows baru.
network	'DHCP Service Startup'	Antarmuka Jaringan • DHCP Service Startup - Mendeteksi apakah layanan DHCP diaktifkan.

Berikut ini adalah opsi yang tersedia:

- /level:<level> - Atribut opsional untuk tingkat pemeriksaan yang harus dipicu oleh tindakan tersebut. Nilai yang diizinkan adalah: `information`, `warning`, `error`, `all`. Secara default, nilainya diatur ke `error`.
- /check-only - Atribut opsional yang menghasilkan laporan tetapi tidak melakukan modifikasi terhadap volume offline.

> **Note**
>
> Jika EC2 Rescue untuk Windows Server mendeteksi kemungkinan tabrakan tanda tangan disk, itu mengoreksi tanda tangan setelah proses offline selesai secara default, bahkan ketika Anda menggunakan opsi. `/check-only` Anda harus menggunakan `/no-fix-signature` opsi untuk mencegah koreksi.

- /no-offline - Atribut opsional yang mencegah volume agar tidak diatur offline setelah menyelesaikan tindakan.
- /no-fix-signature- Atribut opsional yang tidak memperbaiki kemungkinan tabrakan tanda tangan disk setelah menyelesaikan tindakan.

Contoh penyelamatan

Berikut ini adalah contoh menggunakan EC2 Rescue for Windows Server CLI. Volume ditentukan menggunakan nilai device_id.

Upayakan untuk memperbaiki semua masalah yang teridentifikasi pada volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Upayakan untuk memperbaiki semua masalah di dalam grup layanan pada volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Upayakan untuk memperbaiki item tertentu di dalam grup layanan pada volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Tentukan banyak masalah yang akan dicoba diperbaiki pada volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Tindakan pemulihan

EC2Rescue untuk Windows Server dapat mendeteksi dan mengatasi masalah dengan pengaturan layanan berikut:

Grup Layanan	Tindakan yang Tersedia	Deskripsi
Memulihkan Konfigurasi Baik yang Terakhir Diketahui	`lkgc`	Konfigurasi Baik yang Terakhir Diketahui - Berupaya melakukan booting instans ke kondisi terakhir yang diketahui dapat melakukan boot.
Memulihkan registri Windows dari cadangan terbaru	`regback`	Pulihkan registri dari cadangan - Memulihkan registri dari `\Windows\System32\config\RegBack .`

Berikut ini adalah opsi yang tersedia:

- /no-offline - Atribut opsional yang mencegah volume agar tidak diatur offline setelah menyelesaikan tindakan.
- /no-fix-signature—Atribut opsional yang tidak memperbaiki kemungkinan tabrakan tanda tangan disk setelah menyelesaikan tindakan.

Contoh pemulihan

Berikut ini adalah contoh menggunakan EC2 Rescue for Windows Server CLI. Volume ditentukan menggunakan nilai device_id.

Memulihkan konfigurasi baik yang terakhir diketahui pada volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Pulihkan cadangan registri Windows terakhir pada volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Memecahkan masalah instans Windows yang rusak dengan EC2 Rescue and Systems Manager

Dukungan menyediakan dokumen Systems Manager Run Command untuk berinteraksi dengan instans Systems Manager-enabled Anda untuk menjalankan EC2 Rescue for Windows Server. Dokumen Run Command ini disebut `AWSSupport-RunEC2RescueForWindowsTool`.

Dokumen Systems Manager Run Command ini melakukan tugas-tugas berikut:

- Mengunduh dan memverifikasi EC2 Rescue untuk Windows Server.
- Mengimpor PowerShell modul untuk memudahkan interaksi Anda dengan alat ini.
- Berjalan EC2 RescueCmd dengan perintah dan parameter yang disediakan.

Dokumen Systems Manager Run Command menerima tiga parameter:

- Perintah —Tindakan EC2 Penyelamatan untuk Windows Server. Nilai-nilai yang diizinkan saat ini adalah:
  - ResetAccess—Mengatur ulang kata sandi Administrator lokal. Kata sandi Administrator lokal dari instans saat ini akan diatur ulang dan kata sandi yang dihasilkan secara acak akan disimpan dengan aman di Penyimpanan Parameter sebagai `/EC2Rescue/Password/<INSTANCE_ID>`. Jika Anda memilih tindakan ini dan tidak memberikan parameter, kata sandi akan dienkripsi secara otomatis dengan kunci KMS default. Secara opsional, Anda dapat menentukan ID Kunci KMS di Parameter untuk mengenkripsi kata sandi dengan kunci Anda sendiri.
  - CollectLogs—Menjalankan EC2 Rescue untuk Windows Server dengan `/collect:all` tindakan. Jika Anda memilih tindakan ini, `Parameters` harus menyertakan nama bucket Amazon S3 untuk mengunggah log ke dalamnya.
  - FixAll—Menjalankan EC2 Rescue untuk Windows Server dengan `/rescue:all` tindakan. Jika Anda memilih tindakan ini, `Parameters` harus menyertakan nama perangkat blok untuk penyelamatan.
- Parameter PowerShell —Parameter yang harus diteruskan untuk perintah yang ditentukan.

Persyaratan

Untuk menjalankan ResetAccesstindakan, instans Amazon EC2 Anda harus memiliki kebijakan yang dilampirkan yang memberikan izin untuk menulis kata sandi terenkripsi ke Parameter Store. Setelah melampirkan kebijakan, tunggu beberapa menit sebelum mencoba mengatur ulang kata sandi suatu instans setelah Anda melampirkan kebijakan ini ke peran IAM terkait.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

Jika Anda menggunakan kunci KMS kustom, bukan kunci KMS default, gunakan kebijakan ini sebagai gantinya.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
```

```
        "arn:aws:ssm:us-east-1:111122223333:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/<kmskeyid>"
      ]
    }
  ]
}
```

Lihat JSON untuk dokumen

Prosedur berikut menjelaskan cara melihat JSON untuk dokumen ini.

Untuk menampilkan JSON pada dokumen Systems Manager Run Command

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, perluas Alat Manajemen Ubah dan pilih Dokumen.
3. Di bilah pencarian, masukkan`AWSSupport-RunEC2RescueForWindowsTool`, lalu pilih `AWSSupport-RunEC2RescueForWindowsTool` dokumen.
4. Pilih tab Daftar Isi.

Contoh

Berikut adalah beberapa contoh tentang cara menggunakan dokumen Systems Manager Run Command untuk menjalankan EC2 Rescue for Windows Server, menggunakan file AWS CLI. Untuk informasi selengkapnya tentang mengirim perintah menggunakan perintah AWS CLI, lihat send-command.

Contoh

- Upayakan untuk memperbaiki semua masalah yang teridentifikasi pada volume root offline
- Kumpulkan log dari instans Windows Amazon EC2 saat ini

- Atur ulang kata sandi Administrator lokal

Upayakan untuk memperbaiki semua masalah yang teridentifikasi pada volume root offline

Upayakan untuk memperbaiki semua masalah yang teridentifikasi pada volume root offline yang dilampirkan pada instans Amazon EC2 Windows:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=FixAll, Parameters='xvdf'" --output
 text
```

Kumpulkan log dari instans Windows Amazon EC2 saat ini

Kumpulkan semua log dari instans Windows Amazon EC2 online saat ini dan unggah ke bucket Amazon S3:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=CollectLogs, Parameters='amzn-s3-
demo-bucket'" --output text
```

Atur ulang kata sandi Administrator lokal

Contoh berikut menunjukkan metode yang dapat Anda gunakan untuk mengatur ulang kata sandi Administrator lokal. Output ini menyediakan tautan ke Penyimpanan Parameter, di mana Anda dapat menemukan kata sandi yang aman dan dibuat secara acak, yang kemudian dapat Anda gunakan untuk RDP ke instans Windows Amazon EC2 sebagai Administrator lokal.

Setel ulang kata sandi Administrator lokal dari instans online menggunakan default AWS KMS key alias/aws/ssm:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=ResetAccess" --output text
```

Atur ulang kata sandi Administrator lokal untuk instans online menggunakan kunci KMS:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=ResetAccess, Parameters=a133dc3c-
a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> Dalam contoh ini, kunci KMS adalah `a133dc3c-a2g4-4fc6-a873-6c0720104bf0`.

EC2 Serial Console untuk instans

Dengan konsol serial EC2, Anda memiliki akses ke port serial instans Amazon EC2, yang dapat digunakan untuk memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya. Konsol serial tidak memerlukan instans Anda untuk memiliki kemampuan jaringan. Dengan konsol serial, Anda dapat memasukkan perintah ke sebuah instans seolah-olah keyboard dan monitor Anda terpasang secara langsung ke port serial instans. Sesi konsol serial berlangsung selama boot ulang dan penghentian instans. Selama boot ulang, Anda dapat melihat semua pesan boot dari awal.

Akses ke konsol serial tidak tersedia secara default. Organisasi Anda harus memberikan akses akun ke konsol serial dan mengonfigurasi kebijakan IAM untuk memberi pengguna akses ke konsol serial tersebut. Akses konsol serial dapat dikontrol pada tingkat granular dengan menggunakan instance IDs, tag sumber daya, dan tuas IAM lainnya. Untuk informasi selengkapnya, lihat Konfigurasikan akses ke Konsol Serial EC2.

Konsol serial dapat diakses menggunakan konsol EC2 atau AWS CLI.

Konsol serial tersedia tanpa biaya tambahan.

Topik

- Prasyarat untuk Konsol Serial EC2
- Konfigurasikan akses ke Konsol Serial EC2
- Hubungkan ke Konsol Serial EC2
- Memutuskan koneksi dari Konsol Serial EC2
- Memecahkan masalah instans Amazon EC2 Anda menggunakan Konsol Serial EC2

Prasyarat untuk Konsol Serial EC2

Untuk terhubung ke Konsol Serial EC2 dan menggunakan alat yang Anda pilih untuk pemecahan masalah, prasyarat berikut harus dipenuhi:

- Wilayah AWS

- Zona Wavelength dan Outposts AWS
- Zona Lokal
- Tipe instans
- Berikan akses
- Dukungan untuk klien berbasis peramban
- Status instans
- Amazon EC2 Systems Manager
- Konfigurasikan alat pemecahan masalah yang Anda pilih

Wilayah AWS

Didukung di semua Wilayah AWS kecuali Asia Pasifik (Taipei).

Zona Wavelength dan Outposts AWS

Tidak didukung.

Zona Lokal

Didukung di semua Local Zones.

Tipe instans

Tipe instans yang didukung:

- Linux
  - Semua instans virtual dibangun pada Nitro System.
  - Semua instans bare metal kecuali:
    - Tujuan umum: `a1.metal`, `mac1.metal`, `mac2.metal`
    - Komputasi yang dipercepat: `g5g.metal`
    - Memori yang dioptimalkan: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, `u-24tb1.metal`
- Windows

  Semua instans virtual dibangun pada Nitro System. Instans bare metal tidak didukung.

Berikan akses

Anda harus menyelesaikan tugas konfigurasi untuk memberikan akses ke Konsol Serial EC2. Untuk informasi selengkapnya, lihat Konfigurasikan akses ke Konsol Serial EC2.

Dukungan untuk klien berbasis peramban

Untuk terhubung ke konsol serial menggunakan klien berbasis browser, browser Anda harus mendukung. WebSocket Jika browser Anda tidak mendukung WebSocket, sambungkan ke konsol serial menggunakan kunci Anda sendiri dan klien SSH.

Status instans

Harus berupa `running`.

Anda tidak dapat terhubung ke konsol serial jika instans berada dalam status `pending`, `stopping`, `stopped`, `shutting-down`, atau `terminated`.

Untuk informasi selengkapnya tentang status instans, lihat Perubahan status EC2 instans Amazon.

Amazon EC2 Systems Manager

Jika instans menggunakan Amazon EC2 Systems Manager, Agen SSM versi 3.0.854.0 atau yang lebih baru harus diinstal pada instans tersebut. Untuk informasi tentang Agen SSM, lihat Bekerja dengan Agen SSM di Panduan Pengguna AWS Systems Manager .

Konfigurasikan alat pemecahan masalah yang Anda pilih

Untuk memecahkan masalah instans Anda menggunakan konsol serial, Anda dapat menggunakan GRUB atau instans Linux, dan Konsol Admin Khusus (SAC) SysRq pada instance Windows. Sebelum dapat menggunakan alat ini, Anda harus terlebih dahulu melakukan langkah-langkah konfigurasi pada setiap instans di tempat Anda akan menggunakannya.

Gunakan instruksi untuk sistem operasi instans Anda untuk mengonfigurasi alat pemecahan masalah yang Anda pilih.

(Instans Linux) Konfigurasikan GRUB

Untuk mengonfigurasi GRUB, pilih salah satu dari prosedur berikut berdasarkan AMI yang digunakan untuk meluncurkan instans.

Amazon Linux 2

Untuk mengonfigurasi GRUB pada instans Amazon Linux 2

1. Hubungkan ke instans Linux Anda, menggunakan SSH.
2. Tambahkan atau ubah pilihan berikut dalam `/etc/default/grub`:
   - Atur `GRUB_TIMEOUT=1`.
   - Tambahkan `GRUB_TERMINAL="console serial"`.
   - Tambahkan `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Berikut adalah contoh `/etc/default/grub`. Anda mungkin perlu mengubah konfigurasi berdasarkan pengaturan sistem.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
   GRUB_TIMEOUT=1
   GRUB_DISABLE_RECOVERY="true"
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```
3. Terapkan konfigurasi yang diperbarui dengan menjalankan perintah berikut.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

Ubuntu

Untuk mengonfigurasi GRUB pada instans Ubuntu

1. Terhubung ke instans Anda.
2. Tambahkan atau ubah pilihan berikut dalam `/etc/default/grub.d/50-cloudimg-settings.cfg`:
   - Atur `GRUB_TIMEOUT=1`.
   - Tambahkan `GRUB_TIMEOUT_STYLE=menu`.
   - Tambahkan `GRUB_TERMINAL="console serial"`.
   - Hapus `GRUB_HIDDEN_TIMEOUT`.

- Tambahkan `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

Berikut adalah contoh `/etc/default/grub.d/50-cloudimg-settings.cfg`. Anda mungkin perlu mengubah konfigurasi berdasarkan pengaturan sistem.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Terapkan konfigurasi yang diperbarui dengan menjalankan perintah berikut.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

Untuk mengonfigurasi GRUB pada instans RHEL

1. Sambungkan ke instans Anda.
2. Tambahkan atau ubah pilihan berikut dalam `/etc/default/grub`:
   - Hapus `GRUB_TERMINAL_OUTPUT`.
   - Tambahkan `GRUB_TERMINAL="console serial"`.
   - Tambahkan `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

Berikut adalah contoh `/etc/default/grub`. Anda mungkin perlu mengubah konfigurasi berdasarkan pengaturan sistem.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Terapkan konfigurasi yang diperbarui dengan menjalankan perintah berikut.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg --update-bls-cmdline
```

Untuk RHEL 9.2 dan sebelumnya, gunakan perintah berikut.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

CentOS

Untuk instans yang diluncurkan menggunakan CentOS AMI, GRUB dikonfigurasikan untuk konsol serial secara default.

Berikut adalah contoh `/etc/default/grub`. Konfigurasi Anda mungkin berbeda berdasarkan pengaturan sistem.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

(Instans Linux) Konfigurasikan SysRq

Untuk mengkonfigurasi SysRq, Anda mengaktifkan SysRq perintah untuk siklus boot saat ini. Untuk membuat konfigurasi persisten, Anda juga dapat mengaktifkan SysRq perintah untuk boot berikutnya.

Untuk mengaktifkan semua SysRq perintah untuk siklus boot saat ini

1. Sambungkan ke instans Anda.
2. Jalankan perintah berikut.

   ```
   [ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
   ```

   Pengaturan ini akan dihapus pada boot ulang berikutnya.

Untuk mengaktifkan semua SysRq perintah untuk boot berikutnya

1. Buat file `/etc/sysctl.d/99-sysrq.conf` dan buka file tersebut di editor favorit Anda.

   ```
   [ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
   ```
2. Tambahkan baris berikut.

   ```
   kernel.sysrq=1
   ```
3. Boot ulang instans untuk menerapkan perubahan.

   ```
   [ec2-user ~]$ sudo reboot
   ```
4. Pada **`login`** prompt, masukkan nama pengguna pengguna berbasis kata sandi yang Anda atur sebelumnya, lalu tekan Enter.
5. Pada perintah `Password`, masukkan kata sandi, lalu tekan Enter.

(Instans Windows) Aktifkan SAC dan menu boot

> **Note**
>
> Jika Anda mengaktifkan SAC pada instans, layanan EC2 yang mengandalkan pengambilan kata sandi tidak akan bekerja dari konsol Amazon EC2. Agen peluncuran Windows di Amazon EC2 (EC2Config, EC2Launch v1, dan EC2Launch v2) mengandalkan konsol serial

untuk menjalankan berbagai tugas. Tugas-tugas ini tidak berhasil dijalankan saat Anda mengaktifkan SAC pada sebuah instans. Untuk informasi selengkapnya tentang Windows di agen peluncuran Amazon EC2, lihat. the section called “Konfigurasikan instance Windows” Jika mengaktifkan SAC, Anda dapat menonaktifkannya nanti. Untuk informasi selengkapnya, lihat Menonaktifkan SAC dan menu boot.

Gunakan salah satu metode berikut untuk mengaktifkan SAC dan menu boot pada instans.

PowerShell

Untuk mengaktifkan SAC dan menu boot pada instans Windows

1. Connect ke instans Anda dan lakukan langkah-langkah berikut dari baris PowerShell perintah yang ditinggikan.
2. Aktifkan SAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Aktifkan menu boot.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Terapkan konfigurasi yang diperbarui dengan melakukan boot ulang instans.

```
shutdown -r -t 0
```

Command prompt

Untuk mengaktifkan SAC dan menu boot pada instans Windows

1. Hubungkan ke instans Anda dan lakukan langkah-langkah berikut dari prompt perintah.
2. Aktifkan SAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Aktifkan menu boot.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Terapkan konfigurasi yang diperbarui dengan melakukan boot ulang instans.

```
shutdown -r -t 0
```

Konfigurasikan akses ke Konsol Serial EC2

Untuk mengonfigurasi akses ke konsol serial, Anda harus memberikan akses konsol serial pada tingkat akun, lalu mengonfigurasi kebijakan IAM untuk memberikan akses kepada pengguna IAM. Untuk instance Linux, Anda juga harus mengonfigurasi pengguna berbasis kata sandi pada setiap instance sehingga pengguna Anda dapat menggunakan konsol serial untuk pemecahan masalah.

EC2 Serial Console menggunakan koneksi port serial virtual untuk berinteraksi dengan sebuah instans. Koneksi ini independen dari VPC instance, sehingga Anda dapat bekerja dengan sistem operasi instance dan menjalankan alat pemecahan masalah bahkan jika ada kegagalan boot atau masalah konfigurasi jaringan. Karena koneksi ini berada di luar jaringan VPC, EC2 Serial Console tidak menggunakan grup keamanan instans atau jaringan subnet ACL untuk mengotorisasi lalu lintas ke instans.

Sebelum Anda mulai

Verifikasi bahwa prasyarat terpenuhi.

Daftar Isi

- Tingkat akses ke Konsol Serial EC2
- Kelola akses akun ke Konsol Serial EC2
- Konfigurasikan kebijakan IAM untuk akses Konsol Serial EC2
- Tetapkan kata sandi pengguna OS pada instance Linux

Tingkat akses ke Konsol Serial EC2

Secara default, tidak ada akses ke konsol serial pada tingkat akun. Anda perlu secara eksplisit memberikan akses ke konsol serial pada tingkat akun. Untuk informasi selengkapnya, lihat Kelola akses akun ke Konsol Serial EC2.

Anda dapat menggunakan kebijakan kontrol layanan (SCP) untuk mengizinkan akses ke konsol serial dalam organisasi. Anda selanjutnya dapat memiliki kontrol akses terperinci pada tingkat pengguna menggunakan kebijakan IAM untuk mengontrol akses. Dengan menggunakan kombinasi kebijakan SCP dan IAM, Anda memiliki beragam tingkat kontrol akses ke konsol serial.

Tingkat organisasi

Anda dapat menggunakan kebijakan kontrol layanan (SCP) untuk mengizinkan akses ke konsol serial di organisasi Anda. Untuk informasi selengkapnya SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.

Tingkat instans

Anda dapat mengonfigurasi kebijakan akses konsol serial dengan menggunakan IAM PrincipalTag dan ResourceTag konstruksi dan dengan menentukan instance berdasarkan ID mereka. Untuk informasi selengkapnya, lihat Konfigurasikan kebijakan IAM untuk akses Konsol Serial EC2.

Tingkat pengguna

Anda dapat mengonfigurasi akses pada tingkat pengguna dengan mengonfigurasi kebijakan IAM untuk mengizinkan atau menolak pengguna tertentu izin guna mendorong kunci publik SSH ke layanan konsol serial instans tertentu. Untuk informasi selengkapnya, lihat Konfigurasikan kebijakan IAM untuk akses Konsol Serial EC2.

Tingkat OS (hanya instance Linux)

Anda dapat mengatur kata sandi pengguna pada tingkat OS tamu. Tingkat ini menyediakan akses ke konsol serial untuk beberapa kasus penggunaan. Namun, untuk memantau log, Anda tidak memerlukan pengguna berbasis kata sandi. Untuk informasi selengkapnya, lihat Tetapkan kata sandi pengguna OS pada instance Linux.

Kelola akses akun ke Konsol Serial EC2

Secara default, tidak ada akses ke konsol serial pada tingkat akun. Anda perlu secara eksplisit memberikan akses ke konsol serial pada tingkat akun.

Pengaturan ini dikonfigurasi di tingkat akun, baik secara langsung di akun atau dengan menggunakan kebijakan deklaratif. Itu harus dikonfigurasi di setiap AWS Region tempat Anda ingin memberikan akses ke konsol serial. Menggunakan kebijakan deklaratif memungkinkan Anda menerapkan pengaturan di beberapa Wilayah secara bersamaan, serta di beberapa akun secara bersamaan. Saat kebijakan deklaratif sedang digunakan, Anda tidak dapat mengubah setelan secara langsung di dalam akun. Topik ini menjelaskan cara mengonfigurasi pengaturan secara langsung di dalam akun. Untuk informasi tentang penggunaan kebijakan deklaratif, lihat Kebijakan deklaratif di AWS Organizations Panduan Pengguna.

Daftar Isi

- Memberikan izin kepada pengguna untuk mengelola akses akun
- Melihat status akses akun ke konsol serial
- Memberikan akses akun ke konsol serial
- Menolak akses akun ke konsol serial

Memberikan izin kepada pengguna untuk mengelola akses akun

Untuk mengizinkan pengguna mengelola akses akun ke konsol serial EC2, Anda perlu memberi mereka izin IAM yang diperlukan.

Kebijakan berikut memberikan izin untuk melihat status akun serta untuk mengizinkan dan mencegah akses akun ke konsol serial EC2.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Untuk informasi selengkapnya, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Melihat status akses akun ke konsol serial

Console

Untuk melihat akses akun ke konsol serial

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor.
3. Pada kartu Atribut akun, di bawah Pengaturan, pilih Konsol Serial EC2.
4. Pada tab Konsol Serial EC2, nilai akses Konsol Serial EC2 Diizinkan atau Dicegah.

AWS CLI

Untuk melihat akses akun ke konsol serial

Gunakan perintah get-serial-console-access-status.

```
aws ec2 get-serial-console-access-status
```

Berikut ini adalah output contoh. Nilai `true` menunjukkan bahwa akun diizinkan akses ke konsol serial.

```
{
    "SerialConsoleAccessEnabled": true,
    "ManagedBy": "account"
}
```

`ManagedBy`Bidang menunjukkan entitas yang mengkonfigurasi pengaturan. Nilai yang mungkin `account` (dikonfigurasi secara langsung) atau`declarative-policy`. Untuk informasi selengkapnya, lihat Kebijakan deklaratif di Panduan AWS Organizations Pengguna.

PowerShell

Untuk melihat akses akun ke konsol serial

Gunakan Get-EC2SerialConsoleAccessStatuscmdlet.

```
Get-EC2SerialConsoleAccessStatus -Select *
```

Berikut ini adalah output contoh. Nilai `True` menunjukkan bahwa akun diizinkan akses ke konsol serial.

```
ManagedBy SerialConsoleAccessEnabled
--------- --------------------------
account   True
```

`ManagedBy`Bidang menunjukkan entitas yang mengkonfigurasi pengaturan. Nilai yang mungkin `account` (dikonfigurasi secara langsung) atau`declarative-policy`. Untuk informasi selengkapnya, lihat Kebijakan deklaratif di Panduan AWS Organizations Pengguna.

Memberikan akses akun ke konsol serial

Console

Untuk memberikan akses akun ke konsol serial

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor.
3. Pada kartu Atribut akun, di bawah Pengaturan, pilih Konsol Serial EC2.
4. Pilih Kelola.
5. Untuk mengizinkan akses ke konsol serial EC2 dari semua instance di akun, pilih kotak centang Izinkan.
6. Pilih Perbarui.

AWS CLI

Untuk memberikan akses akun ke konsol serial

Gunakan perintah enable-serial-console-access.

```
aws ec2 enable-serial-console-access
```

Berikut ini adalah output contoh.

```
{
```

```
    "SerialConsoleAccessEnabled": true
}
```

PowerShell

Untuk memberikan akses akun ke konsol serial

Gunakan Enable-EC2SerialConsoleAccesscmdlet.

```
Enable-EC2SerialConsoleAccess
```

Berikut ini adalah output contoh.

```
True
```

Menolak akses akun ke konsol serial

Console

Untuk menolak akses akun ke konsol serial

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Dasbor.
3. Pada kartu Atribut akun, di bawah Pengaturan, pilih Konsol Serial EC2.
4. Pilih Kelola.
5. Untuk mencegah akses ke konsol serial EC2 dari semua instance di akun, kosongkan kotak centang Izinkan.
6. Pilih Perbarui.

AWS CLI

Untuk menolak akses akun ke konsol serial

Gunakan perintah disable-serial-console-access.

```
aws ec2 disable-serial-console-access
```

Berikut ini adalah output contoh.

```
{
    "SerialConsoleAccessEnabled": false
}
```

PowerShell

Untuk menolak akses akun ke konsol serial

Gunakan Disable-EC2SerialConsoleAccesscmdlet.

```
Disable-EC2SerialConsoleAccess
```

Berikut ini adalah output contoh.

```
False
```

Konfigurasikan kebijakan IAM untuk akses Konsol Serial EC2

Secara default, pengguna Anda tidak memiliki akses ke konsol serial. Organisasi Anda harus mengonfigurasi kebijakan IAM untuk memberikan akses yang diperlukan kepada pengguna. Untuk informasi selengkapnya, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk akses konsol serial, buat dokumen kebijakan JSON yang mencakup tindakan `ec2-instance-connect:SendSerialConsoleSSHPublicKey`. Tindakan ini memberi pengguna izin untuk mendorong kunci publik ke layanan konsol serial, yang memulai sesi konsol serial. Sebaiknya batasi akses ke instans EC2 tertentu. Jika tidak, semua pengguna IAM dengan izin ini dapat terhubung ke konsol serial dari semua instans EC2.

Contoh kebijakan IAM

- Secara eksplisit mengizinkan akses ke konsol serial
- Secara eksplisit mengizinkan akses ke konsol serial
- Gunakan tanda sumber daya untuk mengontrol akses ke konsol serial

Secara eksplisit mengizinkan akses ke konsol serial

Secara default, tidak ada yang memiliki akses ke konsol serial. Untuk memberikan akses ke konsol serial, Anda perlu mengonfigurasi kebijakan untuk secara eksplisit mengizinkan akses. Sebaiknya konfigurasikan kebijakan yang membatasi akses ke instans tertentu.

Kebijakan berikut memungkinkan akses ke konsol serial instans tertentu, diidentifikasi berdasarkan ID instansnya.

Perhatikan bahwa tindakan `DescribeInstances`, `DescribeInstanceTypes`, dan `GetSerialConsoleAccessStatus` tidak mendukung izin tingkat sumber daya, dan oleh karena itu semua sumber daya, yang ditunjukkan oleh * (tanda bintang), harus ditentukan untuk tindakan ini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Secara eksplisit mengizinkan akses ke konsol serial

Kebijakan IAM berikut memungkinkan akses ke konsol serial semua instans, dilambangkan dengan * (tanda bintang), dan secara eksplisit menolak akses ke konsol serial instans tertentu, diidentifikasi berdasarkan ID-nya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Gunakan tanda sumber daya untuk mengontrol akses ke konsol serial

Anda dapat menggunakan tanda sumber daya untuk mengontrol akses ke konsol serial dari sebuah instans.

Kontrol akses berbasis atribut adalah strategi otorisasi yang mendefinisikan izin berdasarkan tag yang dapat dilampirkan ke pengguna dan sumber daya. AWS Misalnya, kebijakan berikut ini mengizinkan pengguna untuk memulai koneksi konsol serial untuk sebuah instans hanya jika tanda sumber daya instans dan tanda pengguna utama memiliki nilai `SerialConsole` yang sama untuk kunci tanda tersebut.

Untuk informasi selengkapnya tentang penggunaan tag untuk mengontrol akses ke AWS sumber daya Anda, lihat Mengontrol akses ke AWS sumber daya di Panduan Pengguna IAM.

Perhatikan bahwa tindakan `DescribeInstances`, `DescribeInstanceTypes`, dan `GetSerialConsoleAccessStatus` tidak mendukung izin tingkat sumber daya, dan oleh karena itu semua sumber daya, yang ditunjukkan oleh * (tanda bintang), harus ditentukan untuk tindakan ini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Tetapkan kata sandi pengguna OS pada instance Linux

Anda dapat terhubung ke konsol serial tanpa kata sandi. Namun, untuk menggunakan konsol serial untuk memecahkan masalah instance Linux, instance harus memiliki pengguna OS berbasis kata sandi.

Anda dapat mengatur kata sandi untuk pengguna OS apa pun, termasuk pengguna root. Perhatikan bahwa pengguna root dapat memodifikasi semua file, sementara setiap pengguna OS mungkin memiliki izin terbatas.

Anda harus mengatur kata sandi pengguna pada setiap instans untuk konsol serial yang akan Anda gunakan. Ini adalah persyaratan satu kali untuk setiap instans.

> **Note**
>
> Secara default, AMIs disediakan oleh tidak AWS dikonfigurasi dengan pengguna berbasis kata sandi. Jika Anda meluncurkan instans menggunakan AMI yang sudah memiliki kata sandi pengguna root yang dikonfigurasikan, Anda dapat melewati instruksi ini.

Untuk mengatur kata sandi pengguna OS pada instance Linux

1. Terhubung ke instans Anda. Anda dapat menggunakan metode apa pun untuk terhubung ke instans, kecuali metode koneksi Konsol Serial EC2.
2. Untuk mengatur kata sandi pengguna, gunakan perintah passwd. Pada contoh berikut, pengguna adalah `root`.

   ```
   [ec2-user ~]$ sudo passwd root
   ```

   Berikut ini adalah output contoh.

   ```
   Changing password for user root.
   New password:
   ```
3. Pada perintah `New password`, masukkan kata sandi baru.
4. Pada perintah, masukkan kembali kata sandinya.

Hubungkan ke Konsol Serial EC2

Anda dapat terhubung ke konsol serial instans EC2 Anda dengan menggunakan konsol Amazon EC2 atau melalui SSH. Setelah terhubung ke konsol serial, Anda dapat menggunakannya untuk memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya. Untuk informasi selengkapnya tentang pemecahan masalah, lihat Memecahkan masalah instans Amazon EC2 Anda menggunakan Konsol Serial EC2.

Pertimbangan-pertimbangan

- Hanya 1 koneksi konsol serial aktif yang didukung per instans.
- Koneksi konsol serial biasanya berlangsung selama 1 jam kecuali Anda memutuskan sambungan darinya. Namun, selama pemeliharaan sistem, Amazon EC2 akan memutuskan koneksi sesi konsol serial.

  Durasi koneksi tidak ditentukan oleh durasi kredensyal IAM Anda. Jika kredensil IAM Anda kedaluwarsa, koneksi terus berlanjut hingga durasi maksimum koneksi konsol serial tercapai. Saat menggunakan pengalaman konsol Serial Console EC2, jika kredenal IAM Anda kedaluwarsa, hentikan koneksi dengan menutup halaman browser.
- Dibutuhkan waktu 30 detik untuk menghapus sesi setelah Anda memutuskan koneksi dari konsol serial untuk mengizinkan sesi baru.
- Port konsol serial yang didukung: `ttyS0` (instance Linux) dan `COM1` (instance Windows)
- Saat terhubung ke konsol serial, Anda mungkin melihat sedikit penurunan throughput instans.

Topik

- Hubungkan menggunakan klien berbasis peramban
- Hubungkan menggunakan kunci Anda sendiri dan klien SSH
- Titik akhir dan sidik jari Konsol Serial EC2

Hubungkan menggunakan klien berbasis peramban

Anda dapat terhubung ke konsol serial instans EC2 menggunakan klien berbasis peramban. Anda melakukannya dengan memilih instans di konsol Amazon EC2 dan memilih untuk terhubung ke konsol serial. Klien berbasis peramban menangani izin dan menyediakan koneksi yang berhasil.

Konsol serial EC2 bekerja dari sebagian besar peramban dan mendukung input keyboard serta mouse.

Sebelum menghubungkan, pastikan Anda telah menyelesaikan prasyarat.

Untuk terhubung ke port serial instans Anda menggunakan klien berbasis browser (konsol Amazon EC2)

1. Buka konsol Amazon EC2 di. https://console.aws.amazon.com/ec2/
2. Di panel navigasi, pilih Instans.

3. Pilih instans dan pilih Tindakan, Pantau dan pecahkan masalah, Konsol Serial EC2, Hubungkan.

   Atau, pilih instans dan pilih Hubungkan, Konsol Serial EC2, Hubungkan.

   Jendela terminal dalam peramban akan terbuka.
4. Tekan Enter. Jika perintah login ditampilkan, Anda terhubung ke konsol serial.

   Jika layar tetap berwarna hitam, Anda dapat menggunakan informasi berikut untuk membantu menyelesaikan masalah saat menghubungkan ke konsol serial:

   - Pastikan bahwa Anda telah mengonfigurasi akses ke konsol serial. Untuk informasi selengkapnya, lihat Konfigurasikan akses ke Konsol Serial EC2.
   - (Hanya instance Linux) Gunakan SysRq untuk terhubung ke konsol serial. SysRq tidak mengharuskan Anda terhubung menggunakan klien berbasis browser. Untuk informasi selengkapnya, lihat (Instance Linux) Gunakan SysRq untuk memecahkan masalah instance Anda.
   - (Hanya instance Linux) Mulai ulang getty. Jika Anda memiliki akses SSH ke instans, hubungkan ke instans menggunakan SSH, dan mulai ulang getty menggunakan perintah berikut.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```
   - Boot ulang instans Anda. Anda dapat me-reboot instance Anda dengan menggunakan SysRq (instance Linux), konsol EC2, atau. AWS CLI Untuk informasi selengkapnya, lihat (Instance Linux) Gunakan SysRq untuk memecahkan masalah instance Anda (contoh Linux) atauNyalakan ulang EC2 instans Amazon Anda.
5. (Hanya contoh Linux) Pada **`login`** prompt, masukkan nama pengguna pengguna berbasis kata sandi yang Anda atur sebelumnya, lalu tekan Enter.
6. (Hanya contoh Linux) Pada `Password` prompt, masukkan kata sandi, lalu tekan Enter.

Hubungkan menggunakan kunci Anda sendiri dan klien SSH

Anda dapat menggunakan kunci SSH Anda sendiri dan terhubung ke instans dari klien SSH pilihan Anda saat menggunakan API konsol serial. Hal ini memungkinkan Anda untuk mendapatkan manfaat dari kemampuan konsol serial untuk mendorong kunci publik ke instans.

Setelah menekan kunci SSH ke instance, koneksi SSH tidak tunduk pada kebijakan IAM yang Anda konfigurasikan untuk memberikan akses Konsol Serial EC2 kepada pengguna.

Sebelum Anda mulai

Verifikasi bahwa prasyarat terpenuhi.

Untuk terhubung ke konsol serial instans menggunakan SSH

1. Dorong kunci publik SSH Anda ke instans untuk memulai sesi konsol serial

   Gunakan perintah send-serial-console-ssh-public-key untuk mendorong kunci publik SSH Anda ke instance. Tindakan tersebut akan memulai sesi konsol serial.

   Jika sesi konsol serial telah dimulai untuk instans ini, perintah menjadi gagal karena Anda hanya dapat memiliki satu sesi terbuka pada satu waktu. Dibutuhkan waktu 30 detik untuk menghapus sesi setelah Anda memutuskan koneksi dari konsol serial untuk mengizinkan sesi baru.

   ```
   aws ec2-instance-connect send-serial-console-ssh-public-key \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --serial-port 0 \
       --ssh-public-key file://my_key.pub \
       --region us-east-1
   ```

2. Hubungkan ke konsol serial menggunakan kunci privat Anda

   Gunakan perintah ssh untuk terhubung ke konsol serial sebelum kunci publik dihapus dari layanan konsol serial. Anda memiliki waktu 60 detik sebelum kunci publik dihapus.

   Gunakan kunci privat yang sesuai dengan kunci publik.

   Format nama pengguna adalah`instance-id.port0`, yang terdiri dari ID instance dan port 0. Dalam contoh berikut, nama pengguna adalah`i-001234a4bf70dec41EXAMPLE.port0`.

   Titik akhir layanan konsol serial berbeda untuk setiap Wilayah. Lihat tabel Titik akhir dan sidik jari Konsol Serial EC2 untuk setiap titik akhir Wilayah. Pada contoh berikut, layanan konsol serial berada di Wilayah us-east-1.

   ```
   ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-
   connect.us-east-1.aws
   ```

   Contoh berikut digunakan `timeout 3600` untuk mengatur sesi SSH Anda untuk mengakhiri setelah 1 jam. Proses yang dimulai selama sesi dapat terus berjalan pada instans Anda setelah sesi berakhir.

```
timeout 3600 ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
```

3. (Opsional) Verifikasi sidik jari

   Saat terhubung ke konsol serial untuk pertama kalinya, Anda akan diminta untuk memverifikasi sidik jari. Anda dapat membandingkan sidik jari konsol serial dengan sidik jari yang ditampilkan untuk verifikasi. Jika sidik jari ini tidak cocok, seseorang mungkin mencoba serangan “man-in-the-middle”. Jika sidik jari cocok, Anda dapat terhubung ke konsol serial dengan yakin.

   Sidik jari berikut ditujukan untuk layanan konsol serial di Wilayah us-east-1. Untuk sidik jari setiap Wilayah, lihat Titik akhir dan sidik jari Konsol Serial EC2.

   ```
   SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
   ```

   Sidik jari hanya muncul saat pertama kali Anda terhubung ke konsol serial.

4. Tekan Enter. Jika perintah kembali, Anda terhubung ke konsol serial.

   Jika layar tetap berwarna hitam, Anda dapat menggunakan informasi berikut untuk membantu menyelesaikan masalah saat menghubungkan ke konsol serial:

   - Pastikan bahwa Anda telah mengonfigurasi akses ke konsol serial. Untuk informasi selengkapnya, lihat Konfigurasikan akses ke Konsol Serial EC2.
   - (Hanya instance Linux) Gunakan SysRq untuk terhubung ke konsol serial. SysRq tidak mengharuskan Anda terhubung menggunakan SSH. Untuk informasi selengkapnya, lihat (Instance Linux) Gunakan SysRq untuk memecahkan masalah instance Anda.
   - (Hanya instance Linux) Mulai ulang getty. Jika Anda memiliki akses SSH ke instans, hubungkan ke instans menggunakan SSH, dan mulai ulang getty menggunakan perintah berikut.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - Boot ulang instans Anda. Anda dapat me-reboot instance Anda dengan menggunakan SysRq (hanya instance Linux), konsol EC2, atau. AWS CLI Untuk informasi selengkapnya, lihat (Instance Linux) Gunakan SysRq untuk memecahkan masalah instance Anda (hanya instance Linux) atauNyalakan ulang EC2 instans Amazon Anda.

5. (Hanya contoh Linux) Pada **`login`** prompt, masukkan nama pengguna pengguna berbasis kata sandi yang Anda atur sebelumnya, lalu tekan Enter.
6. (Hanya contoh Linux) Pada `Password` prompt, masukkan kata sandi, lalu tekan Enter.

Titik akhir dan sidik jari Konsol Serial EC2

Berikut ini adalah titik akhir layanan dan sidik jari untuk Konsol Serial EC2. Untuk terhubung secara terprogram ke konsol serial instans, Anda menggunakan titik akhir Konsol Serial EC2. Titik akhir dan sidik jari Konsol Serial EC2 bersifat unik untuk setiap Wilayah AWS .

Nama Wilayah	Wilayah	Titik akhir	Sidik jari
AS Timur (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256: EhwPkTzRt TY7 TRSzz26 RM7m CZN0xw xBB0/HVV9 j /d/0
US East (Northern Virginia)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256:DxWN5mA/ XAD VMe BZGEru5l2 gx +Yi5 Ya LDi LUcz0 FMmw
AS Barat (California Utara)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256: OHldlc MET8u7 QLSX3jm RTRAPFHVtqbyo LZBMUCqi H3Y
AS Barat (Oregon)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256: EMCIe23 TqKa BI6y GHainq ZcMwqNkDhh AVHa1 O2Jx VUc
Africa (Cape Town)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256: RMWWZ2f VePe JUqzj KIg XsczoHlz O5JL2 21ED00biiwi

Nama Wilayah	Wilayah	Titik akhir	Sidik jari
Asia Pasifik (Hong Kong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256:T0Q1 Akjbp7tkm2x C9b lpiXxCho ZHpln Ynifk XVi JFsj
Asia Pasifik (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256: WJg PBSw v4/SHN+15 OPITValoew AuYj DVW845 JEh DKRs
Asia Pasifik (Jakarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA256:5 ZwgrCh XITq +lfns32 L/4o0zifbx4bzgs Saya YFqy3o8m
Asia Pasifik (Malaysia)	ap-southeast-5	ec2-serial-console.ap-southeast-5.api.aws	SHA256:c QXTHQMRcq RdIjm AGo AMBSExeo RobYyRw yTjnEi T67 A
Asia Pacific (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	SHA256:Av aq27 hFgLvjn 5g Z0oV7h90p0 OET6 M TSSh GG46wf ZJv
Asia Pasifik (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256:o BLXc HHEbli ARx Ymklq eGH8ISO51rez BSU40 TPi SM35
Asia Pacific (Osaka)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256BKB nBuFnHr:am0/Ji 9aXSG G8tu/VVHF XE/3uCyJSQ EV3

Nama Wilayah	Wilayah	Titik akhir	Sidik jari
Asia Pasifik (Seoul)	ap-northeast-2	serial-console.ec2-instance-connect.ap-northeast-2.aws	SHA256:FOQWXNX +DZ+Gu BX+FRC SRQRI NTztg9 PK49 WYMq ZM2d
Asia Pasifik (Singapura)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256: Wn PLFNn7 CQDHx3qmw Lu1Gy/ O8 TUX7 LQg ZuaC6L45CoY
Asia Pasifik (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256: yFvMw UK9l EUQj QTRo XXzu VSe9 N+CW9/W98 4Cf5Tgzo4
Asia Pasifik (Thailand)	ap-tenggara 7	ec2-serial-console.ap-southeast-7.api.aws	SHA256: KCAZi RYr vTwixWmvc R1q2lqSG7 2wmj DY VT31 XRg SdEf
Asia Pasifik (Tokyo)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256: RQfs DCZTOf Em/ + TRDV1t9 HMr FQe CRI IOT5um4k
Kanada (Pusat)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256:P2o2j MwkPO6 OZwmp Ev2gcz YW738 FIOTHd UTy YMMO7s4
Kanada Barat (Calgary)	ca-west-1	ec2-serial-console.ca-west-1.api.aws	SHA256JNx GAFLPGOLj x7IxxXrGckk:S3rc8l i2xHBHR3iEDJ 6Q

Nama Wilayah	Wilayah	Titik akhir	Sidik jari
Tiongkok (Beijing)	cn-north-1	ec2-serial-console.cn-north-1.api.amazonwebservices.com.cn	SHA256:2g HVFy4 FUx H7UU3+WA D28V/LGGT+Y ggMeqjvSlgngpg
Tiongkok (Ningxia)	cn-northwest-1	ec2-serial-console.cn-northwest-1.api.amazonwebservices.com.cn	SHA256:Tdgr NZki QOd Vf O4Sz M YEBUh UA09 VWI5r YOZGTogpwmi
Eropa (Frankfurt)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256:acmfs/ 8amz1toe+bbnr fy0k0de2c yIcOd OlkXvOl JJ3
Eropa (Irlandia)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256:H2aa Hathhtm6ezs3bj7uDG Uxi2 GAWO4 E qTrHj ZAw CW6
Eropa (London)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256CE/ AEG4Amm53 I6lkD1ZPvS/BCV:a69 rd5 3t 8 TPW2 RnJg
Europe (Milan)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256:LC0k Fy A7N99eClb S7X7 OVJnpg BVrxn0 XSX95cuu QK30
Eropa (Paris)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8ldnaf9pym ene8bn FVng Y3 / kxsw RPAr JUzfrlxe EWs

Nama Wilayah	Wilayah	Titik akhir	Sidik jari
Eropa (Spanyol)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256:Pergi CW2 DFRlu669 QNxq FxEcs ZUz R6f /4f4n7t45 ZcwoEc
Eropa (Stockholm)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256:tk GFFUVUDvoc Di GSS3 Cu8gDL6W2 UI32 X84 EPNp KFKLw
Europe (Zurich)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA256BMf 6WdCw:8ppx2m 0 kfwm4/4Oa NUlz IfRz XFut QXWp6mk
Israel (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256: JR6q8v6k NNPi8 + QSFQ4dj5d im Nm ZPTgwgs M1 SNvt YYu
Meksiko (Tengah)	mx-pusat-1	ec2-serial-console .mx-central-1.api.aws	SHA256: BCu VL13i +18EF4p2 FeTB32 QNk CcVnt ZHUr BBAOxl GS0
Timur Tengah (Bahrain)	me-south-1	ec2-serial-console .me-south-1.api.aws	SHA256:Npj LLKHu2 QnLdUq 2k K5xV C3k8 VArso PJOMRJKCBz CDq
Timur Tengah (UAE)	eu-central-1	ec2-serial-console .me-central-1.api.aws	SHA256:ZPB5DuKibz +L0 B4 dFwPeyyk I/ Xz LE MPBYh XNe FSDKBv

Nama Wilayah	Wilayah	Titik akhir	Sidik jari
Amerika Selatan (Sao Paulo)	sa-east-1	serial-console.ec2-instance-connect.sa-east-1.aws	SHA256VIe mENa:RD2+ /32ognJew1Y QZC +BotbiH62oQ I APDq1d
AWS GovCloud (AS-Timur)	us-gov-east-1	serial-console.ec2 -instance-connect. us-gov-east-1.amaz onaws.com	SHA256:TiWe19+F28 GWsoy LClrtvu38 YEEh DHIkqn DcZnmtebv
AWS GovCloud (AS-Barat)	us-gov-west-1	serial-console.ec2 -instance-connect. us-gov-west-1.amaz onaws.com	SHA256:kf OFRWLa OZf b+utbd3brf8 8n iW5dq OlPf GO2 YZLq XZi

Memutuskan koneksi dari Konsol Serial EC2

Jika tidak perlu lagi terhubung ke Konsol Serial EC2, Anda dapat memutuskan koneksi konsol tersebut. Saat Anda memutuskan koneksi dari konsol serial, sesi shell apa pun yang berjalan pada instans akan terus berjalan. Jika Anda ingin mengakhiri sesi shell, Anda harus mengakhirinya sebelum memutuskan koneksi dari konsol serial.

Pertimbangan-pertimbangan

- Koneksi konsol serial biasanya berlangsung selama 1 jam kecuali jika Anda memutuskan koneksi dari konsol tersebut. Namun, selama pemeliharaan sistem, Amazon EC2 akan memutuskan koneksi sesi konsol serial.
- Dibutuhkan waktu 30 detik untuk menghapus sesi setelah Anda memutuskan koneksi dari konsol serial untuk mengizinkan sesi baru.

Cara untuk memutuskan koneksi dari konsol serial bergantung pada klien.

Klien berbasis peramban

Untuk memutuskan koneksi dari konsol serial, tutup jendela terminal dalam peramban konsol serial.

Klien OpenSSH standar

Untuk memutuskan koneksi dari konsol serial, gunakan perintah berikut untuk menutup koneksi SSH. Perintah ini harus dijalankan segera setelah baris baru.

```
~.
```

Perintah yang digunakan untuk menutup koneksi SSH mungkin berbeda bergantung pada klien SSH yang Anda gunakan.

Memecahkan masalah instans Amazon EC2 Anda menggunakan Konsol Serial EC2

Dengan menggunakan Konsol Serial EC2, Anda dapat memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya dengan terhubung ke port serial instans.

Gunakan instruksi untuk sistem operasi instans Anda dan untuk alat yang telah Anda konfigurasikan pada instans Anda.

Alat

- (Instance Linux) Gunakan GRUB untuk memecahkan masalah instans Anda
- (Instance Linux) Gunakan SysRq untuk memecahkan masalah instance Anda
- (Instans Windows) Gunakan SAC untuk memecahkan masalah instans Anda

Prasyarat

Sebelum memulai, pastikan Anda telah menyelesaikan prasyarat, termasuk mengonfigurasi alat pemecahan masalah yang Anda pilih.

(Instance Linux) Gunakan GRUB untuk memecahkan masalah instans Anda

GNU GRUB (singkatan dari GNU GRand Unified Bootloader, biasa disebut sebagai GRUB) adalah boot loader default untuk sebagian besar sistem operasi Linux. Dari menu GRUB, Anda dapat memilih kernel mana yang akan di-boot, atau memodifikasi entri menu untuk mengubah cara kernel akan di-boot. Hal ini dapat berguna ketika memecahkan masalah kegagalan instans.

Menu GRUB ditampilkan selama proses boot. Menu tidak dapat diakses melalui SSH normal, tetapi Anda dapat mengaksesnya menggunakan Konsol Serial EC2.

Anda dapat boot ke mode pengguna tunggal atau mode darurat. Mode pengguna tunggal akan melakukan boot ulang kernel pada runlevel yang lebih rendah. Misalnya, mode ini mungkin memasang sistem, file tetapi tidak mengaktifkan jaringan, sehingga memberi Anda kesempatan untuk melakukan pemeliharaan yang diperlukan guna memperbaiki instans. Mode darurat mirip dengan mode pengguna tunggal kecuali kernel berjalan pada runlevel terendah.

Untuk melakukan boot ke mode pengguna tunggal

1. Hubungkan ke konsol serial instans.
2. Boot ulang instans menggunakan perintah berikut.

   ```
   [ec2-user ~]$ sudo reboot
   ```

3. Selama boot ulang berlangsung, saat menu GRUB muncul, tekan tombol apa pun untuk menghentikan proses boot.
4. Pada menu GRUB, gunakan tombol panah untuk memilih kernel guna melakukan boot, dan tekan e di keyboard Anda.
5. Gunakan tombol panah untuk meletakkan kursor Anda pada baris yang berisi kernel. Garis dimulai dengan `linux` atau `linux16` bergantung pada AMI yang digunakan untuk meluncurkan instans. Untuk Ubuntu, dua baris dimulai dengan `linux`, yang keduanya harus dimodifikasi pada langkah berikutnya.
6. Di akhir baris, tambahkan kata `single`.

   Berikut ini adalah contoh Amazon Linux 2.

   ```
   linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
   dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
   s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
   ll=0 single
   ```

7. Tekan Ctrl+X untuk melakukan boot ke mode pengguna tunggal.
8. Pada **`login`** prompt, masukkan nama pengguna pengguna berbasis kata sandi yang Anda atur sebelumnya, lalu tekan Enter.
9. Pada perintah `Password`, masukkan kata sandi, lalu tekan Enter.

Untuk boot ke mode darurat

Ikuti langkah yang sama seperti mode pengguna tunggal, tetapi pada langkah 6, tambahkan kata `emergency` sebagai ganti`single`.

(Instance Linux) Gunakan SysRq untuk memecahkan masalah instance Anda

Kunci System Request (SysRq), yang kadang-kadang disebut sebagai SysRq “magic”, dapat digunakan untuk langsung mengirim perintah kernel, di luar shell, dan kernel akan merespons, terlepas dari apa yang dilakukan kernel. Misalnya, jika instance berhenti merespons, Anda dapat menggunakan SysRq kunci untuk memberi tahu kernel agar crash atau reboot. Untuk informasi selengkapnya, lihat SysRq Kunci ajaib di Wikipedia.

Anda dapat menggunakan SysRq perintah di klien berbasis browser EC2 Serial Console atau di klien SSH. Perintah untuk mengirim permintaan jeda berbeda untuk setiap klien.

Untuk menggunakannya SysRq, pilih salah satu prosedur berikut berdasarkan klien yang Anda gunakan.

Browser-based client

Untuk digunakan SysRq di klien berbasis browser konsol serial

1. Hubungkan ke konsol serial instans.
2. Untuk mengirim permintaan jeda, tekan `CTRL+0` (nol). Jika keyboard mendukungnya, Anda juga dapat mengirim permintaan jeda menggunakan tombol Pause atau Break.

   ```
   [ec2-user ~]$ CTRL+0
   ```
3. Untuk mengeluarkan SysRq perintah, tekan tombol pada keyboard Anda yang sesuai dengan perintah yang diperlukan. Misalnya, untuk menampilkan daftar SysRq perintah, tekanh.

   ```
   [ec2-user ~]$ h
   ```

   Perintah h menghasilkan sesuatu yang serupa dengan yang berikut ini.

   ```
   [ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
   tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
   (j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
   tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
   ) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
   buffer(z)
   ```

SSH client

Untuk digunakan SysRq dalam klien SSH

1. Hubungkan ke konsol serial instans.
2. Untuk mengirim permintaan jeda, tekan ~B (tilde, diikuti dengan huruf besar B).

```
[ec2-user ~]$ ~B
```

3. Untuk mengeluarkan SysRq perintah, tekan tombol pada keyboard Anda yang sesuai dengan perintah yang diperlukan. Misalnya, untuk menampilkan daftar SysRq perintah, tekanh.

```
[ec2-user ~]$ h
```

Perintah h menghasilkan sesuatu yang serupa dengan yang berikut ini.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> Perintah yang digunakan untuk mengirim permintaan jeda mungkin berbeda bergantung pada klien SSH yang Anda gunakan.

(Instans Windows) Gunakan SAC untuk memecahkan masalah instans Anda

Kemampuan Konsol Admin Khusus (SAC) Windows menyediakan cara untuk memecahkan masalah instans Windows. Dengan terhubung ke konsol serial instans dan menggunakan SAC, Anda dapat menginterupsi proses boot dan boot Windows dalam mode aman.

> **Note**
>
> Jika Anda mengaktifkan SAC pada instans, layanan EC2 yang mengandalkan pengambilan kata sandi tidak akan bekerja dari konsol Amazon EC2. Agen peluncuran Windows di

Amazon EC2 (EC2Config, EC2Launch v1, dan EC2Launch v2) mengandalkan konsol serial untuk menjalankan berbagai tugas. Tugas-tugas ini tidak berhasil dijalankan saat Anda mengaktifkan SAC pada sebuah instans. Untuk informasi selengkapnya tentang Windows di agen peluncuran Amazon EC2, lihat. the section called “Konfigurasikan instance Windows” Jika mengaktifkan SAC, Anda dapat menonaktifkannya nanti. Untuk informasi selengkapnya, lihat Menonaktifkan SAC dan menu boot.

Tugas

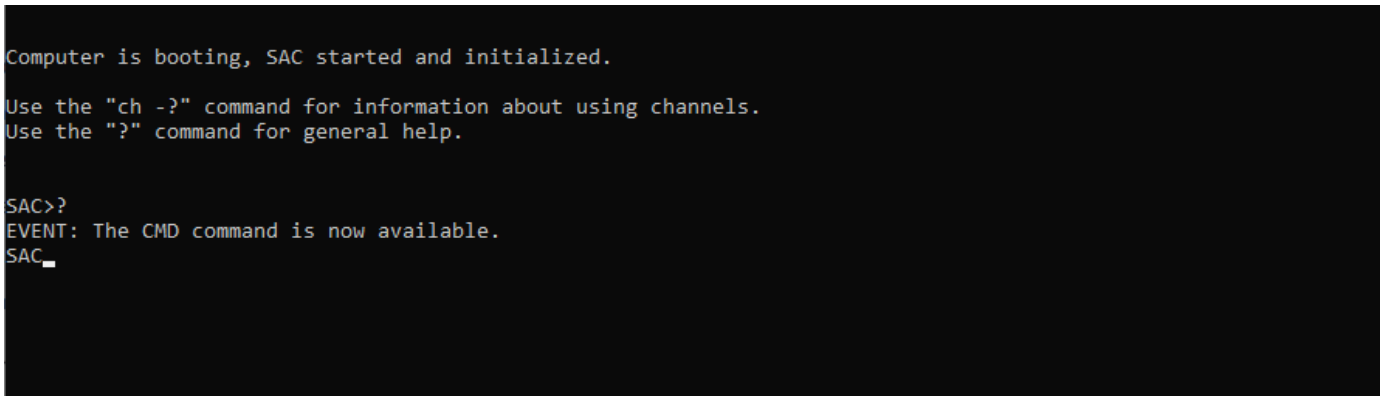
- Menggunakan SAC
- Menggunakan menu boot
- Menonaktifkan SAC dan menu boot

Menggunakan SAC

Untuk menggunakan SAC

1. Hubungkan ke konsol serial.

   Jika SAC diaktifkan pada instans, konsol serial akan menampilkan perintah SAC>.



2. Untuk menampilkan perintah SAC, masukkan? , dan kemudian tekan Enter.

   Output yang diharapkan

```
SAC>?
ch                    Channel management commands.  Use ch -? for more help.
cmd                   Create a Command Prompt channel.
d                     Dump the current kernel log.
f                     Toggle detailed or abbreviated tlist info.
? or help             Display this list.
i                     List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IPv4 addr., subnet and gateway.
id                    Display the computer identification information.
k <pid>               Kill the given process.
l <pid>               Lower the priority of a process to the lowest possible.
lock                  Lock access to Command Prompt channels.
m <pid> <MB-allow>    Limit the memory usage of a process to <MB-allow>.
p                     Toggle paging the display.
r <pid>               Raise the priority of a process by one.
s                     Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm    Set the current time and date (24 hour clock used).
t                     Tlist.
restart               Restart the system immediately.
shutdown              Shutdown the system immediately.
crashdump             Crash the system. You must have crash dump enabled.
```

3. Untuk membuat saluran prompt perintah (seperti `cmd0001` atau`cmd0002`), masukkan cmd, lalu tekan Enter.
4. Untuk melihat saluran prompt perintah, tekan ESC, lalu tekan TAB.

   Output yang diharapkan

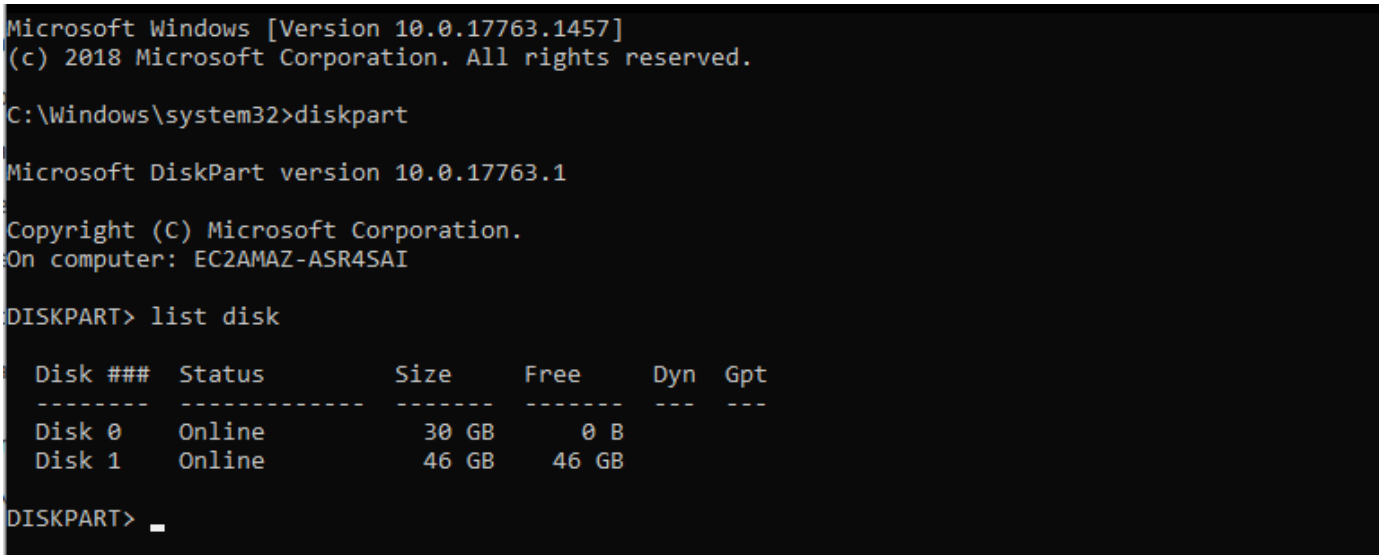
```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Untuk beralih saluran, tekan ESC+TAB+nomor saluran secara bersamaan. Misalnya, untuk beralih ke saluran `cmd0002` (jika sudah dibuat), tekan ESC+TAB+2.
6. Masukkan kredensial yang diperlukan oleh saluran prompt perintah.

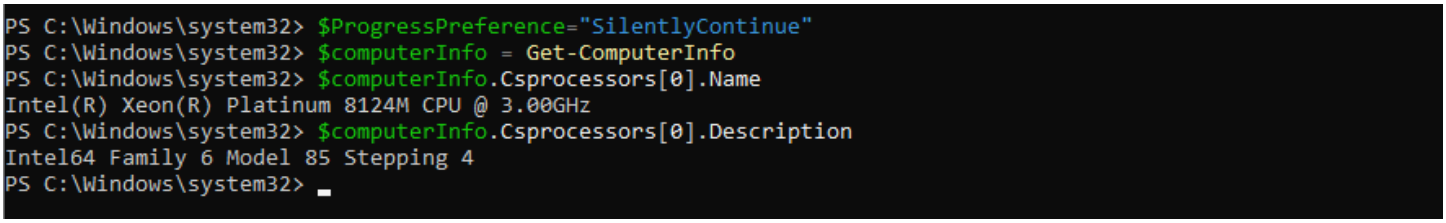
```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

Prompt perintah adalah perintah shell berfitur lengkap yang sama dengan yang Anda dapatkan di desktop, tetapi dengan pengecualian bahwa perintah tersebut tidak mengizinkan pembacaan karakter yang sudah dikeluarkan.



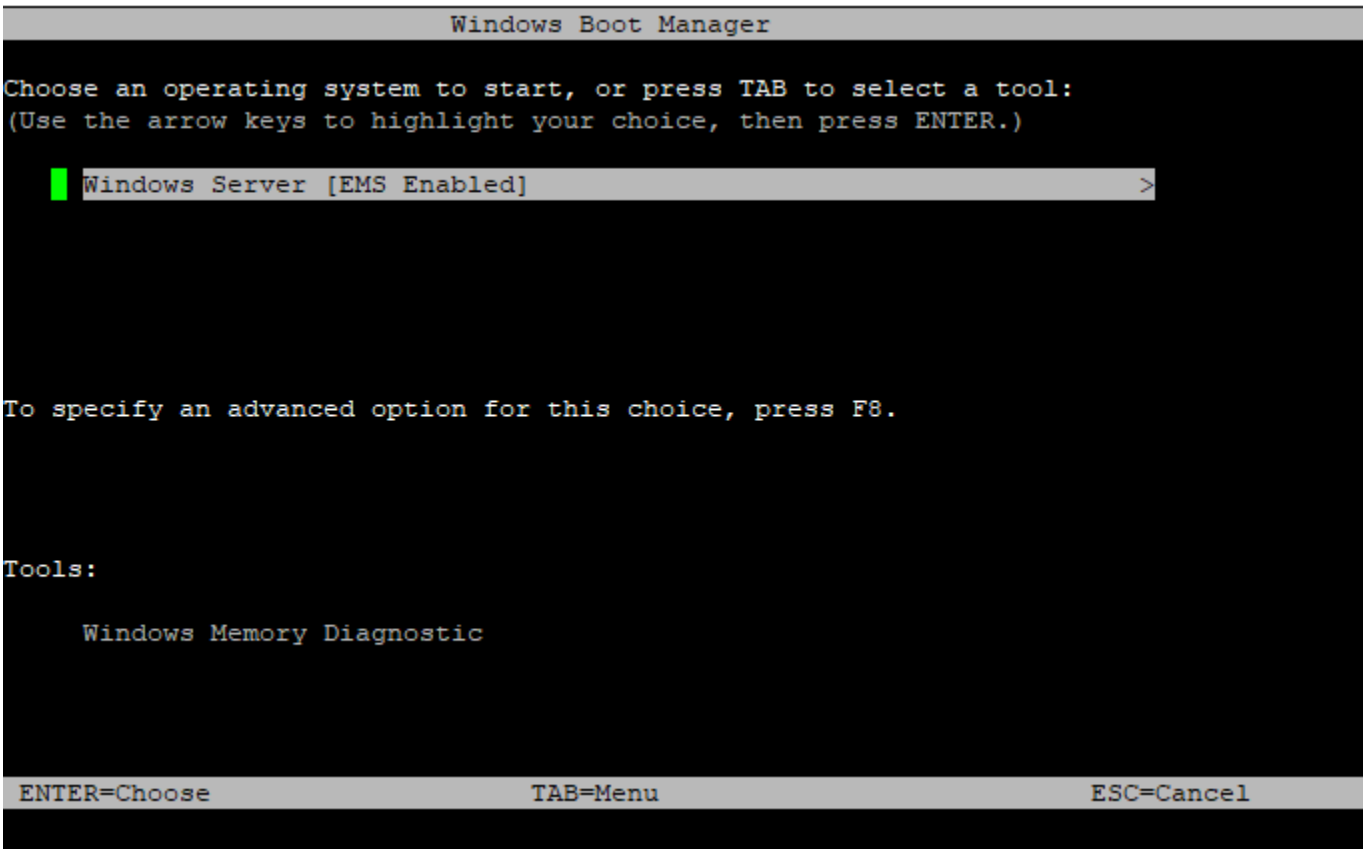
PowerShell juga dapat digunakan dari command prompt.

Perhatikan bahwa Anda mungkin perlu mengatur preferensi perkembangan ke mode diam.



Menggunakan menu boot

Jika instance memiliki menu boot diaktifkan dan dimulai ulang setelah menghubungkan melalui SSH, Anda akan melihat menu boot, sebagai berikut.



Perintah menu boot

ENTER

Mulai entri yang dipilih dari sistem operasi.

TAB

Beralih ke menu Alat.

ESC

Membatalkan dan memulai ulang instans.

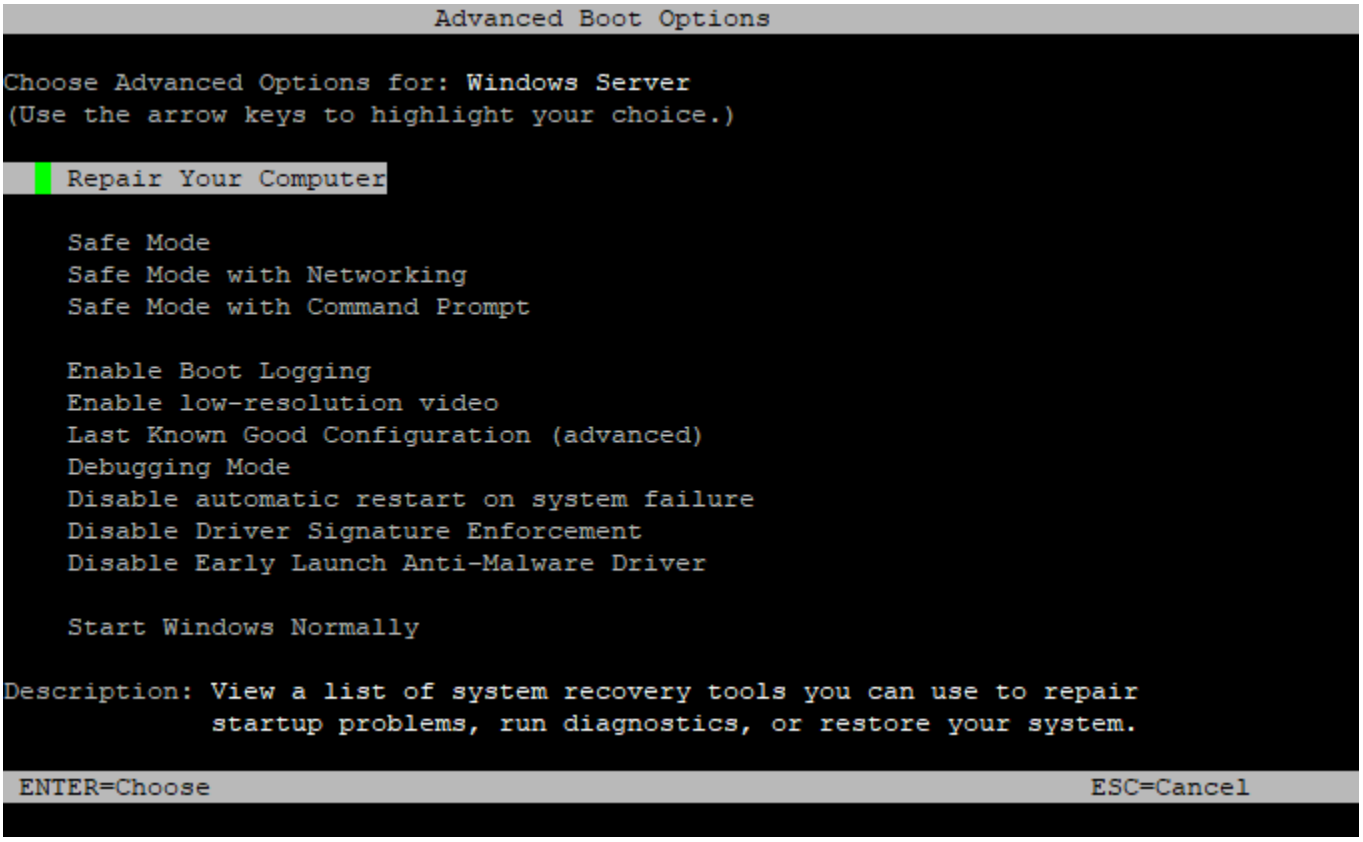
ESC diikuti dengan tombol angka 8

Sama dengan menekan F8. Menampilkan opsi lanjutan untuk item yang dipilih.

Tombol ESC + panah kiri

Kembali ke menu boot awal.

Tombol ESC tidak membawa Anda kembali ke menu utama karena Windows menunggu untuk melihat jika urutan keluar sedang berlangsung.



Menonaktifkan SAC dan menu boot

Jika mengaktifkan SAC dan menu boot, Anda dapat menonaktifkan fitur ini nanti.

Gunakan salah satu metode berikut untuk mengaktifkan SAC dan menu boot pada instans.

PowerShell

Untuk menonaktifkan SAC dan menu boot pada instans Windows

1. Connect ke instans Anda dan lakukan langkah-langkah berikut dari baris PowerShell perintah yang ditinggikan.
2. Pertama nonaktifkan menu boot dengan mengubah nilainya menjadi no.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Kemudian nonaktifkan SAC dengan mengubah nilainya menjadi `off`.

```
bcdedit /ems '{current}' off
```

4. Terapkan konfigurasi yang diperbarui dengan melakukan boot ulang instans.

```
shutdown -r -t 0
```

Command prompt

Untuk menonaktifkan SAC dan menu boot pada instans Windows

1. Hubungkan ke instans Anda dan lakukan langkah-langkah berikut dari prompt perintah.
2. Pertama nonaktifkan menu boot dengan mengubah nilainya menjadi no.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Kemudian nonaktifkan SAC dengan mengubah nilainya menjadi `off`.

```
bcdedit /ems {current} off
```

4. Terapkan konfigurasi yang diperbarui dengan melakukan boot ulang instans.

```
shutdown -r -t 0
```

Kirim interupsi diagnostik untuk men-debug instans Amazon EC2 yang tidak dapat dijangkau

> **Warning**
>
> Interupsi diagnostik ditujukan untuk digunakan oleh pengguna tingkat lanjut. Penggunaan yang salah dapat memengaruhi instans Anda secara negatif. Mengirimkan interupsi diagnostik ke suatu instans dapat memicu crash dan boot ulang pada instans, yang dapat menyebabkan hilangnya data.

Anda dapat mengirim interupsi diagnostik ke instance yang tidak dapat dijangkau atau tidak responsif untuk memicu kepanikan kernel secara manual untuk instance Linux, atau kesalahan berhenti (biasanya disebut sebagai kesalahan layar biru) untuk instance Windows.

Instans Linux

Sistem operasi Linux biasanya akan mengalami crash dan boot ulang ketika kepanikan kernel terjadi. Perilaku khusus dari sistem operasi bergantung pada konfigurasinya. Kepanikan kernel juga dapat digunakan untuk menyebabkan kernel sistem operasi instans melakukan tugas, seperti membuat file dump crash. Anda kemudian dapat menggunakan informasi pada file dump crash tersebut untuk melakukan analisis akar penyebab masalah dan melakukan debug instans. Data dump crash dihasilkan secara lokal oleh sistem operasi pada instans itu sendiri.

Instans Windows

Secara umum, sistem operasi Windows mengalami crash dan melakukan boot ulang ketika terjadi kesalahan penghentian, tetapi perilaku spesifiknya bergantung pada konfigurasinya. Kesalahan penghentian juga dapat menyebabkan sistem operasi menulis informasi debug, seperti dump memori kernel, ke file. Kemudian, Anda dapat menggunakan informasi ini untuk melakukan analisis akar penyebab guna melakukan debug instans. Data dump memori dihasilkan secara lokal oleh sistem operasi pada instans itu sendiri.

Sebelum mengirimkan interupsi diagnostik ke instans Anda, kami sarankan untuk membaca dokumentasi sistem operasi, kemudian membuat perubahan konfigurasi yang diperlukan.

Daftar Isi

- Tipe instans yang didukung
- Prasyarat
- Kirimkan interupsi diagnostik

Tipe instans yang didukung

Interupsi diagnostik didukung pada semua jenis instans berbasis Nitro, kecuali yang didukung oleh prosesor AWS Graviton. Untuk informasi lebih lanjut, lihat contoh yang dibangun di atas Sistem AWS Nitro dan AWS Graviton.

Prasyarat

Sebelum menggunakan interupsi diagnostik, Anda harus mengonfigurasi sistem operasi instans. Ini memastikan bahwa ia melakukan tindakan yang Anda butuhkan ketika kepanikan kernel (instance Linux) atau kesalahan berhenti (instance Windows) terjadi.

Instans Linux

Untuk mengonfigurasi Amazon Linux 2 atau Amazon Linux 2023 untuk menghasilkan crash dump saat terjadi kepanikan kernel

1. Menghubungkan ke instans Anda.
2. Instal kexec dan kdump.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Konfigurasikan kernel untuk mencadangkan jumlah memori yang sesuai untuk kernel sekunder. Jumlah memori yang disimpan bergantung pada total memori yang tersedia pada instans Anda. Buka file `/etc/default/grub` menggunakan editor teks pilihan Anda, temukan baris yang dimulai dengan `GRUB_CMDLINE_LINUX_DEFAULT`, lalu tambahkan parameter `crashkernel` dalam format berikut: `crashkernel=`*`memory_to_reserve`*. Misalnya, untuk mencadangkan `256MB`, modifikasi file `grub` sebagai berikut:

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=256M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. Simpan perubahan Anda dan tutup file `grub`.
5. Membangun kembali file GRUB2 konfigurasi.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Pada instans yang berbasis prosesor Intel dan AMD, perintah `send-diagnostic-interrupt` mengirimkan non-maskable interrupt (NMI) yang tidak dikenal ke instans. Anda harus mengonfigurasi kernel agar mengalami crash saat menerima NMI yang tidak dikenal. Buka file `/etc/sysctl.conf` dengan menggunakan editor teks pilihan Anda dan tambahkan berikut ini.

```
kernel.unknown_nmi_panic=1
```

7. Boot ulang dan terhubung kembali ke instans Anda.
8. Verifikasi bahwa kernel telah dilakukan boot dengan parameter `crashkernel` yang benar.

```
$ grep crashkernel /proc/cmdline
```

Contoh output berikut mengindikasikan konfigurasi yang berhasil.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=256M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. Verifikasi bahwa layanan kdump berjalan.

```
[ec2-user ~]$ systemctl status kdump.service
```

Contoh output berikut menunjukkan hasil jika layanan kdump berjalan.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> Secara default, file dump crash disimpan ke `/var/crash/`. Untuk mengubah lokasi, modifikasi file `/etc/kdump.conf` menggunakan editor teks pilihan Anda.

Untuk mengonfigurasi SUSE Linux Enterprise, Ubuntu, atau Red Hat Enterprise Linux

Pada instans yang berbasis prosesor Intel dan AMD, perintah `send-diagnostic-interrupt` mengirimkan non-maskable interrupt (NMI) yang tidak dikenal ke instans. Anda harus mengonfigurasi kernel agar macet ketika menerima NMI yang tidak dikenal dengan menyesuaikan file konfigurasi untuk sistem operasi Anda. Untuk informasi tentang cara mengonfigurasi kernel agar crash, lihat dokumentasi untuk sistem operasi Anda:

- SUSE Linux Enterprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

Instans Windows

Untuk mengonfigurasi Windows agar menghasilkan dump memori saat terjadi kesalahan penghentian

1. Terhubung ke instans Anda.
2. Buka Panel Kontrol dan pilih Sistem, Pengaturan sistem lanjutan.
3. Dalam kotak dialog Properti Sistem, pilih tab Lanjutan.
4. Di bagian Startup and Pemulihan, pilih Pengaturan...
5. Di bagian Kegagalan sistem, konfigurasikan pengaturan sesuai kebutuhan, lalu pilih OKE.

Untuk informasi selengkapnya tentang mengonfigurasi kesalahan penghentian Windows, lihat Gambaran umum opsi file dump memori untuk Windows.

Kirimkan interupsi diagnostik

Setelah menyelesaikan perubahan konfigurasi yang diperlukan, Anda dapat mengirim interupsi diagnostik ke instans menggunakan AWS CLI atau Amazon EC2 API.

AWS CLI

Untuk mengirim interupsi diagnostik ke instans Anda

Gunakan perintah send-diagnostic-interrupt.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

Untuk mengirim interupsi diagnostik ke instans Anda

Gunakan Send-EC2DiagnosticInterruptcmdlet.

```
Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Riwayat dokumen untuk Panduan Pengguna Amazon EC2

Tabel berikut menjelaskan penambahan penting pada Panduan Pengguna Amazon EC2 mulai tahun 2019. Kami juga sering memperbarui panduan untuk mengatasi umpan balik yang Anda kirimkan kepada kami.

Perubahan	Deskripsi	Tanggal
IMDSv2 penegakan	Anda dapat menerapkan penggunaan IMDSv2 di tingkat akun untuk masing-masing AWS Region. Saat diberlaku kan, instance hanya dapat diluncurkan jika dikonfigurasi untuk membutuhkan. IMDSv2	Februari 24, 2026
Virtualisasi bersarang	Anda dapat menjalankan hypervisor, seperti Hyper-V dan KVM, di dalam instans Amazon EC2 tervirtualisasi.	Februari 16, 2026
Reservasi Kapasitas yang Dapat Diputus	Reservasi Kapasitas Interrupt ible membantu Anda membuat kapasitas yang tidak terpakai tersedia sementara untuk beban kerja lain dalam akun Anda.	November 21, 2025
Topologi instans untuk instance P6-B300	Anda bisa mendapatkan informasi topologi instance untuk `p6-b300.48xlarge` instance.	November 18, 2025
Keturunan AMI	Anda sekarang dapat melacak asal usul AMI dengan mendapatkan daftar semua leluhurnya AMIs.	November 12, 2025

Topologi Reservasi Kapasitas	Anda dapat menggunakan DescribeCapacityReservationTopology API untuk menjelaskan lokasi kapasitas cadangan Anda relatif satu sama lain dalam hierarki jaringan sebelum meluncurkan instance.	Oktober 28, 2025
Optimalkan CPUs untuk penghematan lisensi	Sekarang Anda dapat mengonfigurasi aktif CPUs untuk menghemat biaya lisensi untuk instance Windows dan SQL Server yang disertakan lisensi.	Oktober 15, 2025
Manajer Kapasitas EC2 Baru	Amazon EC2 menambahkan Manajer Kapasitas EC2 yang memungkinkan Anda memantau, menganalisis, dan mengelola penggunaan kapasitas di seluruh Instans Sesuai Permintaan, Instans Spot, dan Reservasi Kapasitas dari satu lokasi.	Oktober 15, 2025
AWSEC2CapacityManagerServiceRolePolicy — kebijakan terkelola baru	Amazon EC2 menambahkan kebijakan AWSEC2 CapacityManagerServiceRolePolicy terkelola untuk memungkinkan Anda mengelola sumber daya kapasitas dan berintegrasi dengan AWS Organizations atas nama Anda.	Oktober 15, 2025

Metrik GPUPowerUtilization	GPUPowerUtilization Metrik baru untuk instance komputasi yang dipercepat.	Oktober 13, 2025
Dukungan Titik Akhir IPv6 Connect Instans EC2	EC2 Instance Connect Endpoint sekarang mendukung konektivitas IPv6. Sekarang Anda dapat mengonfigurasi EC2 Instance Connect Endpoint untuk mendukung dual-stack atau IPv6 hanya untuk terhubung ke instans dengan alamat. IPv6	Oktober 2, 2025
Diizinkan AMIs - parameter baru	Diizinkan AMIs, fitur yang memungkinkan Anda membatasi penemuan dan penggunaan AMIs dalam diri Anda Akun AWS, sekarang mendukung empat parameter baru: kode AWS Marketplace produk, nama AMI, periode maksimum sejak penghenti an AMI, dan usia maksimum untuk. AMIs	September 25, 2025
Statistik kinerja terperinci untuk volume penyimpanan misalnya	Amazon EC2 menyediak an statistik kinerja resolusi tinggi real-time untuk volume penyimpanan NVMe instans yang dilampirkan ke instans berbasis Nitro.	September 16, 2025

Pembaruan Host Khusus Amazon EC2 Mac	Host Khusus Amazon EC2 Mac mendukung pemulihan otomatis Host Khusus dan pemeliharaan host berbasis reboot.	Agustus 28, 2025
Salinan AMI untuk Local Zones	Anda sekarang dapat menyalin Amazon EBS yang didukung AMIs ke dan dari Local Zones.	Agustus 28, 2025
Amazon EC2 ImageReferencesAccessPolicy - kebijakan terkelola baru	Amazon EC2 menambahkan kebijakan ImageReferencesAccessPolicy terkelola AmazonEC2 untuk memberikan izin untuk memindai semua jenis sumber daya yang didukung oleh API EC2. DescribeImageReferences	Agustus 26, 2025

Laporan penggunaan AMI	Jika Anda membagikan Amazon Machine Images (AMIs) dengan yang Akun AWS lain—baik dengan organisasi Akun AWS, organisasi, unit organisasi (OUs), atau publik—Anda dapat melihat bagaimana ini AMIs digunakan dengan membuat laporan penggunaan AMI. Laporan memberikan visibilitas yang Akun AWS menggunakan AMI Anda dalam instans EC2 atau templat peluncuran, dan berapa banyak instans atau templat peluncuran yang mereferensikan setiap AMI.	Agustus 26, 2025
Referensi AMI	Anda dapat mengidentifikasi AWS sumber daya yang mereferensikan Amazon Machine Images (AMIs) tertentu, terlepas dari AMIs apakah itu publik atau pribadi, atau siapa yang memilikinya. Visibilitas ini membantu Anda memastikan sumber daya Anda menggunakan kepatuhan AMIs terbaru.	Agustus 26, 2025
Ubah Titik Akhir Connect Instans EC2	Sekarang Anda dapat memodifikasi Titik Akhir Instance Connect EC2 yang ada menggunakan AWS CLI atau SDK.	Agustus 14, 2025

Peningkatan berbagi kapasitas Reservasi	Sekarang Anda dapat membagikan Reservasi Kapasitas yang Anda buat di grup penempatan klaster.	Agustus 12, 2025
Kebijakan terkelola yang diperbarui untuk EC2 Instance Connect Endpoint	Untuk mendukung modifikasi Titik Akhir Instance Connect EC2 yang ada, Amazon EC2 memperbarui `Ec2InstanceConnectEndpoint` kebijakan untuk menambahkan izin untuk menetapkan dan membatalkan penetapan alamat IPv6 serta memodifikasi grup keamanan pada antarmuka jaringan yang dibuat oleh Titik Akhir Instance Connect EC2. Amazon EC2 juga memperbarui kebijakan ini untuk mengganti operator `Null` kondisi dengan operator `StringLike` kondisi.	Juli 31, 2025
Topologi instans - dukungan Wilayah tambahan	DescribeInstanceTopology API sekarang tersedia di Asia Pasifik (Melbourne).	Juli 31, 2025
Paksa mengakhiri	Anda sekarang dapat memaksa menghentikan instance Anda.	Juli 31, 2025
Topologi instans - dukungan Wilayah tambahan	DescribeInstanceTopology API sekarang tersedia di AWS GovCloud (AS-Barat).	Juli 24, 2025

Lewati shutdown OS selama penghentian instans	Anda dapat melewati shutdown sistem operasi (OS) yang anggun saat mengakhiri sebuah instance.	Juli 23, 2025
Lewati shutdown OS selama penghentian instance	Anda dapat melewati shutdown sistem operasi (OS) yang anggun saat menghenti kan sebuah instance.	Juli 23, 2025
Blok Kapasitas P6-B200 di us-east-1	Blok Kapasitas P6-B200 sekarang tersedia di AS Timur (Virginia N.) -. `us-east-1`	Juli 23, 2025
Kebijakan terkelola yang diperbarui untuk peran terkait layanan Peluncuran Cepat EC2	Untuk membantu mencegah sumber daya yatim piatu, Amazon EC2 memperbar ui kebijakan ini untuk menambahkan izin untuk mendeskripsikan volume, atribut volume, dan antarmuka jaringan, serta menghapus volume dan antarmuka jaringan yang dibuat oleh Peluncuran Cepat EC2.	Juli 17, 2025
Konsol Serial EC2 - dukungan Wilayah tambahan	EC2 Serial Console sekarang juga tersedia di Asia Pasifik (Thailand) dan Meksiko (Tengah).	Juli 15, 2025
EC2 Instance Connect - dukungan Wilayah tambahan	EC2 Instance Connect sekarang juga tersedia di Asia Pasifik (Thailand) dan Meksiko (Tengah).	Juli 15, 2025

Stempel waktu paket perangkat keras	Anda dapat mengaktifkan stempel waktu paket perangkat keras pada instans EC2 Anda untuk menambahkan stempel waktu presisi nanodetik 64-bit ke setiap paket jaringan yang masuk.	Juni 23, 2025
Hapus snapshot selama deregistrasi AMI	Saat membatalkan pendaftaran AMI, Anda dapat secara otomatis menghapus snapshot terkait secara bersamaan.	28 Mei 2025
Migrasi reboot yang diprakarsai pengguna	Saat instans Anda menerima pemberitahuan acara reboot terjadwal EC2, instans diaktifkan secara default untuk migrasi instans saat Anda me-reboot instance sebelum acara.	Mei 20, 2025
Konfigurasi SIP untuk instans Amazon EC2 Mac	Anda dapat mengonfigurasi pengaturan Perlindungan Integritas Sistem (SIP) untuk instans Mac x86 dan instans Apple silicon Mac.	Mei 20, 2025
Delegasi kepemilikan volume root	Anda sekarang dapat mengotomatiskan delegasi kepemilikan volume root untuk volume root Amazon EBS saat memperbarui sistem operasi pada instance Apple silicon Mac.	Mei 20, 2025

Topologi instans untuk instance P6-B200	Anda bisa mendapatkan informasi topologi instance untuk `p6-b200.48xlarge` instance.	15 Mei 2025
Kebijakan terkelola yang diperbarui untuk peran terkait layanan Peluncuran Cepat EC2	Memperbarui kebijakan peran terkait layanan Peluncuran Cepat EC2 dengan akses untuk membuat dan memelihara aturan EventBridge acara Amazon, serta tindakan lain untuk meningkatkan pengalaman Peluncuran Cepat EC2. Untuk informasi selengkapnya tentang izin yang diberikan oleh peran terkait layanan, lihat Izin yang diberikan oleh. `EC2FastLaunchServiceRolePolicy`	14 Mei 2025

Kebijakan terkelola yang diperbarui untuk kebijakan akses penuh EC2 Fast Launch	Memperbarui kebijakan akses penuh Peluncuran Cepat EC2 dengan izin untuk Membuat dan Memodifikasi operasi Template Peluncuran, untuk membuat sumber daya jaringan dan grup keamanan, mengotorisasi aturan masuk, dan menghapus sumber daya yang dibuat oleh Peluncura n Cepat EC2. Kebijakan ini juga dapat menjelaskan dan membuat CloudFormation tumpukan, dan menghapus tumpukan yang dibuat oleh Peluncuran Cepat EC2.	14 Mei 2025
Orientasi yang disederha nakan untuk Peluncuran Cepat EC2	Memperbarui Peluncuran Cepat EC2 untuk menyederh anakan proses orientasi.	14 Mei 2025
AWS Config integrasi dengan Diizinkan AMIs	Gunakan AWS Config aturan ec2- instance-launched-with-allowed -ami untuk memeriksa apakah instance yang sedang berjalan atau dihentikan diluncurkan dengan AMIs yang memenuhi kriteria Diizinkan Anda. AMIs	Maret 11, 2025

Kebijakan AWSEC2CapacityReservationFleetRolePolicy terkelola yang diperbarui	Amazon EC2 memperbarui kebijakan `AWSEC2CapacityReservationFleetRolePolicy` terkelola untuk menggunakan operator `ArnLike` kondisi, bukan operator `StringLike` kondisi.	Maret 3, 2025
Salinan AMI berbasis waktu	Anda sekarang dapat meminta durasi penyelesaian untuk operasi penyalinan AMI yang didukung EBS untuk memastikan bahwa salinan AMI diselesaikan dalam jangka waktu tertentu.	Februari 25, 2025
AmazonEC2ReadOnlyAccessKebijakan yang diperbarui	Amazon EC2 menambahkan `GetSecurityGroupsForVpc` operasi ke kebijakan Amazon EC2 ReadOnlyAccess yang ada.	Desember 27, 2024
Instans terkelola	Anda sekarang dapat melihat instans terkelola Amazon EC2 di konsol EC2.	Desember 1, 2024

Kebijakan deklaratif	Anda sekarang dapat menggunakan kebijakan deklaratif untuk menerapka n pengaturan tingkat akun di beberapa Wilayah dan akun secara bersamaan. Kebijakan deklaratif didukung untuk mengonfigurasi akses konsol serial EC2, Diizinkan, default IMDS AMIs, dan memblokir setelan akses publik untuk,, dan snapshot. VPCs AMIs Untuk informasi selengkapnya, lihat Kebijakan deklaratif di Panduan AWS Organizations Pengguna, serta dokumentasi khusus untuk setiap fitur yang didukung.	Desember 1, 2024
Diizinkan AMIs	Anda sekarang dapat mengontrol penemuan dan penggunaan AMI di Amazon EC2 dengan menentuka n kriteria yang AMIs harus dipenuhi.	Desember 1, 2024
Blok Kapasitas Instan	Anda sekarang dapat memesan Blok Kapasitas untuk ML, yang dapat dimulai segera setelah 30 menit.	November 21, 2024
Reservasi Kapasitas Bertanggal Masa Depan	Anda sekarang dapat meminta Reservasi Kapasitas untuk tanggal yang akan datang.	November 21, 2024

Perluas Blok Kapasitas	Anda sekarang dapat memperpanjang durasi Blok Kapasitas yang ada.	November 21, 2024
Blok Kapasitas 6 bulan	Anda sekarang dapat memesan Blok Kapasitas untuk ML hingga 6 bulan (182 hari).	November 21, 2024
Set filter tersimpan	Anda sekarang dapat membuat grup filter yang disesuaikan dan menggunak annya kembali untuk melihat sumber daya EC2 Anda secara efisien.	November 20, 2024
Perlindungan kinerja	Saat menggunakan pemilihan jenis instans berbasis atribut untuk Armada EC2 atau Armada Spot, kini Anda dapat mengaktifkan perlindungan performa untuk memastika n bahwa jenis instans yang dipilih serupa atau melebihi baseline kinerja yang ditentuka n.	November 20, 2024
Reservasi Kapasitas saja	Sekarang Anda dapat menentukan bahwa instance hanya akan berjalan di grup sumber daya Reservasi Kapasitas atau Reservasi Kapasitas.	November 20, 2024

Identifikasi sumber AMI	Anda sekarang dapat mengidentifikasi sumber AMI yang digunakan untuk membuat AMI.	November 13, 2024
Kapasitas split	Anda dapat memisahkan kapasitas dari Reservasi Kapasitas yang ada untuk membuat reservasi baru.	Oktober 30, 2024
Pindahkan kapasitas	Anda sekarang dapat memindahkan kapasitas dari satu Reservasi Kapasitas ke Reservasi Kapasitas lainnya.	Oktober 30, 2024
Tutorial pemula	Dua tutorial baru untuk pemula: Luncurkan instans EC2 pertama saya dan Luncurkan instance EC2 pengujian dan sambungkan ke sana.	Oktober 21, 2024
Dukungan Windows Server 2025	Tambahkan dukungan untuk Windows Server 2025.	Oktober 16, 2024
Tampilan Global EC2	EC2 Global View sekarang memungkinkan Anda untuk melihat Reservasi Kapasitas dan Blok Kapasitas di akun Anda di semua Wilayah.	Oktober 16, 2024

Pemeliharaan host migrasi langsung	Host Khusus Amazon EC2 sekarang mendukung pemeliharaan host migrasi langsung, yang secara otomatis memigrasikan instans yang didukung dari Host Khusus yang terganggu ke Host Khusus pengganti tanpa menghentikan dan memulai ulang.	Oktober 15, 2024
Penugasan penagihan untuk Reservasi Kapasitas bersama	Anda sekarang dapat menetapkan penagihan kapasitas yang tersedia dari Reservasi Kapasitas bersama ke akun konsumen yang dimiliki oleh organisasi yang sama AWS .	Oktober 14, 2024
Jam perangkat keras PTP - dukungan Wilayah tambahan	Jam perangkat keras PTP sekarang juga tersedia di AS Timur (Ohio) dan Asia Pasifik (Malaysia).	September 23, 2024
EC2 Instance Connect mendukung IPv6	Anda sekarang dapat menggunakan EC2 Instance Connect untuk menyambung ke IPv6 alamat publik instans Anda.	September 23, 2024

Daftar awalan EC2 Instance Connect	Sekarang Anda dapat memilih daftar awalan terkelola untuk alamat IPv4 atau IPv6 saat membuat aturan di grup keamanan Anda untuk mengizinkan lalu lintas SSH dari layanan EC2 Instance Connect.	September 23, 2024
Kemampuan baru untuk mengelola Reservasi Kapasitas Sesuai Permintaan	Sekarang Anda dapat membagi Reservasi Kapasitas , memindahkan kapasitas antara Reservasi Kapasitas , dan mengubah atribut kelayakan instans dari Reservasi Kapasitas Anda.	Agustus 14, 2024
Dukungan hibernasi untuk C6g, C6gN, C6gd, C7g, C7gd, m6g, m6gd, m7g, m7gd, r6g, dan r6gd	Hibernasi instans yang baru diluncurkan yang berjalan pada jenis instans C6g, C6gd, C6gd, C7gd, M6g, M6gd, M7g, M7gd, R6g, dan R6gd.	Juli 30, 2024
Dukungan hibernasi untuk AMIs itu mendukung jenis instans Graviton	Hibernasi instans yang baru diluncurkan yang diluncurk an dari Amazon Linux atau Ubuntu AMI yang mendukung jenis instans Graviton.	Juli 30, 2024
Jenis instans tambahan yang didukung untuk Credential Guard	Anda sekarang dapat mengaktifkan Credential Guard untuk instance C7i, C7-Flex, M7i, M7i-Flex, R7i, R7i-Flex, dan T3.	Juni 26, 2024

Pencari tipe instans EC2 — parameter tambahan	Pencari tipe instans EC2 sekarang menyediakan parameter tambahan bagi Anda untuk menentukan persyaratan yang lebih rinci untuk beban kerja Anda.	Juni 5, 2024
Kebijakan terkelola baru untuk Peluncuran Cepat EC2	Menambahkan EC2FastLaunchFullAccess kebijakan untuk melakukan tindakan API yang terkait dengan fitur Peluncuran Cepat EC2 dari sebuah instance.	14 Mei 2024
Perlindungan deregistrasi AMI	Anda dapat mengaktifkan perlindungan deregistrasi pada AMI untuk mencegah penghapusan yang tidak disengaja atau berbahaya.	April 23, 2024
Jam perangkat keras PTP - dukungan tipe instance	Jam perangkat keras PTP sekarang tersedia pada jenis instans M7a, M7g, M7i, R7a, dan R7i.	April 22, 2024
Menambahkan pertimbangan kinerja Nitro untuk jaringan yang ditingkatkan	Halaman ini berfokus pada pertimbangan jaringan untuk membantu penyetelan kinerja instans Amazon EC2 berbasis Nitro Anda.	April 4, 2024

Kebijakan terkelola baru untuk snapshot EBS berbasis VSS	Amazon EC2 VSS memiliki kebijakan terkelola IAM baru yang tersedia yang dapat Anda tambahkan ke peran profil instans untuk memastikan izin tetap up-to-date dan mengikuti praktik terbaik.	Maret 28, 2024
Jam perangkat keras PTP - AS Timur (Virginia N.)	Jam perangkat keras PTP sekarang tersedia di Wilayah AS Timur (Virginia N.).	26 Maret 2024
Tetapkan IMDSv2 sebagai default akun	Anda dapat mengatur semua peluncuran instans EC2 baru di akun Anda untuk menggunakan Layanan Metadata Instans Versi 2 () IMDSv2 secara default.	Maret 25, 2024
Tag Linux baru AMIs yang dibuat dari snapshot	Saat Anda membuat AMI Linux dari snapshot, Anda dapat menandai AMI baru.	Maret 7, 2024
Tag baru AMIs dan snapshot saat menyalin	Saat Anda menyalin AMI, Anda dapat menandai AMI baru dan snapshot baru dengan tag yang sama, atau Anda dapat menandainya dengan tag yang berbeda.	Maret 7, 2024

Hapus halaman Paket AWS Manajemen	Paket AWS Manajemen terutama digunakan dengan Windows Server 2012 dan sebelumnya. Versi platform OS lama tersebut tidak lagi didukung. Untuk mengelola dan memecahkan masalah armada server yang berjalan di AWS dan lokal, lihat AWS Systems Manager Manajer Armada.	Februari 12, 2024
EC2 Instance Connect sudah diinstal sebelumnya di macOS AMIs	EC2 Instance Connect sekarang sudah diinstal sebelumnya di macOS Sonoma 14.2.1 atau yang lebih baru, macOS Ventura 13.6.3 atau yang lebih baru, dan macOS Monterey 12.7.2 atau yang lebih baru. AMIs	Januari 26, 2024
Dukungan EC2 Instance Connect untuk CentOS, macOS, dan RHEL	Anda sekarang dapat menginstal EC2 Instance Connect pada CentOS, macOS, dan RHEL yang didukung. AMIs	6 Desember 2023
Dukungan hibernasi untuk C7a, C7i, R7a, R7i, dan R7iz	Hibernasikan instans yang baru diluncurkan yang berjalan pada tipe instans C7a, C7i, R7a, R7i, dan R7iz.	1 Desember 2023

Pemilih tipe instans EC2 Amazon Q	Pemilih tipe instans EC2 Amazon Q mempertim bangkan kasus penggunaa n, tipe beban kerja, dan preferensi produsen CPU, serta cara Anda mempriori taskan harga dan performa. Pemilih tipe instans EC2 Amazon Q kemudian menggunakan data ini untuk memberikan panduan dan saran untuk tipe instans Amazon EC2 yang paling cocok untuk beban kerja baru Anda.	28 November 2023
EC2 Tingkat Gratis	Anda dapat melacak penggunaan Tingkat Gratis EC2 dari Dasbor EC2.	26 November 2023
Konsol-ke-Kode	Console-to-Code dapat membantu Anda memulai dengan kode otomatisasi Anda. Console-to-Codemer ekam tindakan konsol Anda, dan kemudian menggunakan AI generatif untuk menyarank an kode dalam infrastruktur pilihan Anda-sebagai format kode. Anda dapat menggunak an kode tersebut sebagai titik awal, menyesuaikannya agar siap produksi untuk kasus penggunaan khusus Anda.	26 November 2023

Batas waktu pelacakan koneksi idle yang dapat dikonfigurasi	Koneksi grup keamanan yang tetap idle dapat menyebabkan terbebaninya pelacakan koneksi dan menyebabkan koneksi tidak dilacak dan paket terputus. Anda sekarang dapat mengatur batas waktu dalam hitungan detik untuk pelacakan koneksi grup keamanan pada antarmuka jaringan Elastis.	17 November 2023
Clock perangkat keras PTP	Instans yang didukung sekarang memiliki clock perangkat keras Precision Time Protocol (PTP). Clock perangkat keras PTP mendukung NTP atau koneksi PTP langsung.	16 November 2023
Mengubah tipe instans dari instans yang diaktifkan untuk hibernasi	Anda sekarang dapat mengubah tipe instans dari instans yang diaktifkan untuk hibernasi saat berada dalam status `stopped`.	16 November 2023
Topologi instans	Anda dapat menggunakan DescribeInstanceTopology API untuk mendeteksi lokasi instans Anda, dan kemudian menggunakan informasi ini untuk mengoptimalkan pekerjaan HPC dan ML dengan menjalankannya pada instans yang secara fisik lebih dekat satu sama lain.	13 November 2023

EC2 Fast Launch berbagi dukungan AMI	Anda sekarang dapat mengaktifkan Peluncuran Cepat EC2 pada AMI yang dibagikan dengan Anda. Saat Anda mengaktifkan Peluncuran Cepat EC2 pada AMI bersama, snapshot yang telah disediakan sebelumnya untuk peluncuran lebih cepat akan dibuat di akun Anda.	6 November 2023
Blok Kapasitas untuk ML	Sekarang Anda dapat memesan instans GPU di masa mendatang untuk mendukung beban kerja machine learning (ML) berdurasi pendek.	31 Oktober 2023
Hibernasi Instans Spot	Sekarang Anda dapat menghibernasikan Instans Spot menggunakan pengalaman hibernasi dan keluarga instans yang sama yang saat ini tersedia untuk Instans Sesuai Permintaan.	24 Oktober 2023
Pengaturan default untuk memblokir akses publik untuk AMIs	Blokir akses publik untuk sekarang AMIs diaktifkan secara default untuk semua akun baru dan untuk akun yang ada tanpa publik AMIs.	20 Oktober 2023
Tampilan Global Amazon EC2	Tampilan Global Amazon EC2 mendukung tipe sumber daya tambahan dan opsi tampilan yang dapat dikustomisasi.	18 Oktober 2023

Dukungan hibernasi untuk Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Hibernasikan instans Anda yang baru diluncurkan dari AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish).	16 Oktober 2023
Menonaktifkan AMI	Anda dapat menonaktifkan AMI untuk mencegahnya digunakan untuk peluncuran instans.	12 Oktober 2023
Pemeriksaan status EBS terlampir	Anda dapat menggunakan pemeriksaan status EBS terlampir untuk memantau apakah volume Amazon EBS yang dilampirkan ke instans dapat dijangkau.	11 Oktober 2023
Dukungan hibernasi untuk Red Hat Enterprise Linux 9	Hibernasikan instans Anda yang baru diluncurkan dari AMI Red Hat Enterprise Linux 9.	2 Oktober 2023
Dukungan hibernasi untuk Microsoft Windows Server 2022	Hibernasikan instans Anda yang baru diluncurkan dari Microsoft Windows Server 2022.	2 Oktober 2023
Dukungan hibernasi untuk AL2023	Hibernasi instance Anda yang baru diluncurkan yang diluncurkan dari AMI. AL2023	2 Oktober 2023
Memulai interupsi Instans Spot di Armada Spot	Anda dapat memilih Armada Spot di konsol Amazon EC2 dan memulai interupsi Instans Spot dalam armada sehingga Anda dapat menguji cara aplikasi di Instans Spot menangani interupsi.	21 September 2023

Blokir akses publik ke AMIs	Anda dapat mengaktifkan blokir akses publik AMIs di tingkat akun untuk memblokir setiap upaya untuk membuat AMIs publik Anda.	12 September 2023
Dukungan hibernasi untuk M7i dan M7i-flex	Hibernasikan instans yang baru diluncurkan yang berjalan pada tipe instans M7i dan M7i-flex.	22 Agustus 2023
EC2-Classic telah diusangkan	Dengan EC2-Classic, instans EC2 berjalan dalam jaringan datar tunggal yang dibagikan dengan pelanggan lain. Amazon VPC menggantikan EC2-Classic. Dengan Amazon VPC, instans Anda berjalan di cloud privat virtual (VPC) yang secara logis terisolasi dari akun AWS Anda.	8 Agustus 2023
Host Khusus	Anda dapat mengalokasikan Host Khusus pada aset perangkat keras tertentu di Outpost.	20 Juni 2023
Titik Akhir EC2 Instance Connect	Anda sekarang dapat terhubung ke sebuah instance melalui SSH atau RDP tanpa memerlukan instance untuk memiliki alamat publik. IPv4	13 Juni 2023

IMDS Package Analyzer	Anda sekarang dapat menggunakan IMDS Packet Analyzer untuk mengident ifikasi sumber panggilan IMDSv1 pada instans EC2 Anda.	1 Juni 2023
Instans bare metal Konsol Serial EC2	Konsol serial EC2 sekarang mendukung konektivitas ke port serial instans bare metal yang dipilih.	11 April 2023
Kuota templat peluncuran	Anda sekarang dapat melihat kuota untuk templat peluncura n dan versi templat peluncuran di konsol Kuota Layanan serta dengan menggunakan CLI Kuota Layanan.	3 April 2023
Notifikasi pemanfaatan Reservasi Kapasitas	AWS Health sekarang mengirimkan pemberitahuan ketika pemanfaatan kapasitas untuk Reservasi Kapasitas di akun Anda turun di bawah 20 persen.	3 April 2023
Grup Reservasi Kapasitas	Anda sekarang dapat menambahkan Reservasi Kapasitas yang dibagikan dengan Anda ke grup Reservasi Kapasitas yang Anda miliki.	30 Maret 2023
Memodifikasi opsi metadata instans	Anda sekarang dapat menggunakan konsol Amazon EC2 untuk memodifikasi opsi metadata instans.	20 Maret 2023

Pembaruan sistem operasi macOS in place	Anda sekarang dapat melakukan pembaruan sistem operasi Apple macOS pada instans M1 Mac.	14 Maret 2023
UEFI diutamakan	Anda sekarang dapat membuat AMI tunggal yang mendukung mode boot Unified Extensible Firmware Interface (UEFI) dan Legacy BIOS.	3 Maret 2023
Memodifikasi AMI untuk IMDSv2	Ubah AMI Anda yang ada sehingga instance yang diluncurkan dari AMI memerlukan secara IMDSv2 default.	28 Februari 2023
Keamanan berbasis Virtualisasi Windows - Credential Guard	Anda dapat mengaktifkan Credential Guard, fitur Keamanan berbasis virtualisasi (VBS), pada instans Amazon EC2 yang didukung.	31 Januari 2023
Kebijakan terkelola baru untuk EC2 Instance Connect Endpoint	Menambahkan `Ec2InstanceConnectEndpoint` kebijakan, yang dilampirkan ke peran AWSServiceRoleForEC2InstanceConnectterkait layanan, untuk memungkinkan Amazon EC2 melakukan tindakan atas nama Anda saat Anda membuat Titik Akhir Connect Instans EC2.	Januari 24, 2023

Alias AMI dalam templat peluncuran	Anda dapat menentukan AWS Systems Manager parameter alih-alih ID AMI di templat peluncuran Anda untuk menghindari keharusan memperbarui templat setiap kali ID AMI berubah.	19 Januari 2023
Dukungan hibernasi untuk C6i, I3en, dan M6i	Hibernasikan instans yang baru diluncurkan yang berjalan pada tipe instans C6i, I3en, dan M6i.	19 Desember 2022
Pencegahan tumpang tindih	Tingkatkan performa beban kerja basis data relasional intensif I/O Anda dan kurangi latensi tanpa berdampak negatif terhadap ketahanan data dengan pencegahan tumpang tindih, sebuah fitur penyimpanan blok.	29 November 2022
ENA Ekspres	Tingkatkan throughput dan minimalkan latensi ekor lalu lintas jaringan antara instans EC2 dengan ENA Ekspres.	28 November 2022
Salin tanda AMI	Saat Anda menyalin AMI, Anda dapat menyalin tanda AMI yang ditentukan pengguna secara bersamaan.	18 November 2022

Ukuran AMI untuk menyimpan dan memulihkan	Ukuran AMI (sebelum kompresi) yang dapat disimpan dan dipulihkan ke dan dari bucket Amazon S3 sekarang dapat mencapai hingga 5.000 GB.	16 November 2022
priceCapacityOptimizedstrategi alokasi untuk Instans Spot	Armada Spot yang menggunakan strategi alokasi `priceCapacityOptimized` melihat harga dan kapasitas untuk memilih kolam Instans Spot yang paling kecil kemungkinannya untuk terganggu dan memiliki harga paling rendah.	10 November 2022
price-capacity-optimizedstrategi alokasi untuk Instans Spot	Armada EC2 yang menggunakan strategi alokasi `price-capacity-optimized` melihat harga dan kapasitas guna memilih kolam Instans Spot yang paling kecil kemungkinannya untuk terganggu dan memiliki harga paling rendah.	10 November 2022
Membatalkan AMI yang dibagikan dengan akun Anda	Jika AMI telah dibagikan dengan Anda Akun AWS dan Anda tidak ingin lagi dibagikan dengan akun Anda, Anda dapat menghapus akun Anda dari izin peluncuran AMI.	4 November 2022
Mentransfer alamat IP Elastis	Anda sekarang dapat mentransfer alamat IP Elastis dari satu Akun AWS ke yang lain.	31 Oktober 2022

Mengganti volume root	Anda dapat mengganti volume Amazon EBS root untuk instans yang berjalan menggunakan AMI.	27 Oktober 2022
Menghubungkan instans ke basis data secara otomatis	Gunakan fitur koneksi otomatis untuk menghubungkan satu instans EC2 atau lebih dengan cepat ke basis data RDS untuk memungkinkan lalu lintas di antaranya.	10 Oktober 2022
Kuota AMI	Kuota sekarang berlaku untuk membuat dan berbagi AMIs.	10 Oktober 2022
Konfigurasikan AMI untuk IMDSv2	Konfigurasikan AMI Anda sehingga instance yang diluncurkan dari AMI memerlukan secara IMDSv2 default.	3 Oktober 2022
Memulai interupsi Instans Spot	Anda dapat memilih Instans Spot di konsol Amazon EC2 dan memulai interupsi sehingga Anda dapat menguji cara aplikasi di Instans Spot menangani interupsi.	26 September 2022
Penyedia AMI terverifikasi	Di konsol Amazon EC2, publik AMIs yang dimiliki oleh Amazon atau mitra Amazon terverifikasi ditandai Penyedia terverifikasi.	22 Juli 2022
Grup penempatan di AWS Outposts	Menambahkan strategi penyebaran host untuk grup penempatan di Outpost.	30 Juni 2022

Tuan Rumah Khusus di AWS Outposts	Anda dapat mengalokasikan Host Khusus pada AWS Outposts.	31 Mei 2022
Perlindungan penghentian instans	Untuk mencegah instans Anda berhenti secara tidak sengaja, Anda dapat mengaktifkan perlindungan penghentian untuk instans.	24 Mei 2022
Boot Aman UEFI	UEFI Secure Boot dibangun di atas proses boot aman lama Amazon EC2 dan menyediakan tambahan yang membantu pelanggan mengamankan perangkat lunak dari ancaman defense-in-depth yang bertahan selama reboot.	10 Mei 2022
NitroTPM	Nitro Trusted Platform Module (NitroTPM) adalah perangkat virtual yang disediakan oleh Sistem AWS Nitro dan sesuai dengan spesifikasi TPM 2.0.	10 Mei 2022
Peristiwa perubahan status AMI	Amazon EC2 sekarang menghasilkan peristiwa saat AMI mengubah status. Anda dapat menggunakan Amazon EventBridge untuk mendeteksi dan bereaksi terhadap peristiwa ini.	9 Mei 2022
Mendeskripsikan kunci publik	Anda dapat mengueri kunci publik dan tanggal pembuatan pasangan kunci Amazon EC2.	28 April 2022

Membuat pasangan kunci	Anda dapat menentukan format kunci (PEM atau PPK) saat membuat pasangan kunci baru.	28 April 2022
Pasang sistem FSx file Amazon saat diluncurkan	Anda dapat memasang sistem file Amazon baru atau yang sudah ada FSx untuk NetApp ONTAP atau Amazon FSx untuk OpenZFS saat peluncuran menggunakan wizard instans peluncuran baru.	12 April 2022
Wizard peluncuran instans baru	Pengalaman peluncuran yang baru dan ditingkatkan di konsol Amazon EC2, yang memberikan cara yang lebih cepat dan mudah untuk meluncurkan instans EC2.	5 April 2022
Secara otomatis menghentikan publik AMIs	Secara default, tanggal penghentian semua publik AMIs diatur ke dua tahun dari tanggal pembuatan AMI.	31 Maret 2022
Kategori metadata contoh: penskalaan otomatis/target-lifecycle-state	Saat menggunakan grup Auto Scaling, Anda dapat mengakses status siklus hidup target instans dari metadata instans.	24 Maret 2022
Waktu peluncuran terakhir AMI	`lastLaunchedTime` menunjukkan waktu AMI Anda terakhir kali digunakan untuk meluncurkan instans.	28 Februari 2022

ED25519 kunci	Kunci ED25519 sekarang didukung untuk EC2 Instance Connect dan Konsol Serial EC2.	20 Januari 2022
Platform RHEL tambahan untuk Reservasi Kapasitas	Platform Red Hat Enterprise Linux tambahan untuk Reservasi Kapasitas Sesuai Permintaan.	11 Januari 2022
Konfigurasikan Windows AMIs untuk peluncuran lebih cepat	Konfigurasikan Windows AMIs untuk meluncurkan instance hingga 65% lebih cepat, menggunakan snapshot yang telah disediakan sebelumnya.	10 Januari 2022
Tanda instans dalam metadata instans	Anda dapat mengakses tanda instans dari metadata instans.	6 Januari 2022
Reservasi Kapasitas dalam grup penempatan klaster	Anda dapat membuat Reservasi Kapasitas dalam grup penempatan klaster.	6 Januari 2022
Armada Spot launch-before-terminate	Armada Spot dapat mengakhiri Instans Spot yang menerima notifikasi penyeimbangan ulang setelah Instans Spot pengganti baru diluncurkan.	4 November 2021
Armada EC2 launch-before-terminate	Armada EC2 dapat mengakhiri Instans Spot yang menerima notifikasi penyeimbangan ulang setelah Instans Spot pengganti baru diluncurkan.	4 November 2021

Membandingkan stempel waktu	Anda dapat menentukan waktu sebenarnya dari suatu peristiwa dengan membandingkan stempel waktu instans Amazon EC2 Linux Anda dengan. ClockBound	2 November 2021
Berbagi AMIs dengan organisasi dan OUs	Anda sekarang dapat berbagi AMIs dengan AWS sumber daya berikut: organisasi dan unit organisasi (OUs).	29 Oktober 2021
Skor penempatan Spot	Dapatkan rekomendasi untuk AWS Wilayah atau Availability Zone berdasarkan persyaratan kapasitas Spot Anda.	27 Oktober 2021
Pemilihan tipe instans berbasis atribut untuk Armada Spot	Tentukan atribut yang harus dimiliki oleh instans, dan Amazon EC2 akan mengidentifikasi semua tipe instans dengan atribut tersebut.	27 Oktober 2021
Pemilihan tipe instans berbasis atribut untuk Armada EC2	Tentukan atribut yang harus dimiliki oleh instans, dan Amazon EC2 akan mengidentifikasi semua tipe instans dengan atribut tersebut.	27 Oktober 2021
Armada Reservasi Kapasitas Sesuai Permintaan	Anda dapat menggunakan Armada Reservasi Kapasitas untuk meluncurkan grup, atau armada, dari Reservasi Kapasitas.	5 Oktober 2021

Dukungan hibernasi untuk Ubuntu 20.04 LTS - Focal	Hibernasikan instans Anda yang baru diluncurkan dari AMI Ubuntu 20.04 LTS - Focal.	4 Oktober 2021
Armada EC2 dan Reservasi Kapasitas Sesuai Permintaan yang ditargetkan	Armada EC2 dapat meluncurkan Instans Sesuai Permintaan ke Reservasi Kapasitas `targeted`.	22 September 2021
Instans T3 pada Host Khusus	Dukungan untuk instans T3 di Host Khusus Amazon EC2.	14 September 2021
Dukungan hibernasi untuk RHEL, Fedora, dan CentOS	Hibernasi instance Anda yang baru diluncurkan yang diluncurkan dari RHEL, Fedora, dan CentOS. AMIs	9 September 2021
Tampilan Global Amazon EC2	Amazon EC2 Global View memungkinkan Anda untuk melihat VPCs, subnet, instans, grup keamanan, dan volume di beberapa AWS Wilayah dalam satu konsol.	1 September 2021
Dukungan hibernasi untuk C5d, M5d, dan R5d	Hibernasikan instans yang baru diluncurkan yang berjalan pada tipe instans C5d, M5d, dan R5d.	19 Agustus 2021
Pasangan kunci Amazon EC2	Amazon EC2 sekarang mendukung ED25519 kunci pada instans Linux dan Mac.	17 Agustus 2021

Prefiks untuk antarmuka jaringan	Anda dapat menetapkan rentang pribadi IPv4 atau IPv6 CIDR, baik secara otomatis atau manual, ke antarmuka jaringan Anda.	22 Juli 2021
Jendela peristiwa	Anda dapat menentukan jendela peristiwa kustom yang berulang setiap minggu untuk peristiwa terjadwal yang melakukan boot ulang, menghentikan, atau mengakhiri instans Amazon EC2 Anda.	15 Juli 2021
Dukungan sumber daya IDs dan penandaan untuk aturan grup keamanan	Anda dapat merujuk ke aturan grup keamanan berdasarkan ID sumber daya. Anda dapat menambahkan tanda ke aturan grup keamanan.	7 Juli 2021
Mengusangkan AMI	Sekarang Anda dapat menentukan waktu AMI diusangkan.	11 Juni 2021
Penagihan per-detik Windows	Amazon EC2 mengenakan biaya untuk penggunaan berbasis Windows dan SQL Server per detik, dengan biaya minimum satu menit.	10 Juni 2021
Reservasi Kapasitas di AWS Outposts	Sekarang Anda dapat menggunakan Pencadangan Kapasitas di AWS Outposts.	24 Mei 2021
Berbagi Reservasi Kapasitas	Anda sekarang dapat berbagi Reservasi Kapasitas yang dibuat Local Zones dan Wavelength Zones.	24 Mei 2021

Penggantian volume root	Anda sekarang dapat menggunakan tugas pengganti an volume root untuk mengganti volume EBS guna menjalankan instans.	22 April 2021
Simpan dan pulihkan AMI menggunakan S3	Simpan EBS yang didukung AMIs di S3 dan pulihkan dari S3 untuk mengaktifkan penyalinan lintas partisi. AMIs	6 April 2021
Konsol Serial EC2	Pecahkan masalah boot dan konektivitas jaringan dengan membuat sambungan ke port serial instans.	30 Maret 2021
Mode boot	Amazon EC2 sekarang mendukung boot UEFI pada instans EC2 berbasis AMD dan Intel yang dipilih.	22 Maret 2021
Membuat catatan DNS terbalik	Anda sekarang dapat mengatur pencarian DNS terbalik untuk alamat IP Elastis.	3 Februari 2021
Tag AMIs dan snapshot pada pembuatan AMI	Saat membuat AMI, Anda dapat menandai AMI dan snapshot dengan tanda yang sama, atau Anda dapat menandainya dengan tanda yang berbeda.	4 Desember 2020
Gunakan Amazon EventBrid ge untuk memantau peristiwa Spot Fleet	Buat EventBridge aturan yang memicu tindakan terprogra m sebagai respons terhadap perubahan dan kesalahan status Armada Spot.	20 November 2020

Gunakan Amazon EventBridge untuk memantau peristiwa Armada EC2	Buat EventBridge aturan yang memicu tindakan terprogram sebagai respons terhadap perubahan dan kesalahan status Armada EC2.	20 November 2020
Menghapus armada instant	Hapus Armada EC2 tipe `instant` dan akhiri semua instans di armada dalam satu panggilan API.	18 November 2020
Dukungan hibernasi untuk T3 dan T3a	Hibernasikan instans yang baru diluncurkan yang berjalan pada tipe instans T3 dan T3a.	17 November 2020
Pembuatan Cepat Amazon EFS	Anda dapat membuat dan memasang sistem file Amazon EFS ke instans saat peluncuran dengan menggunakan Pembuatan Cepat Amazon EFS.	9 November 2020
Kategori metadata contoh: events/recommendations/rebalance	Perkiraan waktu, dalam UTC, ketika notifikasi rekomendasi penyeimbangan ulang instans EC2 dipancarkan untuk instans.	4 November 2020
Rekomendasi penyeimbangan ulang instans EC2	Sinyal yang memberi tahu Anda saat Instans Spot berada pada risiko gangguan yang tinggi.	4 November 2020
Reservasi Kapasitas di Wavelength Zones	Reservasi Kapasitas sekarang dapat dibuat dan digunakan di Wavelength Zones.	4 November 2020

Penyeimbangan Ulang Kapasitas	Konfigurasikan Armada Spot atau Armada EC2 untuk meluncurkan Instans Spot pengganti saat Amazon EC2 memancarkan rekomendasi penyeimbangan ulang.	4 November 2020
Dukungan hibernasi untuk I3, M5ad, dan R5ad	Hibernasikan instans yang baru diluncurkan yang berjalan pada tipe instans I3, M5ad, dan R5ad.	21 Oktober 2020
Batas vCPU Instans Spot	Limit Instans Spot sekarang dikelola dalam hal jumlah v CPUs yang digunakan oleh Instans Spot yang sedang berjalan atau akan digunakan sambil menunggu pemenuhan permintaan terbuka.	1 Oktober 2020
Reservasi Kapasitas di Local Zones	Reservasi Kapasitas sekarang dapat dibuat dan digunakan di Local Zones.	30 September 2020
Dukungan hibernasi untuk M5a dan R5a	Hibernasikan instans yang baru diluncurkan yang berjalan pada tipe instans M5a dan R5a.	28 Agustus 2020
Metadata instans memberikan informasi lokasi dan penempatan instans	Bidang metadata instans baru dalam kategori `placement` : Wilayah, nama grup penempatan, nomor partisi, ID host, dan ID Zona Ketersediaan.	24 Agustus 2020

Grup Reservasi Kapasitas	Anda dapat menggunakan AWS Resource Groups untuk membuat koleksi logis dari Reservasi Kapasitas, dan kemudian menargetkan peluncuran instance ke grup tersebut.	29 Juli 2020
EC2Luncurkan v2	Anda dapat menggunakan EC2 Launch v2 untuk melakukan tugas selama startup instance, jika instance dihentikan dan kemudian dimulai, jika instance dimulai ulang, dan sesuai permintaan. EC2Launch v2 mendukung semua versi Windows Server dan menggantikan EC2 Launch dan EC2 Config.	30 Juni 2020
Bawa IPv6 alamat Anda sendiri	Anda dapat membawa sebagian atau seluruh rentang IPv6 alamat dari jaringan lokal ke AWS akun Anda.	21 Mei 2020
Meluncurkan instans menggunakan parameter Systems Manager	Anda dapat menentukan AWS Systems Manager parameter alih-alih AMI saat meluncurkan instance.	5 Mei 2020
Mengustomisasi notifikasi peristiwa terjadwal	Anda dapat mengustomisasi notifikasi peristiwa terjadwal untuk menyertakan tanda dalam notifikasi email.	4 Mei 2020

Windows Server di Host Khusus	Anda dapat menggunakan Windows Server AMIs yang disediakan oleh Amazon untuk menjalankan versi terbaru Windows Server pada Host Khusus.	7 April 2020
Menghentikan dan memulai Instans Spot	Hentikan Instans Spot Anda yang didukung oleh Amazon EBS dan mulai kapan saja, alih-alih mengandalkan perilaku penghentian interupsi.	13 Januari 2020
Penandaan sumber daya	Anda dapat memberikan tanda pada gateway internet khusus egress, gateway lokal, tabel rute gateway lokal, antarmuka virtual gateway lokal, grup antarmuka virtual gateway lokal, gabungan VPC tabel rute gateway lokal, dan gabungan grup antarmuka virtual tabel rute gateway lokal.	10 Januari 2020
Menghubungkan ke instans Anda menggunakan Session Manager	Anda dapat memulai sesi Session Manager dengan instans dari konsol Amazon EC2.	18 Desember 2019
Host Khusus dan grup sumber daya host	Host Khusus sekarang dapat digunakan dengan grup sumber daya host.	2 Desember 2019
Berbagi Host Khusus	Sekarang Anda dapat membagikan Host Khusus Anda di seluruh AWS akun.	2 Desember 2019

Spesifikasi kredit default di tingkat akun	Anda dapat mengatur spesifikasi kredit default per keluarga instans kinerja burstable di tingkat akun per AWS Wilayah.	25 November 2019
Penemuan tipe instans	Anda dapat menemukan tipe instans yang sesuai dengan kebutuhan.	22 November 2019
Host Khusus	Anda sekarang dapat mengonfigurasi Host Khusus untuk mendukung berbagai tipe instans dalam satu keluarga instans.	21 November 2019
Layanan Metadata Instans Versi 2	Anda dapat menggunakan Layanan Metadata Instans Versi 2, yang merupakan metode berorientasi sesi untuk meminta metadata instans.	19 November 2019
Elastic Fabric Adapter	Elastic Fabric Adapter sekarang dapat digunakan dengan Intel MPI 2019 Update 6.	15 November 2019
Dukungan hibernasi untuk instans Windows Sesuai Permintaan	Anda dapat menghibernasikan instans Windows Sesuai Permintaan.	14 Oktober 2019
Pembelian dalam antrean untuk Instans Terpesan	Anda dapat mengantrekan pembelian Instans Terpesan hingga tiga tahun sebelumnya.	4 Oktober 2019

Interupsi diagnostik	Anda dapat mengirimkan interupsi diagnostik ke instans yang tidak dapat dijangkau atau tidak responsif untuk memicu kepanikan kernel.	14 Agustus 2019
Strategi alokasi kapasitas yang dioptimalkan	Dengan Armada EC2 atau Armada Spot, Anda dapat meluncurkan Instans Spot dari kolam Spot dengan kapasitas optimal untuk jumlah instans yang diluncurkan.	12 Agustus 2019
Pembagian Reservasi Kapasitas Sesuai Permintaan	Sekarang Anda dapat membagikan Reservasi Kapasitas Anda di seluruh AWS akun.	29 Juli 2019
Elastic Fabric Adapter	EFA kini mendukung Open MPI 3.1.4 dan Intel MPI 2019 Update 4.	26 Juli 2019
EC2 Instance Connect	EC2 Instans Connect adalah cara sederhana dan aman untuk terhubung ke instans Anda menggunakan Secure Shell (SSH).	27 Juni 2019
Pemulihan host	Mulai ulang instans Anda secara otomatis di host baru jika terjadi kegagalan perangkat keras yang tidak terduga pada Host Khusus.	5 Juni 2019

Snapshot yang konsisten dengan aplikasi VSS	Ambil snapshot yang konsisten dengan aplikasi dari semua volume Amazon EBS yang dilampirkan ke instance Windows Anda menggunakan Run Command. AWS Systems Manager	13 Mei 2019
Asisten Platforming Ulang Windows ke Linux untuk Basis Data Microsoft SQL Server	Pindahkan beban kerja Microsoft SQL Server yang sudah ada dari sistem operasi Windows ke Linux. Tautan yang diperbarui menunjuk ke Microsoft SQL Server di Panduan Pengguna Amazon EC2.	8 Mei 2019
Peningkatan Otomatis Windows	Lakukan upgrade otomatis instans EC2 Windows menggunakan. AWS Systems Manager	6 Mei 2019
Elastic Fabric Adapter	Anda dapat melampirkan Elastic Fabric Adapter ke instans untuk mempercepat aplikasi Komputasi Performa Tinggi (HPC).	29 April 2019

Untuk informasi tentang rilis jenis instans untuk Amazon EC2, lihat Riwayat dokumen di Panduan Jenis Instans Amazon EC2.

Sejarah untuk 2018 dan sebelumnya

Tabel berikut menjelaskan penambahan penting pada Panduan Pengguna Amazon EC2 di 2018 dan tahun-tahun sebelumnya.

Fitur	Versi API	Deskripsi	Tanggal rilis
Grup penempatan partisi	15-11-2015	Grup penempatan partisi menyebarkan instans di seluruh partisi logis, sehingga memastikan bahwa instans di satu partisi tidak berbagi perangkat keras yang mendasari dengan instans yang berada di partisi lain. Untuk informasi selengkapnya, lihat Grup penempatan partisi.	20 Desember 2018
Menghibernasi instans EC2 Linux	15-11-2015	Anda dapat menghibernasi instans Linux jika diaktifkan untuk hibernasi dan memenuhi prasyarat hibernasi. Untuk informasi selengkapnya, lihat Hibernasi instans Amazon EC2 Anda.	28 November 2018
Akselerator Amazon Elastic Inference	15-11-2015	Anda dapat melampirkan akselerator Amazon EI ke instans guna menambahkan akselerasi yang didukung GPU untuk mengurangi biaya menjalankan inferensi deep learning.	28 November 2018
Konsol spot merekomendasikan armada instans	15-11-2015	Konsol Spot merekomendasikan armada instans berdasarkan praktik terbaik Spot (diversifikasi instans) untuk memenuhi spesifikasi perangkat keras minimum (vCPUs, memori, dan penyimpanan) untuk kebutuhan aplikasi Anda. Untuk informasi selengkapnya, lihat Membuat Armada Spot.	20 November 2018
Tipe permintaan Armada EC2 baru: instant	15-11-2015	Armada EC2 sekarang mendukung tipe permintaan baru, `instant`, yang dapat Anda gunakan untuk menyediakan kapasitas secara sinkron di seluruh tipe instans dan model pembelian. Permintaan `instant` mengembalikan instans yang diluncurkan dalam respons API, dan tidak mengambil tindakan lebih lanjut, sehingga memungkinkan Anda untuk	14 November 2018

Fitur	Versi API	Deskripsi	Tanggal rilis
		mengontrol jika dan waktu instans diluncurkan. Untuk informasi selengkapnya, lihat Jenis permintaan Armada EC2 dan Armada Spot.	
Informasi penghematan Spot	15-11-2015	Anda dapat menampilkan penghematan yang dihasilkan dari penggunaan Instans Spot untuk satu Armada Spot atau untuk semua Instans Spot. Untuk informasi selengkapnya, lihat Penghematan dari pembelian Instans Spot.	5 November 2018
Dukungan konsol untuk mengoptimalkan opsi CPU	15-11-2015	Saat meluncurkan instans, Anda dapat mengoptimalkan opsi CPU untuk menyesuaikan beban kerja atau kebutuhan bisnis tertentu menggunakan konsol Amazon EC2. Untuk informasi selengkapnya, lihat Opsi CPU untuk instans Amazon EC2.	31 Oktober 2018
Dukungan konsol untuk membuat templat peluncuran dari instans	15-11-2015	Anda dapat membuat templat peluncuran dengan instans sebagai dasar untuk templat peluncuran baru menggunakan konsol Amazon EC2. Untuk informasi selengkapnya, lihat Buat template peluncuran Amazon EC2.	30 Oktober 2018
Reservasi Kapasitas Sesuai Permintaan	15-11-2015	Anda dapat memesan kapasitas untuk instans Amazon EC2 di Zona Ketersediaan tertentu untuk durasi waktu berapa pun. Hal ini memungkinkan Anda untuk membuat dan mengelola reservasi kapasitas secara independen dari diskon penagihan yang ditawarkan Instans Terpesan (RI). Untuk informasi selengkapnya, lihat Cadangan kapasitas komputasi dengan Reservasi Kapasitas Sesuai Permintaan EC2.	25 Oktober 2018

Fitur	Versi API	Deskripsi	Tanggal rilis
Bawa Alamat IP Anda Sendiri (BYOIP)	15-11-2015	Anda dapat membawa sebagian atau seluruh rentang IPv4 alamat publik dari jaringan lokal ke AWS akun Anda. Setelah Anda membawa rentang alamat ke AWS, itu muncul di akun Anda sebagai kumpulan alamat. Anda dapat membuat alamat IP Elastis dari kolam alamat Anda dan menggunakannya dengan sumber daya AWS . Untuk informasi selengkapnya, lihat Bawa alamat IP Anda sendiri (BYOIP) ke Amazon EC2.	23 Oktober 2018
Dukungan tanda Host Khusus saat pembuatan dan konsol	15-11-2015	Anda dapat menandai Host Khusus saat pembuatan, dan dapat mengelola tanda Host Khusus menggunakan konsol Amazon EC2. Untuk informasi selengkapnya, lihat Alokasikan Host Khusus Amazon EC2 untuk digunakan di akun Anda.	8 Oktober 2018
Dukungan konsol untuk penskalaan terjadwal pada Armada Spot	15-11-2015	Meningkatkan atau mengurangi kapasitas armada saat ini berdasarkan tanggal dan waktu. Untuk informasi selengkapnya, lihat Penskalaan terjadwal: Scale Spot Fleet sesuai jadwal.	20 September 2018
Strategi alokasi untuk Armada EC2	15-11-2015	Anda dapat menentukan apakah kapasitas Sesuai Permintaan dipenuhi berdasarkan harga (harga terendah dahulu) atau prioritas (prioritas tertinggi dahulu). Anda dapat menentukan jumlah kolam Spot untuk mengalokasikan kapasitas Spot target. Untuk informasi selengkapnya, lihat Gunakan strategi alokasi untuk menentukan bagaimana Armada EC2 atau Armada Spot memenuhi kapasitas Spot dan Sesuai Permintaan.	26 Juli 2018

Fitur	Versi API	Deskripsi	Tanggal rilis
Strategi alokasi untuk Armada Spot	15-11-2015	Anda dapat menentukan apakah kapasitas Sesuai Permintaan dipenuhi berdasarkan harga (harga terendah dahulu) atau prioritas (prioritas tertinggi dahulu). Anda dapat menentukan jumlah kolam Spot untuk mengalokasikan kapasitas Spot target. Untuk informasi selengkapnya, lihat Gunakan strategi alokasi untuk menentukan bagaimana Armada EC2 atau Armada Spot memenuhi kapasitas Spot dan Sesuai Permintaan.	26 Juli 2018
Otomatiskan siklus hidup snapshot	15-11-2015	Anda dapat menggunakan Amazon Data Lifecycle Manager guna mengotomatisasi pembuatan dan penghapusan snapshot untuk volume EBS Anda. Untuk informasi selengkapnya, lihat Amazon Data Lifecycle Manager.	12 Juli 2018
Opsi CPU templat peluncuran	15-11-2015	Saat Anda membuat templat peluncuran alat baris perintah, Anda dapat mengoptimalkan opsi CPU untuk menyesuaikan beban kerja atau kebutuhan bisnis tertentu. Untuk informasi selengkapnya, lihat Buat template peluncuran Amazon EC2.	11 Juli 2018
Menandai Host Khusus	15-11-2015	Anda dapat menandai Host Khusus.	3 Juli 2018
Mendapatkan output konsol terbaru	15-11-2015	Anda dapat mengambil output konsol terbaru untuk beberapa jenis instans saat Anda menggunakan get-console-output AWS CLI perintah.	9 Mei 2018

Fitur	Versi API	Deskripsi	Tanggal rilis
Mengoptimalkan opsi CPU	15-11-2015	Saat meluncurkan instans, Anda dapat mengoptimalkan opsi CPU untuk menyesuaikan beban kerja atau kebutuhan bisnis tertentu. Untuk informasi selengkapnya, lihat Opsi CPU untuk instans Amazon EC2.	8 Mei 2018
Armada EC2	15-11-2015	Anda dapat menggunakan Armada EC2 untuk meluncurkan grup instans di berbagai tipe instans EC2 dan Zona Ketersediaan, dan di seluruh model pembelian Instans Sesuai Permintaan, Instans Terpesan, dan Instans Spot. Untuk informasi selengkapnya, lihat Armada EC2 dan Armada Spot.	2 Mei 2018
Instans Sesuai Permintaan dalam Armada Spot	15-11-2015	Anda dapat menyertakan permintaan untuk kapasitas Sesuai Permintaan dalam permintaan Armada Spot untuk memastikan bahwa Anda tetap memiliki kapasitas instans. Untuk informasi selengkapnya, lihat Armada EC2 dan Armada Spot.	2 Mei 2018
Menandai snapshot EBS saat pembuatan	15-11-2015	Anda dapat menerapkan tanda ke snapshot selama pembuatan.	2 April 2018
Mengubah grup penempatan	15-11-2015	Anda dapat memindahkan instans ke dalam atau ke luar grup penempatan, atau mengubah grup penempatannya. Untuk informasi selengkapnya, lihat Ubah penempatan untuk sebuah EC2 instance.	1 Maret 2018
Sumber daya yang lebih panjang IDs	15-11-2015	Anda dapat menggunakan format ID yang lebih panjang untuk mendapatkan lebih banyak tipe sumber daya.	9 Februari 2018

Fitur	Versi API	Deskripsi	Tanggal rilis
Peningkatan performa jaringan	15-11-2015	Instans di luar grup penempatan klaster sekarang dapat memperoleh keuntungan dari peningkatan bandwidth saat mengirim atau menerima lalu lintas jaringan antara instans lain atau Amazon S3.	24 Januari 2018
Menandai alamat IP Elastis	15-11-2015	Anda dapat menandai alamat IP Elastis.	21 Desember 2017
Layanan Amazon Time Sync	15-11-2015	Anda dapat menggunakan Layanan Amazon Time Sync agar waktu di instans Anda selalu akurat. Untuk informasi selengkapnya, lihat Jam presisi dan sinkronisasi waktu pada instans EC2 Anda.	29 November 2017
T2 Unlimited	15-11-2015	Instans T2 Unlimited dapat melonjak melampaui dasar selama yang dibutuhkan. Untuk informasi selengkapnya, lihat Instance performa yang dapat melonjak.	29 November 2017
Templat peluncuran	15-11-2015	Templat peluncuran dapat berisi semua atau beberapa parameter untuk meluncurkan instans, sehingga Anda tidak perlu menentukannya setiap kali meluncurkan instans. Untuk informasi selengkapnya, lihat Simpan parameter peluncuran instans di templat peluncuran Amazon EC2.	29 November 2017
Penempatan sebaran	15-11-2015	Grup penempatan sebaran direkomendasikan untuk aplikasi yang memiliki instans penting dalam jumlah kecil yang harus disimpan terpisah satu sama lain. Untuk informasi selengkapnya, lihat Grup penempatan tersebar.	29 November 2017

Fitur	Versi API	Deskripsi	Tanggal rilis
Hibernasi Instans Spot	15-11-2015	Layanan Spot dapat menghibernasi Instans Spot jika terjadi interupsi.	28 November 2017
Pelacakan target Armada Spot	15-11-2015	Anda dapat mengatur kebijakan penskalaan pelacakan target untuk Armada Spot. Untuk informasi selengkapnya, lihat Penskalaan pelacakan target: Skala Armada Spot dengan menargetkan nilai untuk metrik tertentu.	17 November 2017
Armada Spot berintegrasi dengan Elastic Load Balancing	15-11-2015	Anda dapat melampirkan satu penyeimbang beban atau lebih ke Armada Spot.	10 November 2017
Menggabungkan dan memisahkan Instans Terpesan Konvertibel	15-11-2015	Anda dapat menukar (menggabungkan) dua atau lebih Instans Terpesan Konvertibel dengan Instans Terpesan Konvertibel yang baru. Anda juga dapat menggunakan proses modifikasi untuk memisahkan Instans Terpesan Konvertibel menjadi beberapa reservasi yang lebih kecil. Untuk informasi selengkapnya, lihat Menukar Instans Terpesan Konvertibel.	6 November 2017
Memodifikasi penghunian VPC	15-11-2015	Anda dapat mengubah atribut penghunian instans dari sebuah VPC dari `dedicated` menjadi `default`. Untuk informasi selengkapnya, lihat Ubah penyewaan instance VPC.	16 Oktober 2017
Penagihan per detik	15-11-2015	Amazon EC2 mengenakan biaya untuk penggunaan berbasis Linux per detik, dengan biaya minimum satu menit.	2 Oktober 2017

Fitur	Versi API	Deskripsi	Tanggal rilis
Berhenti saat terjadi interupsi	15-11-2015	Anda dapat menentukan apakah Amazon EC2 harus menghentikan atau mengakhiri Instans Spot saat terjadi interupsi. Untuk informasi selengkapnya, lihat Perilaku interupsi Instance Spot.	18 September 2017
Menandai gateway NAT	15-11-2015	Anda dapat menandai gateway NAT. Untuk informasi selengkapnya, lihat Tandai sumber daya Anda.	7 September 2017
Deskripsi aturan grup keamanan	15-11-2015	Anda dapat menambahkan deskripsi ke aturan grup keamanan.	31 Agustus 2017
Elastic Graphics	15-11-2015	Lampirkan akselerator Elastic Graphics ke instans Anda untuk mempercepat performa grafis aplikasi Anda.	29 Agustus 2017
Memulihkan alamat IP Elastis	15-11-2015	Jika Anda merilis alamat IP Elastis untuk digunakan di VPC, Anda akan dapat memulihkannya.	11 Agustus 2017
Menandai instans Armada Spot	15-11-2015	Anda dapat mengonfigurasi Armada Spot untuk secara otomatis menandai instans yang diluncurkannya.	24 Juli 2017
Memberi tag pada sumber daya selama pembuatan	15-11-2015	Anda dapat menerapkan tanda pada instans dan volume selama pembuatan. Untuk informasi selengkapnya, lihat Tandai sumber daya Anda. Selain itu, Anda dapat menggunakan izin tingkat sumber daya berbasis tanda untuk mengontrol tanda yang diterapkan. Untuk informasi selengkapnya, lihat Berikan izin untuk menandai sumber daya Amazon EC2 selama pembuatan.	28 Maret 2017

Fitur	Versi API	Deskripsi	Tanggal rilis
Melakukan modifikasi pada volume EBS terlampir	15-11-2015	Dengan sebagian besar volume EBS terlampir ke sebagian besar instans EC2, Anda dapat mengubah ukuran volume, tipe, dan IOPS tanpa mencopot lampiran volume atau menghentikan instans.	13 Februari 2017
Melampirkan peran IAM	15-11-2015	Anda dapat melampirkan, mencopot lampiran, atau mengganti peran IAM untuk instans yang sudah ada. Untuk informasi selengkapnya, lihat IAM role untuk Amazon EC2.	9 Februari 2017
Instans Spot Khusus	15-11-2015	Anda dapat menjalankan Instans Spot di perangkat keras penghuni tunggal di cloud privat virtual (VPC). Untuk informasi selengkapnya, lihat Peluncuran pada perangkat keras penyewa tunggal.	19 Januari 2017
IPv6 dukungan	15-11-2015	Anda dapat mengaitkan IPv6 CIDR dengan VPC dan subnet Anda, dan IPv6 menetapkan alamat ke instance di VPC Anda. Untuk informasi selengkapnya, lihat Pengalamatan IP instans Amazon EC2.	1 Desember 2016
Penskalaan otomatis untuk Armada Spot		Anda sekarang dapat mengatur kebijakan penskalaan untuk Armada Spot. Untuk informasi selengkapnya, lihat Memahami penskalaan otomatis untuk Armada Spot.	1 September 2016
Adaptor Jaringan Elastis (ENA)	01-04-2016	Anda sekarang dapat menggunakan ENA untuk jaringan yang ditingkatkan. Untuk informasi selengkapnya, lihat Jaringan yang disempurnakan di EC2 instans Amazon.	28 Juni 2016

Fitur	Versi API	Deskripsi	Tanggal rilis
Dukungan yang ditingkatkan untuk melihat dan memodifikasi lebih lama IDs	01-04-2016	Anda sekarang dapat melihat dan memodifikasi pengaturan ID yang lebih panjang untuk pengguna IAM lain, peran IAM lain, atau pengguna root.	23 Juni 2016
Salin snapshot Amazon EBS terenkripsi antar akun AWS	01-04-2016	Anda sekarang dapat menyalin snapshot EBS terenkripsi antar akun. AWS	21 Juni 2016
Mengambil tangkapan layar dari konsol instans	01-10-2015	Anda sekarang dapat memperoleh informasi tambahan saat melakukan debugging instans yang tidak dapat dijangkau. Untuk informasi selengkapnya, lihat Mengambil tangkapan layar instans yang tidak dapat dijangkau.	24 Mei 2016
Dua tipe volume EBS baru	01-10-2015	Anda sekarang dapat membuat volume HDD Throughput yang Dioptimalkan (st1) dan HDD Cold (sc1).	19 April 2016
Ditambahkan baru NetworkPacketsIn dan NetworkPacketsOut metrik untuk Amazon EC2		Ditambahkan baru NetworkPacketsIn dan NetworkPacketsOut metrik untuk Amazon EC2. Untuk informasi selengkapnya, lihat Metrik instans.	23 Maret 2016
CloudWatch metrik untuk Spot Fleet		Anda sekarang bisa mendapatkan CloudWatch metrik untuk Armada Spot Anda. Untuk informasi selengkapnya, lihat Pantau Armada EC2 atau Armada Spot Anda menggunakan CloudWatch.	21 Maret 2016

Fitur	Versi API	Deskripsi	Tanggal rilis
Instans Terjadwal	01-10-2015	Instans Terpesan Terjadwal (Instans Terjadwal) memungkinkan Anda membeli reservasi kapasitas yang berulang setiap hari, minggu, atau setiap bulan, dengan waktu mulai dan durasi yang ditentukan.	13 Januari 2016
Sumber daya yang lebih panjang IDs	01-10-2015	Kami secara bertahap memperkenalkan ID yang lebih panjang untuk beberapa tipe sumber daya Amazon EC2 dan Amazon EBS. Selama periode keikutsertaan, Anda dapat mengaktifkan format ID yang lebih panjang untuk tipe sumber daya yang didukung.	13 Januari 2016
ClassicLink Dukungan DNS	01-10-2015	Anda dapat mengaktifkan dukungan ClassicLink DNS untuk VPC Anda sehingga nama host DNS yang dialamatkan antara instans EC2-Classic tertaut dan instance dalam VPC menyelesaikan ke alamat IP pribadi dan bukan alamat IP publik.	11 Januari 2016
Host Khusus	01-10-2015	Host khusus Amazon EC2 adalah server fisik dengan kapasitas instans yang dikhususkan untuk penggunaan Anda. Untuk informasi selengkapnya, lihat Host Khusus Amazon EC.	23 November 2015
Durasi Instans Spot	01-10-2015	Anda sekarang dapat menentukan durasi untuk Instans Spot. Blok Spot tidak didukung (Januari 2023).	6 Oktober 2015
Memodifikasi permintaan Armada Spot	01-10-2015	Anda sekarang dapat memodifikasi kapasitas target permintaan Armada Spot. Untuk informasi selengkapnya, lihat Memodifikasi permintaan Armada Spot.	29 September 2015

Fitur	Versi API	Deskripsi	Tanggal rilis
Strategi alokasi yang terdiversifikasi Armada Spot	15-04-2015	Anda sekarang dapat mengalokasikan Instans Spot di banyak kolam Spot dengan satu permintaan Armada Spot. Untuk informasi selengkapnya, lihat Gunakan strategi alokasi untuk menentukan bagaimana Armada EC2 atau Armada Spot memenuhi kapasitas Spot dan Sesuai Permintaan.	15 September 2015
Pembobotan instans Armada Spot	15-04-2015	Anda sekarang dapat menentukan unit kapasitas yang dikontribusikan oleh setiap tipe instans untuk performa aplikasi, dan menyesuaikan jumlah yang akan Anda bayarkan untuk Instans Spot di setiap kolam Spot yang sesuai. Untuk informasi selengkapnya, lihat Gunakan pembobotan instans untuk mengelola biaya dan kinerja Armada EC2 atau Armada Spot Anda.	31 Agustus 2015
Tindakan alarm boot ulang baru dan peran IAM baru untuk digunakan dengan tindakan alarm		Menambahkan tindakan alarm boot ulang dan peran IAM baru untuk digunakan dengan tindakan alarm. Untuk informasi selengkapnya, lihat Buat alarm yang menghentikan, mengakhiri, melakukan boot ulang, atau memulihkan instans.	23 Juli 2015
Armada Spot	15-04-2015	Anda dapat mengelola kumpulan, atau armada, Instans Spot alih-alih mengelola permintaan Instans Spot yang terpisah. Untuk informasi selengkapnya, lihat Armada EC2 dan Armada Spot.	18 Mei 2015
Memigrasikan alamat IP Elastis ke EC2-Classic	15-04-2015	Anda dapat memigrasikan alamat IP Elastis yang telah dialokasikan untuk digunakan di EC2-Classic agar digunakan di VPC.	15 Mei 2015

Fitur	Versi API	Deskripsi	Tanggal rilis
Mengimpor VMs dengan beberapa disk sebagai AMIs	01-03-2015	Proses Impor VM sekarang mendukung VMs pengimporan dengan beberapa disk sebagai. AMIs Untuk informasi selengkapnya, lihat Mengimpor VM sebagai Gambar Menggunakan Impor/Ekspor VM di Panduan Pengguna VM. Import/Export	23 April 2015
Systems Manager		Systems Manager memungkinkan Anda untuk mengonfigurasi dan mengelola instans EC2.	17 Februari 2015
Systems Manager untuk Microsoft SCVMM 1.5		Anda sekarang dapat menggunakan Systems Manager untuk Microsoft SCVMM guna meluncurkan instans dan mengimpor VM dari SCVMM ke Amazon EC2.	21 Januari 2015
Pemulihan otomatis untuk instans EC2		Anda dapat membuat CloudWatch alarm Amazon yang memantau instans Amazon EC2 dan memulihkan instans secara otomatis jika menjadi rusak karena kegagalan perangkat keras yang mendasarinya atau masalah yang memerlukan AWS keterlibatan untuk memperbaiki. Instans yang dipulihkan identik dengan instans asli, termasuk ID instans, alamat IP, dan semua metadata instans. Untuk informasi selengkapnya, lihat Pemulihan instans otomatis.	12 Januari 2015

Fitur	Versi API	Deskripsi	Tanggal rilis
ClassicLink	01-10-2014	ClassicLink memungkinkan Anda untuk menautkan instans EC2-Classic Anda ke VPC di akun Anda. Anda dapat mengaitkan grup keamanan VPC dengan instans EC2-Classic, yang memungkinkan komunikasi antara instans EC2-Classic dan instans di VPC Anda menggunakan alamat IP privat.	7 Januari 2015
Pemberitahuan pengakhiran Instans Spot.		Cara terbaik untuk melindungi dari interupsi Instans Spot adalah dengan merancang aplikasi Anda agar toleran terhadap kesalahan. Selain itu, Anda dapat memanfaatkan pemberitahuan pengakhiran Instans Spot, yang memberikan peringatan dua menit sebelum Amazon EC2 mengakhiri Instans Spot Anda. Untuk informasi selengkapnya, lihat Pemberitahuan interupsi Instans Spot.	5 Januari 2015
Systems Manager untuk Microsoft SCVMM		Systems Manager untuk Microsoft SCVMM menyediakan easy-to-use antarmuka yang sederhana untuk mengelola AWS sumber daya, seperti instans EC2, dari Microsoft SCVMM.	29 Oktober 2014
Dukungan paginasi `DescribeVolumes`	01-09-2014	Panggilan API `DescribeVolumes` sekarang mendukung paginasi hasil dengan parameter `MaxResults` dan `NextToken`. Untuk informasi selengkapnya, lihat DescribeVolumes dalam Referensi API Amazon EC2.	23 Oktober 2014

Fitur	Versi API	Deskripsi	Tanggal rilis
Ditambahkan dukungan untuk Amazon CloudWatch Logs		Anda dapat menggunakan Amazon CloudWatch Logs untuk memantau, menyimpan, dan mengakses sistem, aplikasi, dan file log kustom dari instans atau sumber lain. Anda kemudian dapat mengambil data log terkait dari CloudWatch Log menggunakan CloudWatch konsol Amazon, perintah CloudWatch Log di AWS CLI, atau Logs CloudWatch SDK.	10 Juli 2014
Halaman Batas Layanan EC2 baru		Gunakan halaman Batas Layanan EC2 di konsol Amazon EC2 guna melihat batas saat ini untuk sumber daya yang disediakan oleh Amazon EC2 dan Amazon VPC, berdasarkan tiap wilayah.	19 Juni 2014
Volume SSD Tujuan Umum Amazon EBS	01-05-2014	Volume SSD Tujuan Umum menawarkan penyimpanan hemat biaya yang ideal untuk berbagai beban kerja. Volume ini memberikan latensi satu digit milidetik, kemampuan melonjak hingga 3.000 IOPS untuk waktu yang lama, dan performa dasar 3 IOPS/GiB. Ukuran volume SSD Tujuan Umum dapat bervariasi mulai 1 GiB hingga 1 TiB.	16 Juni 2014
AWS Paket Manajemen		AWS Management Pack sekarang mendukung untuk System Center Operations Manager 2012 R2.	22 Mei 2014

Fitur	Versi API	Deskripsi	Tanggal rilis
Enkripsi Amazon EBS	01-05-2014	Enkripsi Amazon EBS menawarkan enkripsi volume dan snapshot data EBS yang mulus, sehingga tidak perlu membangun dan memelihara infrastruktur manajemen kunci yang aman. Enkripsi EBS memungkinkan keamanan data diam dengan mengenkripsi data Anda menggunakan Kunci yang dikelola AWS. Enkripsi dilakukan di server yang melakukan hosting instans EC2, yang menyediakan enkripsi data saat berpindah antara instans EC2 dan penyimpanan EBS.	21 Mei 2014
Laporan Penggunaan Amazon EC2		Laporan Penggunaan Amazon EC2 adalah set laporan yang menunjukkan biaya dan data penggunaan EC2 Anda.	28 Januari 2014
Mengimpor mesin virtual Linux	15-10-2013	Proses VM Import sekarang mendukung pengimporan instans Linux. Untuk informasi selengkapnya, lihat Panduan Import/Export Pengguna VM.	16 Desember 2013
Izin tingkat sumber daya untuk RunInstances	15-10-2013	Anda sekarang dapat membuat kebijakan AWS Identity and Access Management untuk mengontrol izin tingkat sumber daya untuk tindakan Amazon EC2 API. RunInstances Untuk informasi selengkapnya dan kebijakan contoh, lihat Manajemen identitas dan akses untuk Amazon EC2.	20 November 2013
Meluncurkan sebuah instance dari AWS Marketplace		Anda sekarang dapat meluncurkan instance dari AWS Marketplace menggunakan wizard peluncuran Amazon EC2. Untuk informasi selengkapnya, lihat Luncurkan instans Amazon EC2 dari AMI AWS Marketplace.	11 November 2013

Fitur	Versi API	Deskripsi	Tanggal rilis
Wizard peluncuran baru		Terdapat wizard peluncuran EC2 yang baru dan didesain ulang. Untuk informasi selengkapnya, lihat Luncurkan instans EC2 menggunakan wizard instans peluncuran di konsol.	10 Oktober 2013
Memodifikasi tipe instans dari Instans Cadangan	01-10-2013	Anda sekarang dapat memodifikasi tipe instans dari Instans Terpesan Linux dalam keluarga yang sama (misalnya, M1, M2, M3, C1). Untuk informasi selengkapnya, lihat Memodifikasi Instans Terpesan.	9 Oktober 2013
Memodifikasi Instans Terpesan Amazon EC2	15-08-2013	Anda sekarang dapat memodifikasi Instans Terpesan di satu Wilayah. Untuk informasi selengkapnya, lihat Memodifikasi Instans Terpesan.	11 September 2013
Menetapkan alamat IP publik	15-07-2013	Anda sekarang dapat menetapkan alamat IP publik saat meluncurkan instans di VPC. Untuk informasi selengkapnya, lihat Tetapkan IPv4 alamat publik saat peluncuran.	20 Agustus 2013
Memberikan izin tingkat sumber daya	15-06-2013	Amazon EC2 mendukung Nama Sumber Daya Amazon (ARNs) dan kunci kondisi baru. Untuk informasi selengkapnya, lihat Kebijakan berbasis identitas untuk Amazon EC2.	8 Juli 2013
Salinan Snapshot Inkremental	01-02-2013	Anda sekarang dapat menjalankan salinan snapshot inkremental.	11 Juni 2013
AWS Paket Manajemen		Paket AWS Manajemen menghubungkan instans Amazon EC2 dan sistem operasi Windows atau Linux yang berjalan di dalamnya. Paket AWS Manajemen adalah ekstensi untuk Microsoft System Center Operations Manager.	8 Mei 2013

Fitur	Versi API	Deskripsi	Tanggal rilis
Halaman Tanda baru		Terdapat halaman Tanda baru di konsol Amazon EC2. Untuk informasi selengkapnya, lihat Tandai sumber daya Amazon EC2 Anda.	4 April 2013
Salin AMI dari satu Wilayah ke Wilayah lainnya	01-02-2013	Anda dapat menyalin AMI dari satu Wilayah ke Wilayah lainnya, memungkinkan Anda meluncurkan instans yang konsisten di lebih dari satu AWS Wilayah dengan cepat dan mudah. Untuk informasi selengkapnya, lihat Salin Amazon EC2 AMI.	11 Maret 2013
Meluncurkan instans ke VPC default	01-02-2013	AWS Akun Anda mampu meluncurkan instans ke EC2-Classic atau VPC, atau hanya ke VPC, secara dasar. region-by-region Jika Anda hanya dapat meluncurkan instans ke dalam VPC, kami membuatkan VPC default untuk Anda. Saat meluncurkan instans, kami akan meluncurkannya ke dalam VPC default, kecuali jika Anda membuat VPC non-default dan menentukannya saat meluncurkan instans tersebut.	11 Maret 2013
Salinan snapshot EBS	01-12-2012	Anda dapat menggunakan salinan snapshot untuk membuat cadangan data, untuk membuat volume Amazon EBS baru, atau untuk membuat Amazon Machine Images (). AMIs	17 Desember 2012
Memperbarui metrik dan pemeriksaan status EBS untuk volume IOPS SSD yang Tersedia	01-10-2012	Memperbarui metrik EBS untuk menyertakan dua metrik baru untuk volume IOPS SSD yang Tersedia. Selain itu juga menambahkan pemeriksaan status baru untuk volume SSD IOPS yang Tersedia.	20 November 2012

Fitur	Versi API	Deskripsi	Tanggal rilis
Status permintaan Instans Spot	01-10-2012	Status permintaan Instans Spot memudahkan untuk menentukan status permintaan Spot Anda.	14 Oktober 2012
Marketplace Instans Terpesan Amazon EC2	15-08-2012	Marketplace Instans Terpesan mencocokkan penjual yang memiliki Instans Terpesan Amazon EC2 yang tidak lagi mereka perlukan dengan pembeli yang ingin membeli kapasitas tambahan. Instans Terpesan yang dibeli dan dijual melalui Marketplace Instans Terpesan berfungsi seperti Instans Terpesan lainnya, tetapi instans ini dapat memiliki sisa jangka waktu kurang dari standar penuh dan dapat dijual dengan harga berbeda.	11 September 2012
SSD IOPS yang Tersedia untuk Amazon EBS	20-07-2012	Volume SSD dengan IOPS yang tersedia memberikan performa tinggi yang dapat diprediksi untuk beban kerja intensif I/O, seperti aplikasi basis data, yang mengandalkan waktu respons yang konsisten dan cepat.	31 Juli 2012
Peran IAM di instans Amazon EC2	01-06-2012	Peran IAM untuk Amazon EC2 menyediakan: • AWS kunci akses untuk aplikasi yang berjalan di instans Amazon EC2. • Rotasi otomatis tombol AWS akses pada instans Amazon EC2. • Izin terperinci untuk aplikasi yang berjalan di instans Amazon EC2 yang membuat permintaan ke layanan Anda. AWS	11 Juni 2012

Fitur	Versi API	Deskripsi	Tanggal rilis
Fitur Instans Spot yang memudahkan untuk memulai dan menangani potensi interupsi.		Anda sekarang dapat mengelola Instans Spot sebagai berikut: • Tentukan jumlah yang akan Anda bayarkan untuk Instans Spot menggunakan konfigurasi peluncuran Auto Scaling, dan mengatur jadwal untuk menentukan jumlah yang akan Anda bayarkan untuk Instans Spot. Fatau informasi selengkapnya, lihat Meminta Instans Spot di Panduan Pengguna Amazon EC2 Auto Scaling. • Dapatkan notifikasi saat instans diluncurkan atau diakhiri. • Gunakan CloudFormation template untuk meluncurkan Instans Spot dalam tumpukan dengan AWS sumber daya.	7 Juni 2012
Mengekspor instans EC2 dan stempel waktu untuk pemeriksaan status pada Amazon EC2	01-05-2012	Menambahkan dukungan untuk mengekspor instans Windows Server yang awalnya Anda impor ke EC2. Menambahkan dukungan untuk stempel waktu pada status instans dan status sistem untuk menunjukkan tanggal dan waktu ketika pemeriksaan status mengalami kegagalan.	25 Mei 2012
Mengekspor instans EC2 dan stempel waktu dalam pemeriksaan status instans serta sistem untuk Amazon VPC	01-05-2012	Menambahkan dukungan untuk ekspor instans EC2 ke Citrix Xen, Microsoft Hyper-V, dan vSphere. VMware Menambahkan dukungan untuk stempel waktu dalam instans dan pemeriksaan status sistem.	25 Mei 2012

Fitur	Versi API	Deskripsi	Tanggal rilis
AWS Marketplace AMIs	01-04-2012	Menambahkan dukungan untuk AWS Marketplace AMIs.	19 April 2012
Tingkat harga Instans Terpesan	15-12-2011	Menambahkan bagian baru yang berisi cara memanfaatkan harga diskon yang ada di dalam tingkatan harga Instans Terpesan.	5 Maret 2012
Antarmuka Jaringan Elastis (ENI) untuk instans EC2 di Amazon Virtual Private Cloud	01-12-2011	Menambahkan bagian baru tentang antarmuka jaringan elastis (ENI) untuk instans EC2 di VPC. Untuk informasi selengkapnya, lihat Antarmuka jaringan elastis.	21 Desember 2011
Tipe penawaran baru untuk Instans Terpesan Amazon EC2	01-11-2011	Anda dapat memilih dari berbagai penawaran Instans Terpesan yang berisi tentang proyeksi penggunaan instans.	1 Desember 2011
Status instans Amazon EC2	01-11-2011	Anda dapat melihat detail tambahan tentang status instans Anda, termasuk acara terjadwal yang direncanakan oleh AWS yang mungkin berdampak pada instans Anda. Aktivitas operasional ini mencakup boot ulang instans yang diperlukan untuk menerapkan pembaruan perangkat lunak atau patch keamanan, atau pemensiunan instans yang diperlukan jika terjadi masalah perangkat keras. Untuk informasi selengkapnya, lihat Pantau status instans Amazon EC2 Anda.	16 November 2011

Fitur	Versi API	Deskripsi	Tanggal rilis
Instans Spot di Amazon VPC	15-07-2011	Menambahkan informasi tentang dukungan untuk Instans Spot di Amazon VPC. Dengan pembaruan ini, pengguna dapat meluncurkan Instans Spot sebagai cloud privat virtual (VPC). Dengan meluncurkan Instans Spot di VPC, pengguna Instans Spot dapat menikmati manfaat Amazon VPC.	11 Oktober 2011
Proses VM Import untuk pengguna alat CLI disederhanakan	15-07-2011	Proses VM Import disederhanakan dengan fungsionalitas yang ditingkatkan dari `ImportInstance` dan `ImportVolume`, yang sekarang akan melakukan penggunggahan gambar ke Amazon EC2 setelah membuat tugas impor. Selain itu, dengan diperkenalkannya `ResumeImport`, pengguna dapat memulai kembali unggahan yang belum selesai pada titik saat tugas tersebut terhenti.	15 September 2011
Dukungan untuk mengimpor dalam format file VHD		VM Import sekarang dapat mengimpor file citra mesin virtual dalam format VHD. Format file VHD kompatibel dengan platform virtualisasi Citrix Xen dan Microsoft Hyper-V. Dengan rilis ini, VM Import sekarang mendukung format gambar RAW, VHD dan VMDK VMware (ESX-kompatibel). Untuk informasi selengkapnya, lihat Panduan Import/Export Pengguna VM.	24 Agustus 2011
Perbarui ke Amazon EC2 VM Import Connector untuk vCenter VMware		Menambahkan informasi tentang versi 1.1 dari Amazon EC2 VM Import Connector untuk alat virtual VMware vCenter (Konektor). Pembaruan ini mencakup dukungan proksi untuk akses Internet, penanganan kesalahan yang lebih baik, akurasi bilah kemajuan tugas yang lebih baik, dan beberapa perbaikan bug.	27 Juni 2011

Fitur	Versi API	Deskripsi	Tanggal rilis
Perubahan harga Zona Ketersediaan Instans Spot	15-05-2011	Menambahkan informasi tentang fitur harga Zona Ketersediaan Instans Spot. Dalam rilis ini, kami telah menambahkan opsi harga Zona Ketersediaan baru sebagai bagian dari informasi yang ditampilkan saat Anda membuat kueri untuk permintaan Instans Spot dan riwayat harga Spot. Tambahan ini memudahkan penentuan harga yang diperlukan untuk meluncurkan Instans Spot ke dalam Zona Ketersediaan tertentu.	26 Mei 2011
AWS Identity and Access Management		Menambahkan informasi tentang AWS Identity and Access Management (IAM), yang memungkinkan pengguna menentukan tindakan Amazon EC2 mana yang dapat digunakan pengguna dengan sumber daya Amazon EC2 secara umum. Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk Amazon EC2.	26 April 2011
Instans Khusus		Diluncurkan dalam Amazon Virtual Private Cloud (Amazon VPC) Anda, Instans Khusus adalah instans yang secara fisik diisolasi di tingkat perangkat keras host. Instans Khusus memungkinkan Anda memanfaatkan Amazon VPC dan AWS cloud, dengan manfaat termasuk penyediaan elastis sesuai permintaan dan hanya membayar untuk apa yang Anda gunakan, sekaligus mengisolasi instans komputasi Amazon EC2 Anda di tingkat perangkat keras. Untuk informasi selengkapnya, lihat Instans EC2 Khusus Amazon.	27 Maret 2011

Fitur	Versi API	Deskripsi	Tanggal rilis
Instans Cadangan diperbarui ke Konsol AWS Manajemen		Pembaruan pada Konsol AWS Manajemen memudahkan pengguna untuk melihat Instans Cadangan mereka dan membeli Instans Cadangan tambahan, termasuk Instans Cadangan Khusus.	27 Maret 2011
Informasi metadata	01-01-2011	Menambahkan informasi tentang metadata untuk merefleksikan perubahan dalam rilis 01-01-2011. Untuk informasi lebih lanjut, lihat Gunakan metadata instans untuk mengelola instans EC2 dan Kategori metadata instans.	11 Maret 2011
Amazon EC2 VM Import Connector untuk vCenter VMware		Menambahkan informasi tentang Amazon EC2 VM Import Connector untuk peralatan virtual VMware vCenter (Connector). Connector adalah plug-in untuk VMware vCenter yang berintegrasi dengan Klien VMware vSphere dan menyediakan antarmuka pengguna grafis yang dapat Anda gunakan untuk mengimpor mesin virtual VMware ke Amazon EC2.	3 Maret 2011
Memaksa pelepasan lampiran volume		Anda sekarang dapat menggunakan Konsol Manajemen AWS untuk memaksa pelepasan volume Amazon EBS dari sebuah instans.	23 Februari 2011
Perlindungan pengakhiran instans		Sekarang Anda dapat menggunakan AWS Management Console untuk mencegah instance dihentikan. Untuk informasi selengkapnya, lihat Ubah perlindungan penghentian instance.	23 Februari 2011

Fitur	Versi API	Deskripsi	Tanggal rilis
VM Import	15-11-2010	Menambahkan informasi tentang VM Import, yang memungkinkan Anda mengimpor mesin virtual atau volume ke Amazon EC2. Untuk informasi selengkapnya, lihat Panduan Import/Export Pengguna VM.	15 Desember 2010
Pemantauan dasar untuk instans	31-08-2010	Menambahkan informasi tentang pemantauan dasar untuk instans EC2.	12 Desember 2010
Filter dan Tanda	31-08-2010	Menambahkan informasi tentang membuat daftar, memfilter, dan menandai sumber daya. Untuk informasi lebih lanjut, lihat Temukan sumber daya Amazon EC2 Anda dan Tandai sumber daya Amazon EC2 Anda.	19 September 2010
Peluncuran Instans Idempotensi	31-08-2010	Menambahkan informasi tentang memastikan idempotensi saat menjalankan instans.	19 September 2010
AWS Identity and Access Management untuk Amazon EC2		Amazon EC2 sekarang terintegrasi dengan AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk Amazon EC2.	2 September 2010
Penetapan Alamat IP Amazon VPC	15-06-2010	Pengguna Amazon VPC sekarang dapat menentukan alamat IP untuk menetapkan instans yang diluncurkan di VPC.	12 Juli 2010
CloudWatch Pemantauan Amazon untuk Volume Amazon EBS		CloudWatch Pemantauan Amazon sekarang tersedia secara otomatis untuk volume Amazon EBS.	14 Juni 2010

Fitur	Versi API	Deskripsi	Tanggal rilis
Instans Terpesan dengan Windows		Amazon EC2 sekarang mendukung Instans Terpesan dengan Windows.	22 Februari 2010

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.