



Panduan Administrasi

AWS Directory Service



Versi 1.0

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

AWS Directory Service: Panduan Administrasi

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 hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS Directory Service?	1
AWS Directory Service pilihan	1
Mana yang harus dipilih	5
Bekerja dengan Amazon EC2	6
AWS Microsoft AD yang dikelola	7
Mana yang harus dipilih	8
Topik	8
AWS Microsoft AD yang Dikelola (Edisi Hybrid)	9
Prasyarat direktori hybrid	9
Membuat direktori hybrid	17
Melihat dan mengedit direktori hybrid	18
Menghapus direktori hybrid	20
Penilaian direktori	21
Pemecahan masalah	25
Memulai	59
AWS Prasyarat Microsoft AD yang dikelola	60
AWS IAM Identity Center prasyarat	61
Prasyarat autentikasi multi-faktor	61
Membuat Microsoft AD yang AWS Dikelola	62
Apa yang dibuat dengan Microsoft AD yang AWS Dikelola	65
Izin akun dan grup administrator	76
Konsep kunci dan praktik terbaik	79
Konsep utama	80
Praktik terbaik	84
Kasus penggunaan	94
Kasus Penggunaan 1: Masuk ke AWS aplikasi dan layanan dengan kredensial Active Directory	96
Kasus Penggunaan 2: Mengelola instans Amazon EC2	100
Kasus Penggunaan 3: Menyediakan layanan direktori ke beban kerja sadar Direktori Aktif Anda	101
Kasus Penggunaan 4: AWS IAM Identity Center ke Office 365 dan aplikasi cloud lainnya	101
Kasus Penggunaan 5: Perluas Direktori Aktif lokal Anda ke AWS Cloud	102
Kasus Penggunaan 6: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 dengan mulus ke domain di seluruh akun AWS	102

Memelihara direktori Anda	103
Melihat informasi direktori	103
Memulihkan direktori Anda dengan snapshot	106
Menyebarkan pengontrol domain tambahan	111
Memutakhirkan Microsoft AD yang AWS Dikelola	115
Memperbarui jenis jaringan direktori	117
Menambahkan sufiks UPN alternatif	118
Mengganti nama situs direktori Anda	119
Menghapus iklan Microsoft yang AWS Dikelola	119
Mengamankan direktori Anda	121
Memahami kebijakan kata sandi	122
Mengaktifkan autentikasi multi-faktor	128
Aktifkan LDAP Aman atau LDAPS	132
Mengelola kepatuhan untuk direktori Anda	145
Meningkatkan keamanan jaringan	147
Mengedit pengaturan keamanan direktori	161
Aktifkan Kriptografi Kunci Publik untuk Otentikasi Awal (PKINIT)	174
Siapkan AWS Private CA Konektor untuk AD	177
Memantau direktori Anda	183
Memahami status direktori Anda	184
Mengaktifkan pemberitahuan status direktori dengan Amazon SNS	185
Memahami log direktori Anda	188
Mengaktifkan penerusan CloudWatch log Amazon	191
Menggunakan CloudWatch untuk memantau direktori Anda	194
Menonaktifkan penerusan log Amazon CloudWatch	198
Memantau DNS Server dengan Microsoft Event Viewer	199
Akses ke AWS aplikasi dan layanan	199
Kompatibilitas aplikasi	200
Mengaktifkan akses ke AWS aplikasi dan layanan	203
Mengaktifkan akses ke Konsol Manajemen AWS	205
Membuat URL akses	209
Mengaktifkan single sign-on	210
Memberikan akses ke sumber daya AWS	218
Membuat peran baru	218
Mengedit hubungan kepercayaan untuk peran yang ada	220
Menetapkan pengguna atau grup ke peran yang ada	221

Melihat pengguna dan grup yang ditetapkan ke peran	222
Menghapus pengguna atau grup dari peran	223
Menggunakan kebijakan AWS terkelola	224
Konfigurasi replikasi Multi-Wilayah	225
Cara kerjanya	226
Manfaat	228
Fitur Global vs Regional	229
Region utama vs tambahan	230
Menambahkan Wilayah yang direplikasi	231
Menghapus Wilayah yang direplikasi	234
Bagikan direktori Anda	234
Konsep utama	235
Pertimbangan-pertimbangan	236
Tutorial: Bagikan direktori Microsoft AD AWS Terkelola Anda	237
Membatalkan berbagi direktori Anda	248
Memigrasi pengguna Active Directory ke Microsoft AD yang AWS Dikelola	249
Connect infrastruktur Active Directory yang ada	249
Menciptakan hubungan kepercayaan	250
Menambahkan rute IP	257
Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri	257
Tutorial: Buat hubungan kepercayaan antara domain Microsoft AD yang AWS Dikelola	269
Perluas skema direktori Anda	275
Kapan harus memperpanjang skema AD Microsoft AWS Terkelola	275
Tutorial: Memperluas skema AD Microsoft AWS Terkelola Anda	276
Cara untuk bergabung dengan instance ke direktori Anda	283
Meluncurkan instance administrasi direktori	284
Bergabung dengan instance Windows	287
Bergabung dengan Instance Linux	295
Bergabung dengan instans Mac	349
Mendelegasikan hak istimewa bergabung direktori	351
Membuat atau mengubah set opsi DHCP	354
Manajemen pengguna dan grup	356
Konsol Manajemen AWS	356
AWS CLI	357
AWS Tools for PowerShell	358

Instans lokal atau Amazon EC2	359
Kelola pengguna dan grup dengan konsol, CLI, atau PowerShell	359
Mengelola pengguna dan grup dengan EC2 instans Amazon	402
Directory Service Data	413
Replikasi dan konsistensi	414
AWS Atribut Directory Service Data	415
Jenis grup dan ruang lingkup grup	420
Menghubungkan ke Microsoft Entra Connect Sync	422
Prasyarat	422
Buat pengguna domain Active Directory	423
Unduh Entra Connect Sync	423
Jalankan PowerShell Script	423
Instal Entra Connect Sync	425
AWS Tutorial lab uji Microsoft AD yang dikelola	428
Tutorial: Siapkan lab pengujian Microsoft AD AWS Terkelola basis Anda	429
Tutorial: Buat kepercayaan dari Microsoft AD yang AWS Dikelola ke instalasi AD yang dikelola sendiri di EC2	447
Kuota	458
Pemecahan masalah	460
Masalah dengan Microsoft AD yang AWS Dikelola	460
Masalah dengan Netlogon dan komunikasi saluran aman	460
Anda menerima kesalahan 'Status Respons: 400 Permintaan Buruk' saat mencoba mengatur ulang kata sandi pengguna	461
Pemulihan kata sandi	461
Sumber daya tambahan	461
Kesalahan gabungan domain instans Amazon EC2 Linux	462
Ruang penyimpanan yang tersedia rendah	465
Kesalahan ekstensi skema	468
Alasan status pembuatan kepercayaan	471
Pemanfaatan CPU yang tinggi	475
AD Connector	480
Memulai	481
Prasyarat AD Connector	481
Membuat AD Connector	497
Apa yang dibuat dengan AD Connector Anda	499
Praktik terbaik	500

Menyiapkan: Prasyarat	500
Memprogram aplikasi Anda	502
Menggunakan direktori Anda	503
Memelihara direktori Anda	503
Melihat informasi direktori	504
Memperbarui jenis jaringan direktori	504
Memperbarui alamat DNS untuk AD Connector	505
Menghapus AD Connector	506
Mengamankan direktori Anda	507
Mengaktifkan autentikasi multi-faktor	508
Mengaktifkan LDAPS sisi klien	510
Mengaktifkan otentikasi mTLS	516
Memperbarui kredensi akun layanan AD Connector	526
Siapkan AWS Private CA Konektor untuk AD	527
Memantau direktori Anda	529
Memahami status direktori Anda	529
Mengaktifkan pemberitahuan status direktori dengan Amazon SNS	530
Akses ke AWS aplikasi dan layanan	533
Kompatibilitas aplikasi	533
Mengaktifkan akses ke AWS aplikasi dan layanan dari AD Connector	534
Cara untuk bergabung dengan EC2 instans Amazon ke Direktori Aktif Anda	536
Kuota	537
Pemecahan masalah	537
Masalah pembuatan	538
Masalah konektivitas	539
Masalah otentikasi	541
Masalah pemeliharaan	550
Saya tidak dapat menghapus AD Connector	551
Alat umum untuk menyelidiki emiten AD Connector	551
Simple AD	552
Memulai	553
Prasyarat Simple AD	554
Buat Simple AD Anda	556
Apa yang dibuat dengan Simple AD Anda	559
Praktik terbaik	560
Menyiapkan: Prasyarat	560

Pengaturan: Membuat direktori Anda	562
Memprogram aplikasi Anda	563
Memelihara direktori Anda	564
Melihat informasi direktori	564
Memperbarui jenis jaringan direktori	565
Mengkonfigurasi server DNS	566
Memulihkan direktori Anda dengan snapshot	568
Menghapus Simple AD	570
Mengamankan direktori Anda	572
Setel ulang kata sandi akun krbtgt	572
Memantau direktori Anda	577
Memahami status direktori Anda	577
Mengaktifkan pemberitahuan status direktori dengan Amazon Simple Notification Service ..	579
Akses ke AWS aplikasi dan layanan	581
Kompatibilitas aplikasi	582
Mengaktifkan akses ke AWS aplikasi dan layanan	583
Mengaktifkan akses ke Konsol Manajemen AWS	584
Membuat URL akses	586
Mengaktifkan single sign-on	587
Cara untuk bergabung dengan instance ke direktori Anda	595
Bergabung dengan instance Windows	596
Bergabunglah dengan instance Linux	604
Mendelegasikan hak istimewa bergabung direktori	630
Membuat set opsi DHCP	632
Manajemen pengguna dan grup	634
Menginstal Alat Administrasi AD	635
Membuat pengguna	637
Menghapus pengguna	639
Menyetel ulang kata sandi pengguna	640
Membuat grup	642
Menambahkan pengguna ke grup	643
Kuota	645
Pemecahan masalah	645
Pemulihan kata sandi	646
Saya menerima kesalahan 'KDC tidak dapat memenuhi opsi yang diminta' saat menambahkan pengguna ke Simple AD	646

Saya tidak dapat memperbarui nama DNS atau alamat IP instans bergabung ke domain saya (pembaruan dinamis DNS)	646
Saya tidak bisa masuk ke SQL Server menggunakan akun SQL Server	646
Simple AD saya macet dalam status 'Diminta'	647
Saya menerima kesalahan 'AZ terkendali' saat membuat Simple AD	647
Beberapa pengguna saya tidak dapat mengautentikasi dengan Simple AD saya	647
Sumber daya tambahan	461
Memecahkan masalah pesan status direktori	648
Keamanan	652
Manajemen identitas dan akses	653
Autentikasi	654
Kontrol akses	654
Gambaran umum manajemen akses	654
AWS kebijakan terkelola	659
Menggunakan kebijakan berbasis identitas (kebijakan IAM)	664
Directory Service Referensi izin API	673
Kunci kondisi Directory Service Data	675
Otorisasi untuk AWS aplikasi dan layanan menggunakan Directory Service	681
Mengotorisasi AWS aplikasi pada Active Directory	682
AWS otorisasi aplikasi dengan Directory Service Data	683
Menggunakan Peran Terkait Layanan	684
Izin peran terkait layanan untuk Directory Service	685
Membuat peran terkait layanan untuk Directory Service	686
Mengedit peran terkait layanan untuk Directory Service	686
Menghapus peran terkait layanan untuk Directory Service	687
Wilayah yang Didukung untuk Directory Service peran terkait layanan	687
Pencatatan log dan pemantauan	689
AWS Directory Service log	690
AWS Log data Directory Service	693
Validasi kepatuhan	702
Ketahanan	703
Keamanan infrastruktur	703
Pencegahan "confused deputy" lintas layanan	703
AWS PrivateLink	707
Pertimbangan-pertimbangan	708
Ketersediaan	708

Buat antarmuka titik akhir Amazon VPC	708
Membuat kebijakan titik akhir	708
Perjanjian tingkat layanan	711
Ketersediaan wilayah	712
Didukung Wilayah AWS untuk Directory Service Data	719
Kompabilitas peramban	722
Apa itu TLS?	722
Versi TLS mana yang didukung oleh IAM Identity Center	722
Bagaimana cara mengaktifkan versi TLS yang didukung di peramban saya	723
Riwayat dokumen	724
.....	dccxxix

Apa itu AWS Directory Service?

AWS Directory Service menyediakan beberapa cara untuk menggunakan Microsoft Active Directory (AD) dengan AWS layanan lain. Direktori menyimpan informasi tentang pengguna, grup, dan perangkat, dan administrator menggunakannya untuk mengelola akses ke informasi dan sumber daya. AWS Directory Service menyediakan beberapa pilihan direktori untuk pelanggan yang ingin menggunakan aplikasi sadar Microsoft AD atau Lightweight Directory Access Protocol (LDAP) yang ada di cloud. Ini juga menawarkan pilihan yang sama untuk developer yang membutuhkan direktori untuk mengelola pengguna, grup, perangkat, dan akses.

AWS Directory Service pilihan

AWS Directory Service mencakup beberapa jenis direktori untuk dipilih. Untuk informasi selengkapnya, pilih salah satu dari tab berikut:

AWS Directory Service for Microsoft Active Directory

Juga dikenal sebagai AWS Managed Microsoft AD, AWS Directory Service untuk Microsoft Active Directory didukung oleh Microsoft Windows Server Active Directory (AD) aktual, dikelola oleh AWS di AWS Cloud. Ini memungkinkan Anda untuk memigrasikan berbagai aplikasi Active Directory—aware ke Cloud. AWS AWS Microsoft AD yang dikelola bekerja dengan Microsoft SharePoint, Microsoft SQL Server Always On Availability Groups, dan banyak aplikasi.NET. Ini juga mendukung aplikasi dan layanan AWS terkelola termasuk [Amazon WorkSpaces](#), [Amazon Quick WorkDocs](#), [Amazon Chime](#), [Amazon Connect](#), dan [Amazon Relational Database Service untuk \(Amazon RDS for\)](#) Microsoft SQL Server Amazon RDS for SQL Server, dan Amazon RDS Oracle for PostgreSQL).

[AWS Microsoft AD yang dikelola disetujui untuk aplikasi di AWS Cloud yang tunduk pada kepatuhan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan AS \(HIPAA\) atau Standar Keamanan Data Industri Kartu Pembayaran \(PCI DSS\) saat Anda mengaktifkan kepatuhan untuk direktori Anda.](#)

Semua aplikasi yang kompatibel bekerja dengan kredensial pengguna yang Anda simpan di Microsoft AD yang Dikelola AWS , atau Anda dapat [Hubungkan ke infrastruktur AD yang ada](#) dengan kepercayaan dan menggunakan kredensial dari Direktori Aktif yang berjalan on-premise atau di EC2 Windows. Jika Anda [menggabungkan instans EC2 ke AWS Microsoft AD Terkelola](#), pengguna dapat mengakses beban kerja Windows di AWS Cloud dengan pengalaman masuk

tunggal (SSO) Windows yang sama seperti saat mereka mengakses beban kerja di jaringan lokal Anda.

AWS Microsoft AD yang dikelola juga mendukung kasus penggunaan federasi menggunakan kredensial Active Directory. Sendiri, Microsoft AD yang AWS Dikelola memungkinkan Anda untuk masuk ke file [Konsol Manajemen AWS](#). Dengan [AWS IAM Identity Center](#), Anda juga dapat memperoleh kredensial jangka pendek untuk digunakan dengan AWS SDK dan CLI, dan menggunakan integrasi SAMP yang telah dikonfigurasi sebelumnya untuk masuk ke banyak aplikasi cloud. Dengan menambahkan Microsoft Entra Connect (sebelumnya dikenal sebagai Azure Active Directory Connect), dan secara opsional Active Directory Federation Service (AD FS), Anda dapat masuk ke Microsoft Office 365 dan aplikasi cloud lainnya dengan kredensial yang disimpan di Microsoft AD yang Dikelola. AWS

Layanan ini mencakup fitur-fitur utama yang memungkinkan Anda untuk [Memperpanjang skema Anda](#), [Mengelola kebijakan kata sandi](#), dan [mengaktifkan komunikasi LDAP yang aman](#) melalui Lapisan Soket Aman (SSL)/Keamanan Lapisan Pengangkutan (TLS). Anda juga dapat [mengaktifkan otentikasi multi-faktor \(MFA\) untuk AWS Microsoft AD yang Dikelola](#) untuk memberikan lapisan keamanan tambahan saat pengguna mengakses AWS aplikasi dari Internet. Karena Direktori Aktif adalah direktori LDAP, Anda juga dapat menggunakan Microsoft AD yang Dikelola AWS untuk autentikasi Linux Secure Shell (SSH) dan untuk aplikasi yang mengaktifkan LDAP.

AWS menyediakan pemantauan, snapshot harian, dan pemulihan sebagai bagian dari layanan —Anda [menambahkan pengguna dan grup ke AWS Microsoft AD yang Dikelola](#), dan mengelola Kebijakan Grup menggunakan alat Active Directory yang sudah dikenal yang berjalan di Windows komputer yang bergabung dengan domain Microsoft AD Terkelola AWS . Anda juga dapat menskalakan direktori dengan [men-deploy pengendali domain tambahan](#) dan membantu meningkatkan performa aplikasi dengan mendistribusikan permintaan di sejumlah besar pengendali domain.

AWS Microsoft AD yang dikelola tersedia dalam dua edisi: Standar dan Perusahaan.

- Edisi Standar: Microsoft AD yang Dikelola AWS (Edisi Standar) dioptimalkan untuk menjadi direktori primer untuk bisnis kecil dan menengah sampai dengan 5.000 karyawan. Ini menyediakan kapasitas penyimpanan yang cukup untuk mendukung hingga 30.000* objek direktori, seperti pengguna, grup, dan komputer.
- Edisi Enterprise: Microsoft AD yang Dikelola AWS (Edisi Enterprise) dirancang untuk mendukung organisasi korporasi dengan hingga 500.000* direktori objek.

* batas atas adalah perkiraan. Direktori Anda mungkin mendukung lebih atau kurang objek direktori tergantung pada ukuran objek Anda dan perilaku dan kebutuhan performa aplikasi Anda.

Kapan harus digunakan

AWS Microsoft AD yang dikelola adalah pilihan terbaik Anda jika Anda memerlukan fitur Active Directory yang sebenarnya untuk mendukung AWS aplikasi atau Windows beban kerja, termasuk Amazon Relational Database Service untuk Microsoft SQL Server. Ini juga terbaik jika Anda menginginkan Active Directory mandiri di AWS Cloud yang mendukung Office 365 atau Anda memerlukan direktori LDAP untuk mendukung aplikasi Linux Anda. Untuk informasi selengkapnya, lihat [AWS Microsoft AD yang dikelola](#).

AD Connector

AD Connector adalah layanan proxy yang menyediakan cara mudah untuk menghubungkan AWS aplikasi yang kompatibel, seperti Amazon, Amazon Quick WorkSpaces, dan [Amazon EC2](#) untuk Windows Server instans, ke Active Directory lokal Microsoft yang ada. Dengan AD Connector, Anda cukup [tambahkan satu akun layanan](#) ke Direktori Aktif. AD Connector juga menghilangkan kebutuhan sinkronisasi direktori atau biaya dan kompleksitas hosting infrastruktur federasi.

Saat Anda menambahkan pengguna ke AWS aplikasi seperti Amazon Quick, AD Connector akan membaca Active Directory yang ada untuk membuat daftar pengguna dan grup yang dapat dipilih. Saat pengguna masuk ke AWS aplikasi, AD Connector meneruskan permintaan masuk ke pengontrol domain Active Directory lokal untuk autentikasi. [AD Connector bekerja dengan banyak AWS aplikasi dan layanan termasuk Amazon WorkSpaces, Amazon WorkDocs, Amazon Quick, Amazon Chime, Amazon Connect, dan Amazon. WorkMail](#) Anda juga dapat [menggabungkan Windows instans EC2](#) ke domain Active Directory lokal melalui AD Connector menggunakan gabungan domain [tanpa batas](#). AD Connector juga memungkinkan pengguna Anda mengakses Konsol Manajemen AWS dan mengelola AWS sumber daya dengan masuk dengan kredensial Active Directory yang ada. AD Connector tidak kompatibel dengan RDS SQL Server.

Anda juga dapat menggunakan AD Connector untuk [mengaktifkan otentikasi multi-faktor](#) (MFA) bagi pengguna AWS aplikasi Anda dengan menghubungkannya ke infrastruktur MFA berbasis Radius yang ada. Ini memberikan lapisan keamanan tambahan saat pengguna mengakses aplikasi AWS .

Dengan AD Connector, Anda terus mengelola Direktori Aktif seperti yang Anda lakukan sekarang. Misalnya, Anda menambahkan pengguna dan grup baru serta memperbarui kata sandi

menggunakan alat administrasi Active Directory standar di Direktori Aktif on-premise Anda. Ini membantu Anda secara konsisten menegakkan kebijakan keamanan Anda, seperti kedaluwarsa kata sandi, riwayat kata sandi, dan penguncian akun, baik pengguna mengakses sumber daya di tempat atau di Cloud. AWS

Kapan harus digunakan

AD Connector adalah pilihan terbaik Anda saat ingin menggunakan direktori lokal yang ada dengan AWS layanan yang kompatibel. Untuk informasi selengkapnya, lihat [AD Connector](#).

Simple AD

Simple AD adalah Direktori Microsoft Aktif- direktori yang kompatibel dari AWS Directory Service yang didukung oleh Samba 4. Simple AD mendukung fitur Active Directory dasar seperti akun pengguna, keanggotaan grup, bergabung dengan domain Linux atau instans EC2 Windows berbasis, SSO berbasis Kerberos, dan kebijakan grup. AWS menyediakan pemantauan, snapshot harian, dan pemulihan sebagai bagian dari layanan.

Simple AD adalah direktori mandiri di cloud, di mana Anda membuat dan mengelola identitas pengguna dan mengelola akses ke aplikasi. Anda dapat menggunakan banyak aplikasi yang sadar Direktori Aktif yang familiar dan alat yang memerlukan fitur dasar Direktori Aktif. Simple AD kompatibel dengan AWS aplikasi berikut: [Amazon WorkSpaces](#), [Amazon WorkDocs](#), [Amazon Quick](#), dan [Amazon WorkMail](#). Anda juga dapat masuk ke akun pengguna Simple AD Konsol Manajemen AWS dengan Simple AD dan mengelola AWS sumber daya.

Simple AD tidak mendukung otentikasi multi-faktor (MFA), hubungan kepercayaan, pembaruan dinamis DNS, ekstensi skema, komunikasi melalui LDAPS, cmdlet AD, atau transfer peran FSMO. PowerShell Simple AD tidak kompatibel dengan RDS SQL Server. Pelanggan yang memerlukan fitur Microsoft Active Directory yang sebenarnya, atau yang membayangkan menggunakan direktori mereka dengan RDS SQL Server harus menggunakan Managed AWS Microsoft AD sebagai gantinya. Pastikan aplikasi yang Anda butuhkan kompatibel sepenuhnya dengan Samba 4 sebelum menggunakan Simple AD. Untuk informasi selengkapnya, lihat <https://www.samba.org>.

Kapan harus digunakan

Anda dapat menggunakan Simple AD sebagai direktori mandiri di cloud untuk mendukung Windows beban kerja yang memerlukan fitur Active Directory dasar, AWS aplikasi yang kompatibel, atau untuk mendukung beban kerja Linux yang memerlukan layanan LDAP. Untuk informasi selengkapnya, lihat [Simple AD](#).

Lihat [Ketersediaan wilayah untuk Directory Service](#) untuk daftar jenis direktori yang didukung per Region.

Mana yang harus dipilih

Anda dapat memilih layanan direktori dengan fitur dan skalabilitas yang paling sesuai dengan kebutuhan Anda. Gunakan tabel berikut untuk membantu Anda menentukan opsi AWS Directory Service direktori mana yang paling cocok untuk organisasi Anda.

Apa yang perlu Anda lakukan?	AWS Directory Service Opsi yang disarankan
Saya memerlukan Direktori Aktif atau LDAP untuk aplikasi saya di cloud	Gunakan AWS Directory Service untuk Microsoft Active Directory (Edisi Standar atau Edisi Perusahaan) jika Anda memerlukan Microsoft Active Directory yang sebenarnya di AWS Cloud yang mendukung beban kerja yang sadar Active Directory, atau AWS aplikasi dan layanan seperti Amazon dan WorkSpaces Amazon Quick, atau Anda memerlukan dukungan LDAP untuk aplikasi Linux. Gunakan AWS Directory Service untuk Microsoft Active Directory (Hybrid Edition) untuk memperluas AD yang dikelola sendiri yang ada ke dalam with AWS Cloud AWS Directory Service Gunakan AD Connector jika Anda hanya perlu mengizinkan an pengguna lokal untuk masuk ke AWS aplikasi dan layanan dengan kredensyal Active Directory mereka. Anda juga dapat menggunakan AD Connector untuk menggabungkan instans Amazon EC2 ke domain Direktori Aktif yang ada. Gunakan Simple AD jika Anda memerlukan direktori berskala rendah dan berbiaya rendah dengan kompatibilitas Active Directory dasar yang mendukung aplikasi yang kompatibel dengan Samba 4, atau Anda memerlukan kompatibilitas LDAP untuk aplikasi sadar LDAP.

Apa yang perlu Anda lakukan?	AWS Directory Service Opsi yang disarankan
Saya mengembangkan aplikasi SaaS	Gunakan Amazon Cognito jika Anda mengembangkan aplikasi SaaS skala tinggi dan memerlukan direktori yang dapat diskalakan untuk mengelola dan mengautentikasi pelanggan Anda dan yang berfungsi dengan identitas media sosial.

Untuk informasi selengkapnya tentang opsi AWS Directory Service direktori, lihat [Cara memilih solusi Direktori Aktif AWS](#).

Bekerja dengan Amazon EC2

Sebuah pemahaman dasar Amazon EC2 sangat penting untuk menggunakan Directory Service. Kami menyarankan Anda untuk memulai dengan membaca topik berikut:

- [Apa itu Amazon EC2?](#) di Panduan Pengguna Amazon EC2.
- [Luncurkan instans Amazon EC2](#) di Panduan Pengguna Amazon EC2.
- [Grup keamanan Amazon EC2 untuk instans EC2 Anda di Panduan Pengguna](#) Amazon EC2.
- [Apa itu Amazon VPC?](#) di Panduan Pengguna Amazon VPC.
- [Hubungkan VPC Anda ke jaringan jarak jauh menggunakan AWS Virtual Private Network](#) Panduan Pengguna Amazon VPC.

AWS Microsoft AD yang dikelola

AWS Directory Service untuk Microsoft Active Directory, juga disebut sebagai AWS Managed Microsoft AD, berjalan Microsoft Active Directory sebagai layanan terkelola yang didukung oleh Windows Server 2019. Ini menciptakan sepasang pengontrol domain yang sangat tersedia di VPC Amazon Anda di berbagai Availability Zone, AWS dengan secara otomatis mengelola pemantauan host, pemulihan, replikasi data, snapshot, dan pembaruan perangkat lunak. Layanan ini memungkinkan Anda menjalankan beban kerja yang sadar direktori, mengelola pengguna dan grup, menyediakan sistem masuk tunggal, membuat dan menerapkan kebijakan grup, dan terhubung dengan aman ke instans Amazon EC2.

Directory Service menawarkan dua Microsoft Active Directory solusi: AWS Directory Service untuk Microsoft Active Directory menyediakan layanan Active Directory yang dikelola sepenuhnya di AWS Cloud, sementara AWS Managed Microsoft AD (Hybrid Edition) memperluas AD yang ada yang dikelola sendiri. AWS

AWS Microsoft AD yang dikelola (Edisi Standar dan Edisi Perusahaan) membuat domain AD terkelola baru untuk mengelola pengguna, perangkat, dan komputer AWS. Direktori ini membangun hutan sumber daya yang menciptakan hubungan kepercayaan dengan domain AD Anda yang ada di tempat, di AWS, atau di lingkungan multi-cloud. Pengguna dapat mengakses AWS sumber daya dengan kredensialnya yang ada dari domain AD Anda saat ini. Identitas pengguna tetap berada di domain AD Anda yang ada saat hutan sumber daya mengelola sumber AWS daya Anda, menjaga isolasi operasional antar lingkungan sambil menyediakan sistem masuk tunggal yang mulus.

AWS Microsoft AD yang dikelola (Edisi Hybrid) menghubungkan Active Directory yang dikelola sendiri dengan AWS Directory Service untuk Microsoft Active Directory, menciptakan lingkungan identitas terintegrasi yang mencakup infrastruktur dan jaringan. AWS Cloud Solusi ini memperluas layanan direktori Anda AWS tanpa menyinkronkan identitas pengguna, membangun hubungan kepercayaan antar lingkungan, dan menyediakan akses tanpa batas menggunakan kredensial yang ada.

Dengan Microsoft AD yang AWS Dikelola, Anda dapat menjalankan beban kerja yang sadar direktori di AWS Cloud, termasuk aplikasi berbasis .NET Microsoft SharePoint dan SQL Server kustom. Anda juga dapat mengonfigurasi hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan Direktori Microsoft Aktif yang dikelola sendiri yang ada, memberikan pengguna dan grup akses ke sumber daya di salah satu domain yang digunakan AWS IAM Identity Center.

Mana yang harus dipilih

Anda dapat memilih antara dua AWS Directory Service layanan dengan fitur dan skalabilitas yang paling sesuai dengan kebutuhan Anda. Tabel berikut membantu Anda menentukan Directory Service opsi mana yang paling cocok untuk organisasi Anda.

Kasus penggunaan	Solusi yang direkomendasikan
Jalankan beban kerja, AWS aplikasi, atau aplikasi Linux yang sadar direktori yang membutuhkan dukungan LDAP	AWS Microsoft AD yang dikelola (Edisi Standar dan Edisi Perusahaan) membuat domain AD terkelola baru untuk mengelola pengguna, perangkat, dan komputer AWS. Direktori ini membangun hutan sumber daya yang menciptakan hubungan kepercayaan dengan domain AD Anda yang ada di tempat, di AWS, atau di lingkungan multi-cloud. Pengguna dapat mengakses AWS sumber daya dengan kredensialnya yang ada dari domain AD Anda saat ini. Identitas pengguna tetap berada di domain AD Anda yang ada saat hutan sumber daya mengelola sumber AWS daya Anda, menjaga isolasi operasional antar lingkungan sambil menyediakan sistem masuk tunggal yang mulus.
Perluas Direktori Aktif yang ada ke AWS	AWS Microsoft AD yang dikelola (Edisi Hybrid) menghubungkan Active Directory yang dikelola sendiri dengan AWS Directory Service untuk Microsoft Active Directory, menciptakan lingkungan identitas terintegrasi yang mencakup infrastruktur dan jaringan. AWS Cloud Solusi ini memperluas layanan direktori Anda AWS tanpa menyinkronkan identitas pengguna, membangun hubungan kepercayaan antar lingkungan, dan menyediakan akses tanpa batas menggunakan kredensial yang ada.

Topik

- [Memulai dengan Microsoft AD yang AWS Dikelola](#)
- [Memahami Microsoft AD yang AWS Dikelola \(Edisi Hybrid\)](#)

Memahami Microsoft AD yang AWS Dikelola (Edisi Hybrid)

AWS Microsoft AD yang dikelola (Edisi Hybrid) memungkinkan Anda memperluas Direktori Aktif yang ada ke AWS Cloud dengan Microsoft AD yang AWS Dikelola. Fitur ini memudahkan Anda memindahkan beban kerja yang bergantung pada iklan ke AWS, mengadopsi AWS layanan, dan meningkatkan redundansi Direktori Aktif Anda. AWS akan secara berkala menjalankan penilaian direktori pada direktori hybrid Anda yang dapat Anda lihat di Directory Service konsol.

Direktori hybrid di Directory Service menghubungkan yang sudah ada Microsoft Active Directory dengan AWS Directory Service untuk Microsoft Active Directory (AWS Managed Microsoft AD). Ini menciptakan lingkungan identitas terintegrasi yang mencakup infrastruktur lokal AWS, dan multi-cloud, memungkinkan Anda mempertahankan satu sumber identitas sambil memperluas layanan direktori Anda. AWS

Konfigurasi direktori hybrid menyediakan beberapa kemampuan penting:

- Perpanjangan AD yang dikelola sendiri ke AWS Cloud tanpa perlu membangun hubungan kepercayaan
- Otentikasi dan otorisasi tanpa batas di seluruh lingkungan menggunakan kredensi Active Directory yang ada
- Kredensi pengguna yang konsisten dan keanggotaan grup di kedua lingkungan iklan Anda
- Manajemen terpusat kebijakan dan izin akses AD

Topik

- [Prasyarat direktori hybrid](#)
- [Membuat direktori hybrid](#)
- [Melihat dan mengedit direktori hybrid](#)
- [Menghapus direktori hybrid](#)
- [Penilaian direktori untuk direktori hybrid](#)
- [Pemecahan masalah direktori hibrida dan penilaian direktori](#)

Prasyarat direktori hybrid

Direktori Hybrid memperluas Direktori Aktif yang dikelola sendiri ke file. AWS Cloud Sebelum membuat direktori hybrid, pastikan lingkungan Anda memenuhi persyaratan ini:

Microsoft Active Directory persyaratan domain

Sebelum membuat direktori hybrid, pastikan lingkungan dan infrastruktur AD yang dikelola sendiri memenuhi persyaratan berikut, dan kumpulkan informasi yang diperlukan.

Persyaratan domain

Lingkungan AD yang dikelola sendiri harus memenuhi persyaratan berikut:

- Menggunakan tingkat Windows Server 2012 R2 atau 2016 fungsional.
- Menggunakan pengontrol domain standar untuk dinilai untuk pembuatan direktori hybrid. Read-only domain controllers (RODC) tidak dapat digunakan untuk pembuatan direktori hybrid.
- Memiliki dua pengontrol domain dengan semua layanan Active Directory berjalan.
- Pengontrol Domain Utama (PDC) harus dapat dirutekan setiap saat.

Secara khusus, PDC Emulator dan RID Master IPs dari AD yang dikelola sendiri harus berada dalam salah satu kategori berikut:

- Bagian dari rentang alamat IP RFC1918 pribadi (10.0.0.0/8, 172.16.0.0/12, atau 192.168.0.0/16)
- Dalam rentang CIDR VPC Anda
- Cocokkan DNS instance IPs yang dikelola sendiri untuk direktori

Anda dapat menambahkan rute IP tambahan untuk direktori setelah direktori hybrid dibuat.

Informasi yang diperlukan

Kumpulkan informasi berikut tentang iklan yang dikelola sendiri:

- Nama DNS Direktori
- Direktori DNS IPs
- Kredensial akun layanan dengan izin Administrator untuk AD yang dikelola sendiri
- AWS Rahasia ARN untuk menyimpan kredensial akun layanan Anda (lihat [AWS Rahasia ARN untuk direktori hybrid](#))

AWS Rahasia ARN untuk direktori hybrid

Untuk mengonfigurasi direktori hybrid dengan AD yang dikelola sendiri, Anda perlu membuat kunci KMS untuk mengenkripsi AWS rahasia Anda dan kemudian membuat rahasia itu sendiri. Kedua sumber daya harus dibuat sama Akun AWS yang berisi direktori hybrid.

Buat kunci KMS

Kunci KMS digunakan untuk mengenkripsi rahasia Anda AWS .

Important

Untuk Kunci Enkripsi, jangan gunakan kunci KMS default AWS . Pastikan untuk membuat kunci AWS KMS yang sama yang berisi direktori hybrid Akun AWS yang ingin Anda buat untuk bergabung dengan AD yang dikelola sendiri.

Untuk membuat kunci AWS KMS

1. Di AWS KMS konsol, pilih tombol Buat.
2. Untuk Tipe Kunci, pilih Simetris.
3. Untuk Penggunaan Kunci, pilih Enkripsi dan dekripsi.
4. Untuk Opsi lanjutan:
 - a. Untuk Asal materi kunci, pilih KMS.
 - b. Untuk Regionalitas, pilih kunci Wilayah Tunggal dan pilih Berikutnya.
5. Untuk Alias, berikan nama untuk kunci KMS.
6. (Opsional) Untuk Deskripsi, berikan deskripsi kunci KMS.
7. (Opsional) Untuk Tag, tambahkan tag untuk kunci KMS dan pilih Berikutnya.
8. Untuk administrator Key, pilih pengguna IAM.
9. Untuk penghapusan Kunci, pertahankan pilihan default untuk Izinkan administrator kunci untuk menghapus kunci ini dan pilih Berikutnya.
10. Untuk pengguna Key, pilih pengguna IAM yang sama dari langkah sebelumnya dan pilih Berikutnya.
11. Tinjau konfigurasi tersebut.
12. Untuk kebijakan Kunci, tambahkan pernyataan berikut ke kebijakan:
13. Pilih Selesai.

Buat AWS rahasia

Buat rahasia di Secrets Manager untuk menyimpan kredensial akun pengguna AD yang dikelola sendiri.

 Important

Buat rahasia yang sama Akun AWS yang berisi direktori hybrid yang ingin Anda gabungkan dengan AD yang dikelola sendiri.

Untuk membuat rahasia

- Di Secrets Manager, pilih Simpan rahasia baru
- Untuk tipe Rahasia, pilih Jenis rahasia lainnya
- Untuk Pasangan kunci/nilai, tambahkan dua kunci Anda:
 1. Tambahkan kunci nama pengguna
 - a. Untuk kunci pertama, masukkan `customerAdAdminDomainUsername`.
 - b. Untuk nilai kunci pertama, masukkan hanya nama pengguna (tanpa awalan domain) dari pengguna AD. Jangan sertakan nama domain karena ini menyebabkan pembuatan instance gagal.
 2. Tambahkan kunci kata sandi
 - a. Untuk kunci kedua, masukkan `customerAdAdminDomainPassword`.
 - b. Untuk nilai kunci kedua, masukkan kata sandi yang Anda buat untuk pengguna AD di domain Anda.

Selesaikan konfigurasi rahasia

1. Untuk kunci Enkripsi, pilih kunci KMS yang Anda buat [Buat kunci KMS](#) dan pilih Berikutnya.
2. Untuk nama Rahasia, masukkan deskripsi untuk rahasia.
3. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk rahasia.
4. Pilih Berikutnya.
5. Untuk Konfigurasi pengaturan rotasi, pertahankan nilai default dan pilih Berikutnya.
6. Tinjau pengaturan untuk rahasia dan pilih Store.
7. Pilih rahasia yang Anda buat dan salin nilai ARN Rahasia. Anda akan menggunakan ARN ini di langkah berikutnya untuk mengatur Direktori Aktif yang dikelola sendiri.

Persyaratan infrastruktur

Siapkan komponen infrastruktur berikut:

- Dua AWS Systems Manager node dengan hak administrator untuk agen SSM
 - Jika Active Directory dikelola sendiri di luar AWS Cloud, Anda memerlukan dua node Systems Manager untuk lingkungan hybrid dan multicloud. Untuk informasi selengkapnya tentang cara menyediakan node ini, lihat [Menyiapkan Systems Manager untuk lingkungan hybrid dan multicloud](#).
 - Jika Active Directory dikelola sendiri di dalam AWS Cloud, Anda memerlukan dua instans EC2 terkelola Systems Manager. Untuk informasi selengkapnya tentang cara menyediakan instans ini, lihat [Mengelola instans EC2 dengan Systems Manager](#).

Layanan Direktori Aktif yang Diperlukan

Pastikan layanan berikut berjalan pada iklan yang dikelola sendiri:

- Layanan Domain Direktori Aktif
- Layanan Web Direktori Aktif (ADWS)
- Sistem Acara COM+
- Distributed File System Replication (DFSR)
- Sistem Nama Domain (DNS)
- Server DNS
- Klien Kebijakan Grup
- Pesan Antar Situs
- Panggilan Prosedur Jarak Jauh (RPC)
- Manajer Akun Keamanan
- Server Waktu Windows

Note

Direktori hybrid membutuhkan port UDP 123 untuk terbuka dan Windows Time Server diaktifkan dan berfungsi. Kami menyinkronkan waktu dengan pengontrol domain Anda untuk memastikan replikasi direktori hybrid berfungsi dengan baik.

Persyaratan otentikasi Kerberos

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Untuk petunjuk terperinci tentang cara mengaktifkan setelan ini, lihat [Memastikan pra-otentikasi Kerberos](#) diaktifkan. Untuk informasi umum tentang pengaturan ini, buka [Preauthentication](#) on. Microsoft TechNet

Jenis enkripsi yang didukung

direktori hybrid mendukung jenis enkripsi berikut saat mengautentikasi melalui Kerberos ke pengontrol domain Active Directory Anda:

- AES-256-HMAC

Persyaratan port jaringan

AWS Untuk memperluas pengontrol domain Active Directory yang dikelola sendiri, firewall untuk jaringan yang ada harus memiliki port berikut yang terbuka CIDRs untuk kedua subnet di VPC Amazon Anda:

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Autentikasi Kerberos
- UDP 123 - Server waktu
- TCP 135 - Panggilan Prosedur Jarak Jauh
- TCP/UDP 389 - LDAP
- TCP 445 - SMB
- TCP 636 - Hanya diperlukan untuk lingkungan dengan Lightweight Directory Access Protocol Secure (LDAPS)
- TCP 49152-65535 - RPC secara acak mengalokasikan port TCP tinggi
- TCP 3268 dan 3269 - Katalog Global
- TCP 9389 Layanan Web Direktori Aktif (ADWS)

Ini adalah port minimum yang diperlukan untuk membuat direktori hybrid. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

 Note

DNS yang IPs disediakan untuk Pengontrol Domain dan pemegang Peran FSMO Anda harus memiliki port di atas terbuka CIDRs untuk kedua subnet di Amazon VPC.

 Note

Direktori hybrid membutuhkan port UDP 123 untuk terbuka dan Windows Time Server diaktifkan dan berfungsi. Kami menyinkronkan waktu dengan pengontrol domain Anda untuk memastikan replikasi direktori hybrid berfungsi dengan baik.

Akun AWS izin

Anda akan memerlukan izin untuk tindakan berikut di: Akun AWS

- EC2: AuthorizeSecurityGroupEgress
- EC2: AuthorizeSecurityGroupIngress
- EC2: CreateNetworkInterface
- EC2: CreateSecurityGroup
- EC2: DescribeNetworkInterfaces
- EC2: DescribeSubnets
- EC2: DescribeVpcs
- EC2: CreateTags
- EC2: CreateNetworkInterfacePermission
- ssm: ListCommands
- ssm: GetCommandInvocation
- ssm: GetConnectionStatus
- ssm: SendCommand
- manajer rahasia: DescribeSecret
- manajer rahasia: GetSecretValue
- saya: GetRole
- saya: CreateServiceLinkedRole

Persyaratan jaringan Amazon VPC

VPC dengan yang berikut ini:

- Setidaknya dua subnet. Masing-masing subnet harus berada di Availability Zone yang berbeda
- VPC harus memiliki tenancy default

Anda tidak dapat membuat direktori hybrid di VPC menggunakan alamat di ruang alamat 198.18.0.0/15.

Directory Service menggunakan dua struktur VPC. Instans EC2 yang membentuk direktori Anda berjalan di luar Akun AWS, dan dikelola oleh AWS Mereka memiliki dua adaptor jaringan, ETH0 dan ETH1. ETH0 adalah adaptor pengelola, dan berada di luar akun Anda. ETH1 dibuat dalam akun Anda.

Rentang IP manajemen ETH0 jaringan untuk direktori Anda adalah 198.18.0.0/15.

Untuk informasi selengkapnya, lihat topik berikut dalam Panduan Pengguna Amazon VPC:

- [Apa itu Amazon VPC?](#)
- [Apa itu Amazon VPC?](#)
- [VPCs dan subnet](#)
- [Apa itu AWS Site-to-Site VPN?](#)

Untuk informasi lebih lanjut tentang AWS Direct Connect, lihat [Apa itu AWS Direct Connect?](#)

AWS konfigurasi grup keamanan

Secara default, AWS melampirkan grup keamanan untuk memungkinkan akses jaringan ke node AWS Systems Manager terkelola di VPC Anda. Anda dapat secara opsional menyediakan grup keamanan Anda sendiri yang memungkinkan lalu lintas jaringan ke dan dari pengontrol domain yang dikelola sendiri di luar VPC Anda.

Anda dapat secara opsional menyediakan grup keamanan Anda sendiri yang memungkinkan lalu lintas jaringan ke dan dari pengontrol domain yang dikelola sendiri di luar VPC Anda. Jika Anda menyediakan grup keamanan Anda sendiri, maka Anda perlu:

- Izinkan daftar VPC CIDR rentang dan rentang yang dikelola sendiri.

- Pastikan rentang ini tidak tumpang tindih dengan rentang [IP yang AWS dicadangkan](#)

Pertimbangan penilaian direktori

Berikut ini adalah pertimbangan saat membuat penilaian direktori dan jumlah penilaian yang dapat Anda miliki di: Akun AWS

- Penilaian direktori dibuat secara otomatis saat Anda membuat direktori hybrid. Ada dua jenis penilaian: CUSTOMER dan SYSTEM. Anda Akun AWS memiliki batas 100 penilaian CUSTOMER direktori.
- Jika Anda mencoba membuat direktori hybrid dan Anda sudah memiliki 100 penilaian CUSTOMER direktori, Anda akan menemukan kesalahan. Hapus penilaian untuk membebaskan kapasitas sebelum mencoba lagi.
- Anda dapat meminta peningkatan kuota penilaian CUSTOMER direktori Anda dengan menghubungi Dukungan atau menghapus penilaian direktori PELANGGAN yang ada untuk membebaskan kapasitas.

Membuat direktori hybrid

Sebelum membuat direktori hybrid, Anda harus membuat dan berhasil lulus penilaian direktori yang memverifikasi konektivitas dan interoperabilitas dengan Active Directory yang dikelola sendiri

Membuat direktori hybrid dengan AD yang dikelola sendiri

Ikuti langkah-langkah berikut untuk membuat direktori hybrid dengan AD yang dikelola sendiri:

Untuk membuat direktori hybrid

1. Buka Directory Service konsol untuk wilayah yang Anda inginkan.
2. Pada halaman Pilih jenis direktori, pilih AWS Dikelola Microsoft AD.
3. Di bawah Memulai dengan Microsoft AD yang AWS Dikelola, pilih Perluas domain AD Anda dengan direktori hibrid — baru, lalu pilih Berikutnya. Ini mengarahkan Anda ke halaman Create directory assessment.
4. Sebelum Anda dapat membuat direktori hybrid, Anda harus terlebih dahulu membuat dan berhasil lulus penilaian direktori. Untuk membuat penilaian direktori, ikuti langkah-langkahnya [Membuat penilaian direktori](#). Setelah Anda berhasil melewati penilaian direktori, Anda dapat melanjutkan prosedur ini.

5. Setelah Anda berhasil melewati penilaian direktori, arahkan ke halaman Direktori.
6. Pada halaman Direktori, di bawah Uji coba penilaian direktori hibrida pilih ID Penilaian dengan Status. SUCCESS Kemudian pilih Buat direktori hybrid, yang mengarahkan Anda ke halaman detail penilaian
7. Pada halaman detail penilaian, konfirmasi tindakan ini dengan memilih Create hybrid directory, yang membuka halaman Create hybrid using assessment id.
8. Pada direktori Create hybrid menggunakan halaman assessment id, Tinjau informasi Active Directory yang dikelola sendiri. Setelah mengonfirmasi informasi, pilih Buat direktori hybrid.

Setelah memilih Buat direktori hybrid, AWS jalankan penilaian direktori lain berdasarkan informasi ini untuk mengonfirmasi bahwa konfigurasi AD yang dikelola sendiri masih valid. Jika penilaian direktori berhasil lolos, maka kami membuat direktori hybrid.

9. Memilih Buat direktori hybrid mengembalikan Anda ke halaman Direktori.
 - a. Spanduk hijau akan muncul setelah direktori hybrid berhasil dibuat.
 - b. Spanduk merah akan muncul jika pembuatan direktori hybrid gagal. Bersihkan kegagalan pembuatan direktori hybrid dengan menyelesaikan yang berikut:
 1. Hapus direktori hybrid yang gagal di konsol.
 2. Hapus semua AWS Cadangan yang tersisa OUs di AD yang dikelola sendiri.

Informasi lebih lanjut

- [Menghapus direktori hybrid](#)
- [Pemecahan masalah](#)

Melihat dan mengedit direktori hybrid

Gunakan prosedur berikut untuk melihat atau mengedit direktori hybrid Anda.

Melihat direktori hybrid

Anda dapat melihat direktori hybrid di Directory Service konsol.

Untuk melihat informasi direktori terperinci.

1. Pada panel navigasi [konsol Directory Service](#), pilih Direktori.

2. Pilih tautan ID direktori untuk direktori Anda. Informasi tentang direktori muncul di halaman Detail direktori.

Informasi Direktori Aktif yang dikelola sendiri

Bagian ini memberikan informasi tentang Active Directory yang dikelola sendiri yang digabungkan dengan AWS infrastruktur.

- Jenis direktori
- ID Direktori
- Status direktori
- Detail jaringan untuk iklan yang dikelola sendiri, seperti:
 - VPC
 - Subnet
 - Alamat DNS
- Node terkelola Systems Manager

Tab direktori hibrid

Anda dapat menemukan informasi berikut tentang Microsoft AD yang AWS Dikelola:

- Pada tab Bagikan & bagikan, Anda dapat membagikan iklan Microsoft AWS Terkelola dengan AWS akun lain dan melihat detail jaringan untuk pengontrol domain Anda.
- Pada tab Manajemen aplikasi, Anda dapat mengaktifkan URL akses aplikasi untuk iklan Microsoft AWS Terkelola dan mengaktifkan AWS aplikasi dan layanan untuk iklan Microsoft yang AWS Dikelola.
- Pada tab Pemeliharaan, Anda dapat mengaktifkan SNS untuk menerima pemberitahuan status Microsoft AD yang AWS Dikelola dan meninjau snapshot dari AWS Microsoft AD yang Dikelola.
- Untuk informasi selengkapnya tentang bidang Status, lihat [Memahami status direktori Microsoft AD yang AWS Dikelola](#).

Memperbarui direktori hybrid

Anda dapat memperbarui direktori hybrid di Directory Service konsol untuk mengubah pengaturan DNS atau memulihkan akses akun administrator.

Untuk memperbarui informasi direktori hybrid

1. Pada panel navigasi [konsol Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda untuk membuka halaman detail Direktori.
3. Pilih Tindakan, lalu pilih Perbarui informasi direktori hybrid.
4. Pada halaman Perbarui informasi direktori hybrid, Anda dapat memperbarui pengaturan DNS atau memulihkan akun administrator Anda.

Perbarui pengaturan DNS (opsional)

Di bawah informasi Direktori Aktif yang dikelola sendiri, Anda dapat mengubah yang berikut ini:

- a. Nama DNS Direktori
- b. Alamat IP DNS

Anda dapat memperbarui kedua pengaturan bersama-sama atau secara individual. Setidaknya satu perubahan diperlukan untuk proses pembaruan.

5. Pulihkan akun administrator direktori hybrid

Untuk memulihkan akun administrator direktori hybrid Anda, kami memerlukan akses sementara ke pengguna. Akses ini disediakan melalui rahasia dari Secrets Manager. Kami menggunakan kredensi ini hanya sekali selama pemulihan dan tidak menyimpannya. Jika akun administrator direktori hybrid Anda ada, Anda tidak perlu memperbarui rahasia ini, bahkan jika Anda memperbarui pengguna administrator Active Directory yang dikelola sendiri.

- Rahasia kredensial admin - Kami membuat akun administrator direktori hybrid saat kami membuat direktori hybrid. Jika Anda menghapus rahasia ini, masukkan rahasia Secrets Manager untuk pengguna administrator AD yang dikelola sendiri.

Menghapus direktori hybrid

Saat Anda menghapus direktori hybrid, semua data direktori dan snapshot dihapus dan tidak dapat dipulihkan. Setelah direktori dihapus, semua instance yang bergabung ke direktori tetap utuh.

Namun, Anda tidak dapat menggunakan kredensi direktori untuk masuk ke instance ini. Anda harus masuk ke instance ini dengan akun pengguna lokal.

Untuk menghapus direktori

1. Di panel navigasi [konsol Directory Service](#), pilih Direktori. Pastikan Anda berada di AWS Region tempat direktori hybrid Anda digunakan. Untuk informasi selengkapnya, lihat [Memilih Wilayah](#).
2. Pastikan tidak ada AWS aplikasi yang diaktifkan untuk direktori yang ingin Anda hapus. AWS Aplikasi yang diaktifkan akan mencegah Anda menghapus direktori hybrid Anda.
3. Pada halaman Direktori, pilih ID direktori Anda.
4. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi. Di bagian AWS aplikasi & layanan, Anda melihat AWS aplikasi mana yang diaktifkan untuk direktori Anda.
 - a. Nonaktifkan Konsol Manajemen AWS akses. Untuk informasi selengkapnya, lihat [Menonaktifkan akses Konsol AWS Manajemen](#).
 - b. Untuk menonaktifkan Amazon FSx untuk Windows File Server, Anda harus menghapus sistem FSx file Amazon dari domain. Untuk informasi selengkapnya, lihat [Bekerja dengan Active Directory FSx untuk Windows File Server](#) di Amazon FSx untuk Windows File Server User Guide.
 - c. Untuk menonaktifkan Amazon Relational Database Service, Anda harus menghapus instans Amazon RDS dari domain. Untuk informasi selengkapnya, lihat [Mengelola instans DB dalam domain](#) dalam Panduan Pengguna Amazon RDS.
5. Di panel navigasi, pilih Direktori.
6. Pilih hanya direktori yang akan dihapus dan pilih Hapus. Ini akan memerlukan beberapa menit agar direktori dihapus. Ketika direktori telah dihapus, itu akan dihapus dari daftar direktori Anda.
7. Hapus secara manual objek pengontrol domain yang tersisa, termasuk AWS Cadangan apa pun OUs. Anda dapat menghapus seluruh direktori AWS Reserved untuk menyelesaikan pembersihan lingkungan Anda.

Penilaian direktori untuk direktori hybrid

Penilaian direktori memeriksa lingkungan Active Directory yang dikelola sendiri untuk memastikannya memenuhi persyaratan untuk membuat direktori hybrid. Penilaian ini memverifikasi konektivitas jaringan, konfigurasi pengontrol domain, dan layanan yang diperlukan untuk membantu mengidentifikasi dan menyelesaikan masalah potensial sebelum membuat koneksi antara AD yang dikelola sendiri dan Directory Service

Ada dua jenis penilaian direktori:

- *CUSTOMER*penilaian — Dimulai oleh Anda di konsol saat Anda mulai menyiapkan direktori hybrid. Anda dapat menghapus penilaian direktori pelanggan, bahkan saat penilaian tersebut sedang berlangsung. Anda dapat memiliki hingga 100 penilaian pelanggan.
- *SYSTEM*penilaian — Secara otomatis dibuat oleh AWS dan dijalankan secara berkala setelah pembuatan berhasil. Anda tidak dapat menghapus *SYSTEM* penilaian.

Penilaian direktori memberikan informasi berharga tentang kesiapan lingkungan Anda, termasuk:

- Konektivitas antara AD yang dikelola sendiri dan AWS
- Ketersediaan layanan yang diperlukan pada pengontrol domain Anda
- Kompatibilitas konfigurasi dengan persyaratan AWS Directory Service
- Potensi masalah yang mungkin mencegah pembuatan direktori hybrid yang berhasil

Penilaian direktori yang berhasil (lulus) diperlukan sebelum Anda dapat membuat direktori hybrid. Jika penilaian gagal, Anda dapat melihat laporan terperinci untuk mengidentifikasi dan mengatasi masalah sebelum mencoba lagi. AWS menghapus *SYSTEM* penilaian setelah 30 hari.

Topik

- [Membuat penilaian direktori](#)
- [Melihat penilaian direktori](#)
- [Menghapus penilaian direktori](#)

Membuat penilaian direktori

Anda dapat membuat penilaian direktori sebagai bagian dari membuat direktori hybrid, atau Anda dapat membuatnya secara manual. Untuk membuat penilaian secara manual, buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>. Pada halaman Direktori, di bawah bagian Penilaian direktori, pilih Buat penilaian.

Untuk membuat penilaian direktori

1. Pada halaman Buat penilaian direktori, untuk nama DNS Direktori, masukkan nama DNS Direktori Aktif yang dikelola sendiri.
2. Untuk Alamat IP DNS, masukkan dua alamat IP DNS untuk AD yang dikelola sendiri.

3. Direktori hybrid membutuhkan VPC Amazon dengan setidaknya dua subnet. Jika Anda belum memilikinya, Anda dapat membuatnya. Di bagian Jaringan, berikan yang berikut ini:
 - a. Untuk VPC, pilih pengidentifikasi VPC Anda.
 - b. Untuk Subnet, pilih pengenalan untuk masing-masing dari dua subnet. Setiap subnet harus berada di Availability Zone yang berbeda. Untuk informasi selengkapnya, lihat [Persyaratan jaringan Amazon VPC](#).
 - c. Untuk grup Keamanan, pilih pengenalan grup keamanan. Secara default, AWS melampirkan grup keamanan untuk memungkinkan akses jaringan ke node AWS Secrets Manager terkelola di VPC Amazon Anda. Anda dapat secara opsional menyediakan grup keamanan Anda sendiri yang memungkinkan lalu lintas jaringan ke dan dari pengontrol domain yang dikelola sendiri di luar VPC Amazon Anda.
4. Di bagian AWS Systems Manager node, pilih dua node Systems Manager atau instance berdasarkan persyaratan berikut:
 - Jika Active Directory Anda dikelola sendiri di luar AWS Cloud, Anda akan memerlukan dua node Systems Manager untuk lingkungan hybrid dan multicloud. Untuk informasi selengkapnya tentang cara menyediakan node ini, lihat [Menyiapkan Systems Manager untuk lingkungan hybrid dan multicloud](#).
 - Jika Active Directory dikelola sendiri di dalam AWS Cloud, Anda memerlukan dua EC2 instans yang dikelola Systems Manager. Untuk informasi selengkapnya tentang cara menyediakan instance ini, lihat [Mengelola EC2 instans dengan Systems Manager](#).
5. Pilih Berikutnya untuk membuka halaman Ulasan dan membuat penilaian direktori.
6. Pada halaman Tinjau dan buat penilaian direktori, tinjau informasi penilaian direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat penilaian. Membuat penilaian direktori membutuhkan waktu sekitar 30 menit. Anda dikembalikan ke halaman detail Direktori. Spanduk hijau muncul saat penilaian direktori berhasil.

 Warning

Untuk membuat direktori hybrid, penilaian direktori harus memasukkan status SUCCESS. Anda tidak dapat membuat direktori hybrid tanpa terlebih dahulu berhasil melewati penilaian direktori.

Melihat penilaian direktori

Anda dapat melihat penilaian direktori di Konsol Manajemen AWS untuk meninjau hasil penilaian dan mengelola laporan penilaian Anda.

Untuk melihat penilaian direktori

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Pada halaman Direktori, di bawah bagian Penilaian direktori hibrida percobaan, pilih penilaian yang ingin Anda lihat. Ini membuka halaman detail penilaian.
3. Pada halaman detail penilaian, Anda dapat memilih:
 - Unduh untuk mengunduh laporan penilaian direktori sebagai file CSV.
 - Hapus untuk menghapus laporan penilaian direktori.
 - Buat penilaian untuk membuat penilaian direktori baru.
4. Dari halaman detail penilaian, Anda dapat melihat informasi berikut:
 - a. Informasi penilaian, seperti ID penilaian, status, apakah itu dibuat oleh pelanggan atau sistem, dan kapan terakhir diperbarui.
 - b. Detail AD yang dikelola sendiri seperti nama DNS, VPC, dan subnet.
 - c. AWS Systems Manager mengelola informasi node, seperti alamat IP, status penilaian, dan jumlah tes penilaian yang lulus dan gagal.
 - d. Status penilaian untuk pengontrol domain. Anda juga dapat meninjau detail pengujian penilaian dengan memilih pengontrol domain. Kode kesalahan muncul di kolom Status untuk pengujian penilaian yang gagal.

Menghapus penilaian direktori

Anda dapat menghapus penilaian direktori yang dibuat pelanggan di. Konsol Manajemen AWS Anda tidak dapat menghapus penilaian yang dimulai sistem yang dibuat secara otomatis. AWS

Untuk menghapus penilaian direktori pelanggan

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Pada halaman Direktori, di bawah bagian Penilaian direktori, pilih penilaian pelanggan yang ingin Anda hapus. Atau, Anda dapat memilih kotak centang di samping penilaian direktori yang ingin Anda hapus dan kemudian dari menu Tindakan, pilih Hapus.

3. Anda diarahkan ke halaman Detail Penilaian. Pilih Tindakan dan kemudian pilih Hapus Penilaian. Kotak dialog penilaian direktori Hapus muncul. Pilih Hapus.

Pemecahan masalah direktori hibrida dan penilaian direktori

Penilaian direktori diperlukan untuk membuat direktori hybrid. Tes penilaian dijalankan pada setiap pengontrol domain. Tes penilaian memeriksa area yang berbeda dan menghasilkan status Lulus atau Gagal. Jika penilaian direktori Anda gagal, Anda dapat melihat pengujian penilaian pengontrol domain Anda untuk mengidentifikasi masalah apa yang menyebabkan kegagalan.

Important

Direktori hybrid dapat dibuat ketika status penilaian direktori Lulus dengan peringatan. Kami menyarankan Anda mengatasi masalah yang menyebabkan peringatan sebelum membuat direktori hybrid

Topik

- [Pemecahan masalah penilaian direktori hybrid yang gagal](#)
- [Kesalahan Status Direktori](#)
- [Pesan Kesalahan Penilaian Direktori](#)
- [Pesan kesalahan Uji Penilaian](#)
- [Pesan peringatan Tes Penilaian](#)

Pemecahan masalah penilaian direktori hybrid yang gagal

Anda dapat memecahkan masalah penilaian direktori yang gagal dari halaman Direktori di halaman. Konsol Manajemen AWS

1. Masuk ke Konsol Manajemen AWS dan buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Di bawah bagian Penilaian direktori, pilih penilaian direktori hybrid yang gagal.
3. Pada halaman Rincian Penilaian, tinjau penilaian direktori dan identifikasi tes apa yang gagal.
 - Tes penilaian pengontrol domain akan memiliki informasi lebih lanjut tentang tes apa yang berhasil atau gagal. Kolom Status memberikan rincian lebih lanjut tentang apa yang

menyebabkan tes gagal. Untuk melihat pengujian penilaian pengontrol domain Anda, lihat [Melihat penilaian direktori](#).

4. Mengatasi masalah yang menyebabkan kegagalan pada Direktori Aktif yang dikelola sendiri atau Microsoft AD yang AWS dikelola sendiri. Lihat [Pesan Kesalahan Penilaian Direktori](#) dan [Pesan kesalahan Uji Penilaian](#) untuk informasi lebih lanjut.
5. Kembali ke penilaian yang gagal di Directory Service konsol. Pilih Buat penilaian di pesan peringatan merah. Lihat [Membuat direktori hybrid dengan AD yang dikelola sendiri](#) untuk informasi selengkapnya tentang membuat penilaian direktori.

Kesalahan Status Direktori

Directory Service direktori dapat menemukan berbagai negara yang menunjukkan berbagai jenis masalah. Memahami status ini membantu Anda menentukan langkah pemecahan masalah yang sesuai.

Jenis Status Direktori

Status	Deskripsi	Tindakan yang Diperlukan
Aktif	Pembuatan direktori selesai dengan sukses dan beroperasi secara normal.	Tidak ada tindakan diperlukan.
Terganggu	Direktori berhasil dibuat, tetapi pengontrol domain mengalami masalah sesudahnya. Sistem mencoba pemulihan otomatis.	Pantau status direktori. Jika masalah berlanjut, hubungi AWS Support.
Gagal	Pembuatan direktori gagal dan tidak dapat dipulihkan.	Hapus direktori yang gagal dan buat yang baru.
Tidak dapat dioperasikan (hanya iklan hibrida)	AWS mendeteksi masalah keamanan dan secara otomatis mengisolasi direktori untuk perlindungan. Direktori menjadi benar-benar tidak dapat digunakan sampai dipulihkan.	Contact AWS Dukungan Center segera. Status ini memerlukan Dukungan intervensi untuk menyelidiki dan memulihkan direktori.

Pesan Kesalahan Penilaian Direktori

Untuk membuat direktori hybrid, Anda perlu penilaian direktori yang lulus. Penilaian direktori dapat gagal karena berbagai alasan.

Tabel berikut menunjukkan pesan kesalahan penilaian direktori dan cara mengatasinya.

Pesan Kesalahan Penilaian Direktori & Resolusi

Pesan Kesalahan Penilaian Direktori	Resolusi
Penilaian ini gagal beberapa pengujian pada kedua instance terkelola. Selidiki pengujian yang gagal dengan memilih setiap instans terkelola dan menyelesaikannya di direktori lokal Anda. Kemudian, buat penilaian baru.	Satu atau beberapa pengujian penilaian direktori gagal untuk AD yang dikelola sendiri. Tinjau informasi lebih Pesan kesalahan Uji Penilaian lanjut tentang kegagalan pengujian tertentu dan resolusinya.
Penilaian ini gagal karena Pengecualian Layanan Internal. Silakan coba lagi dengan membuat penilaian baru atau layanan kontak untuk pemecahan masalah.	Cobalah untuk membuat penilaian direktori baru. Jika Anda terus mengalami kesalahan ini, hubungi Dukungan .
Penilaian ini gagal karena tidak ada izin untuk melakukan tindakan seperti <code>ec2:CreateSecurityGroup</code> , <code>ec2:DeleteSecurityGroup</code> , <code>ec2:CreateNetworkInterface</code> , <code>ec2:DeleteNetworkInterface</code> , <code>ec2:DescribeSubnets</code> , dan <code>ec2:DescribeNetworkInterface</code> .	Untuk membuat penilaian direktori, Anda Akun AWS membutuhkan yang diperlukan Akun AWS izin .
Penilaian ini gagal karena tidak ada izin untuk melakukan tindakan seperti <code>ssm:GetConnectionStatus</code> , <code>ssm:GetCommandInvocation</code> , <code>ssm:ListCommands</code> , dan <code>ssm:SendCommand</code> .	Untuk membuat penilaian direktori, Anda memerlukan dua node Systems Manager dengan yang diperlukan Akun AWS izin .
Penilaian ini gagal karena Anda telah mencapai batas jumlah antarmuka jaringan	Untuk membuat penilaian direktori, Anda harus membuat antarmuka jaringan dan grup keamanan. Ada batasan jumlah

Pesan Kesalahan Penilaian Direktori	Resolusi
yang dapat Anda buat. Untuk informasi selengkapnya, lihat kuota Amazon VPC .	sumber daya VPC yang dapat Anda buat namun Anda dapat menyesuaikan beberapa batasan ini. Untuk informasi selengkapnya, lihat kuota Amazon VPC .
Penilaian ini gagal karena Anda telah mencapai batas jumlah grup keamanan yang dapat Anda buat, atau tetapkan ke sebuah instans. Untuk informasi selengkapnya, lihat kuota Amazon VPC .	Untuk membuat penilaian direktori, Anda harus membuat antarmuka jaringan dan grup keamanan. Ada batasan jumlah sumber daya VPC yang dapat Anda buat namun Anda dapat menyesuaikan beberapa batasan ini. Untuk informasi selengkapnya, lihat kuota Amazon VPC .
Penilaian ini gagal. Tidak dapat terhubung ke instans pelanggan dari AWS Systems Manager.	Untuk membuat penilaian direktori, Anda memerlukan dua AWS Systems Manager node yang memiliki status terhubung. Lihat Pemecahan Masalah Agen SSM .
Penilaian ini gagal beberapa tes kritis. Selidiki pengujian yang gagal dengan memilih setiap instans terkelola dan selesaikan di direktori lokal Anda. Kemudian, buat penilaian baru.	Satu atau beberapa pengujian penilaian direktori gagal untuk AD yang dikelola sendiri. Tinjau Pesan kesalahan Uji Penilaian untuk informasi lebih lanjut.

Pesan kesalahan Uji Penilaian

Tabel berikut menjelaskan pesan kesalahan yang dapat terjadi selama pengujian penilaian. Kesalahan ini menunjukkan masalah pemblokiran yang harus diselesaikan sebelum melanjutkan dengan pengaturan direktori hybrid.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Active Directory	testActiv eDirector	AD_CRITIC AL_SERVIC	Critical AD Services: [service_	Terjadi jika AD layanan yang diperlukan tidak	AD Layanan khusus yang diperlukan

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
ServicesUji	yServices	ES_NOT_RUNNING	list] not running on hostname.	berjalan di iklan yang dikelola sendiri.	harus berjalan di iklan yang dikelola sendiri. Untuk informasi selengkapnya, lihat Layanan Direktori Aktif yang Diperlukan .
Active Directory ServicesUji	testActiveDirectoryServices	DOMAIN_CONTROLLER_NOT_FOUND	No domain controllers found for testActiveDirectoryServices.	Occurs if your self-managed AD domain controllers could not be both detected and queried during AD service validation.	Pastikan pengontrol domain AD yang dikelola sendiri beroperasi dan dapat dihubungi. Verifikasi konektivitas dan DNS resolusi jaringan untuk pengontrol domain AD yang dikelola sendiri.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
ADUji Kebijakan Kata Sandi	testPassw ordPolici es	PASSWORD_ POLICY_VI OLATIONS	<i>ErrorMess age</i>	Terjadi jika kebijakan kata sandi AD yang dikelola sendiri tidak memenuhi persyaratan Microsoft AD AWS Terkelola.	Kebijakan kata sandi AD yang dikelola sendiri harus memenuhi persyaratan kata sandi Microsoft AD AWS Terkelola. Untuk selengkapnya, lihat Memahami kebijakan kata sandi Microsoft AD yang AWS Dikelola .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
AWS Tes Ada Pengguna Admin	testAwsAdminUserExist	ADMINISTRATOR_ACCOUNT_MISSING	AWS Admin user not found or invalid.	Terjadi jika pengguna administrator direktori hibrid tidak ada di AWS Cadangan OU pada iklan yang dikelola sendiri.	Pastikan pengguna administrator direktori hibrid ada di AWS Cadangan OU pada iklan yang dikelola sendiri. Jika pengguna hilang, verifikasi akun telah dibuat dengan benar selama proses pengaturan direktori hybrid. Memperbarui direktori hybrid. Jika status direktori hybrid Anda tidak dapat dioperasikan, hubungi. Dukungan

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
AWS SPN Test Pengguna Admin	testNoSpnOnAwsAdminAccount	SPN_FOUND_ON_AWS_AD_MIN	Found <i>spnCount</i> Service Principal Names (SPNs) set on AWS admin user <i>Username</i> . Please remove all SPNs from this account.	Terjadi jika pengguna administrator direktori hibrid memiliki SPNs konfigurasi apa pun pada AD yang dikelola sendiri.	Hapus semua Nama Utama Layanan (SPNs) dari akun pengguna administrator direktori AWS hibrid. Pengguna administrator direktori hybrid tidak boleh memiliki SPNs konfigurasi apa pun karena mereka dapat mengganggu otentikasi direktori hybrid.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
AWS Pengontrol Domain Bukan Tes FSMO Pemilik	testAwsDomainNotFsmoOwner	AWS_DC_HOST_LDS_FSMO_ROLE	AWS Domain Controller owns FSMO roles: <i>rolesList</i> . Please remove these roles.	Terjadi jika Anda telah mentransfer FSMO peran (PDC Emulator, RID Master, atau Infrastructure Master) dari AD yang dikelola sendiri ke pengontrol domain direktori hibrid.	Transfer semua FSMO peran (PDC Emulator, RID Master, Infrastructure Master) kembali ke pengontrol domain AD yang dikelola sendiri sebelum melanjutkan. Untuk informasi selengkapnya, lihat Microsoft dokumentasi tentang mentransfer FSMO peran .
AWS Tes Keanggotaan Grup Cadangan	testValidateAwsReservedGroupMembership	AWS_RESERVED_OU_NOT_FOUND	AWS Reserved OU not found.	Terjadi jika AWS Cadangan OU pada iklan yang dikelola sendiri tidak ada.	AWS Cadangan OU harus ada di AD yang dikelola sendiri untuk memvalidasi keanggotaan grup. Hubungi Dukungan .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
AWS Tes Keanggotaan Grup Cadangan	testValidateAwsReservedGroupMembership	GROUP_MEMBERSHIP_MISMATCH	AWS Reserved OU Group [GroupNameA]: Missing User(s) [Object1], [Object2] and Extra user(s) [Object3].	Terjadi jika grup dalam AWS Cadangan OU pada iklan yang dikelola sendiri berisi pengguna yang tidak sah.	Hapus pengguna yang tidak sah dari OU grup AWS Cadangan pada iklan yang dikelola sendiri.
AWS OU ACLs Tes Cadangan	testReservedOuAclsPermissions	RESERVED_OU_NON_COMPLIANT_ACL	AWS Reserved OU ACLs permissions are invalid.	Terjadi jika AWS Cadangan OU ACLs pada iklan yang dikelola sendiri tidak memberlakukan izin hanya-baca untuk entitas non-#-AWS dan tidak mencegah akses tidak sah ke sumber daya yang dikelola. AWS	Tinjau dan perbaiki izin pada AWS Cadangan OU ACLs pada iklan yang dikelola sendiri. Pastikan bahwa AWS non-entitas hanya memiliki izin baca (ListChildren, ReadProperty, ListObjectReadControl, GenericRead, Synchronize) dan hapus izin yang berlebihan.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
AWS Tes OU GPO Asosiasi Cadangan	testReservedOuGPOs	AWS_RESERVED_OU_NO_RESERVE_D_GPO_FOUL	Found non-AWS GPOs attached to the AWS Reserved OU: AWS Reserved OU (<i>count</i> unauthorized). Allowed GPOs: [<i>allowedAwsGpos</i>]. Domain Controllers OU (<i>count</i> unauthorized). Allowed GPOs: [<i>allowedDcGpos</i>]. Please, remove extra GPOs from the AWS Reserved OU.	Terjadi jika Pengontrol AWS Cadangan OU dan Domain OU pada iklan yang dikelola sendiri ditautkan ke yang tidak sah. GPOs	(Hanya Objek Kebijakan Grup AWS terkelola (GPOs) yang dapat ditautkan ke iniOUs. Hapus semua yang tidak sah yang GPOs ditautkan ke Pengontrol AWS Cadangan OU dan Domain OU pada iklan yang dikelola sendiri.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
AWS Tes OU Sumber Daya Cadangan	testAwsRe servedOUR esources	AWS_RESER VED_OU_NO T_FOUND	The AWS Reserved OU does not exist. Please contact AWS Support.	Terjadi jika AWS Cadangan OU tidak ada di AD yang dikelola sendiri yang diperlukan untuk fungsiona litas direktori Microsoft AD AWS Terkelola.	AWS Reserved OU harus dibuat secara otomatis selama pengaturan direktori hybrid dan tidak boleh dihapus. Jika kesalahan ini berlanjut , hubungi Dukungan .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
AWS Tes OU Sumber Daya Cadangan	testAwsReservedOUResources	AWS_RESERVED_OU_RESOURCES_MISMATCH	The following required resources are missing from AWS Reserved OU - Objects: <i>missing objects</i> , GPOs: <i>missing GPOs</i> . The following resources should not exist but were found in AWS Reserved OU: Objects: <i>unexpected objects</i> , GPOs: <i>unexpected GPOs</i>	Terjadi jika AWS Cadangan yang OU dibuat pada AD yang dikelola sendiri tidak berisi objek yang diperlukan dan GPOs untuk operasi direktori hibrid yang tepat.	Pastikan tidak ada yang mengedit AWS ReservedOU. Itu harus berisi sumber daya yang AWS dikelola yang diperlukan. Hapus objek yang tidak sah atauGPOs, dan hubungi Dukungan jika sumber daya yang diperlukan hilang.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
AWS OUTes Cadangan	testClean AwsReservedOU	AWS_RESERVED_RESOURCES_STILL_EXISTS	AWS Reserved OU or AWS Reserved GPO still exists, please delete.	Terjadi jika sumber daya AWS Cadangan yang ditemukan di AD yang dikelola sendiri dari penyiapan direktori hibrid sebelumnya masih ada.	Hapus direktori hybrid gagal yang ada dari konsol. Kemudian hapus semua yang AWS Dicadangkan OU dan terkait GPOs dari iklan yang dikelola sendiri sebelum melanjutkan.
BridgeheadTes Konteks Penamaan	testBridgeheadNamingContext	NAMING_CONTEXT_INCONSISTENT	<i>failureDetails</i>	Terjadi jika replikasi AD yang dikelola sendiri antar situs yang menggunakan Bridgehead tidak berfungsi seperti yang diharapkan. Ini juga dapat terjadi jika konteks penamaan tidak disinkronkan antar situs.	bridgeheadSitus iklan yang dikelola sendiri harus berhasil. Anda dapat mendiagnosis lebih lanjut dengan: repadmin / bridgeheadads / verbose Atasi masalah dari penilaian itu sebelum melanjutkan.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Tes Domain Anak	testChildDomain	CHILD_DOMAIN_NOT_SUPPORTED	Child Domains are not supported for Hybrid Directory.	Terjadi jika hutan AD yang dikelola sendiri berisi domain anak, yang tidak didukung dengan direktori AD AWS Microsoft Terkelola.	AWS Direktori Microsoft AD yang dikelola tidak mendukung domain anak. Anda harus menggunakan hutan domain tunggal untuk iklan yang dikelola sendiri. Untuk informasi selengkapnya, lihat Microsoft Active Directory persyaratan domain .
DcDiagUji	testDcDiag	DCDIAG_TEST_FAILED	DCDiag test failed due to issue from [formattedFailedTests].	Terjadi jika ada Microsoft DCDiag pengujian yang gagal pada AD yang dikelola sendiri.	AWS digunakan DCDiag untuk menguji AD yang dikelola sendiri. Jika ada kesalahan, Anda tidak dapat membuat direktori hybrid. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
DNSTes Pertandin gan IP	testDnsIp Match	DNS_IP_MI SMATCH	DNS IP address does not match expected IP addresses.	Terjadi jika alamat DNS IP yang disediakan dari AD yang dikelola sendiri tidak cocok dengan alamat DNS IP pada pengontrol domain AD yang dikelola sendiri yang diaktifkan. AWS Systems Manager	Berikan alamat DNS IP yang benar.
DNSUji Pencocoka n Nama	testDnsNa meMatch	DOMAIN_DN S_NAME_MI SMATCH	DNS name does not match expected domain name.	Terjadi jika DNS nama yang diberikan untuk iklan yang dikelola sendiri tidak cocok dengan DNS nama pada pengontrol domain AD yang dikelola sendiri yang diaktifkan. AWS Systems Manager	Berikan DNS nama yang benar.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
DNSTes Rekaman	testDnsRe cords	DNS_REC ORD_MISSING	Unable to resolve the following DNS queries: <i>[missingRecordsString]</i> .	Terjadi jika Windows DNS catatan tidak disetel untuk tipe ANS,SOA,, SRV dan dapat ditanyakan.	DNSCatatan untuk Address (A), Namespace (NS), State of Authority (SOA), dan Service Record (SRV) harus disetel dan dapat ditanyakan. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Uji Tingkat Fungsional Hutan Domain	testDomainForestFunctionalLevel	UNSUPPORTED_FUNCTIONAL_LEVEL	Detected unsupported domain functional level: <i>DomainFunctionalLevel</i> , we require minimum of <i>MinimumDomainMode</i> . Detected unsupported forest functional level: <i>ForestFunctionalLevel</i> , we require minimum of <i>MinimumForestMode</i> .	Terjadi jika domain AD yang dikelola sendiri dan tingkat fungsional hutan Anda tidak memenuhi persyaratan minimum.	AD yang dikelola sendiri harus menggunakan Windows 2012 R2 atau tingkat 2016 fungsional. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Tes Kesehatan Domain	testOnPremDcNumber	DC_NUMBER_BELOW_LIMIT	On-Prem DC count is lower than required number. DC count is <i>NumberOfDc</i> , AWS required number is <i>DcMinimum</i> .	Terjadi jika AD yang dikelola sendiri tidak memiliki jumlah pengontrol domain minimum yang diperlukan.	Pastikan AD yang dikelola sendiri memiliki setidaknya dua pengontrol domain yang diaktifkan. AWS Systems Manager Untuk informasi selengkapnya, lihat Microsoft Active Directory persyaratan domain .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Uji Domain yang Ada	testDomainAlreadyJoined	DOMAIN_ALREADY_JOINED	Instance is already joined to a domain.	Terjadi jika domain AD yang dikelola sendiri sudah bergabung dengan direktori hybrid yang ada.	Domain AD yang dikelola sendiri sudah bergabung dengan direktori hybrid yang ada. Setiap domain AD yang dikelola sendiri yang digabungkan dengan direktori hybrid harus unik. Buat domain AD baru yang dikelola sendiri atau hapus dari konfigurasi direktori hybrid tempat mereka bergabung.

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
FSMO Uji Konektivitas	testFsmoConnectivity	FSMO_ROLE _HOLDER_NOT_ROUTABLE	(PDC Emulator Ip: 1.1.1.1, RID Master Ip: 1.1.1.1) is not in routable ranges: [2.2.0.0/16, 3.3.0.0/16, 4.4.0.0/16, 5.5.0.0/16, 6.6.0.0/16].	Terjadi jika FSMO peran, PDC Emulator, and/or RID Master IPs pada iklan yang dikelola sendiri tidak dapat dirutekan.	Pengontrol Domain Utama (PDC) harus dapat dirutekan setiap saat. Secara khusus, PDC Emulator dan RID Master IPs dari AD yang dikelola sendiri. Untuk informasi selengkapnya, lihat Microsoft Active Directory persyaratan domain .
FSMO Uji Konektivitas	testFsmoConnectivity	FSMO_ROLE _MISSING	FSMO role(s): [<i>missingRolesString</i>] missing or DNS Record not found.	Terjadi jika pengontrol domain AD yang dikelola sendiri tidak dapat mengakses peran Anda FSMO.	Peran Fleksibel Single Master Operation (FSMO) Anda dalam AD yang dikelola sendiri harus terhubung ke pengontrol domain AD yang dikelola sendiri. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Tes Konflik IP	testIpConflict	IP_RANGE_CONFLICT	Conflicting IP address detected: <i>ipOverlaps</i>	Terjadi jika Rentang IP AD yang dikelola sendiri tumpang tindih dengan rentang AWS cadangan.	AD yang dikelola sendiri tidak dapat menggunakan rentang alamat IP yang tumpang tindih dengan rentang IP Cadangan AWS . Untuk informasi selengkapnya, lihat Microsoft Active Directory persyaratan domain .
KerberosUji	testKerberos	KERBEROS_AUTHENTICATION_FAILED	Unable to get kerberos TGT.	Terjadi jika tidak Kerberos dikonfigurasi dengan benar dan digunakan.	Kerberos harus diaktifkan pada iklan yang dikelola sendiri. Untuk informasi selengkapnya, lihat Dokumentasi Microsoft .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
LDAP Uji Konektivitas	testLdapConnectivity	LDAP_TEST_FAILED	Unable to query LDAP with rootDSE call.	Terjadi jika LDAP tidak bekerja.	Protokol Akses Direktori Ringan (LDAP) harus diaktifkan dan berfungsi pada AD yang dikelola sendiri. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .
Tidak Baca Hanya Pengontrol Domain Untuk FSMO Pengujian	testNotReadOnlyForFsmo	FSMO_FOUND_ON_RODC	FSMO Role Found on RODC	Terjadi jika FSMO peran pengontrol domain AD yang dikelola sendiri adalah RODC.	Pengontrol domain untuk AD yang dikelola sendiri tidak boleh menggunakan peran Read-Only Domain Controller (RODC) Flexible Single Master Operation (FSMO). Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Baca Hanya Uji Replikasi Kata Sandi Pengontrol Domain	testRodcPasswordReplication	RODC_REPLICATION_PASSWORD_CONTROL_FAILED_FOR_GROUPS_STRING	ReadOnly Domain Controller password replication is not explicitly denied for following groups: [missingGroupsString].	Terjadi jika RODC memiliki izin untuk mereplikasi kata sandi Admin.	RODC untuk iklan yang dikelola sendiri harus secara eksplisit ditolak izinnya untuk mereplikasi kata sandi Admin. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .
Baca Hanya Uji Pengontrol Domain	testIsDCReadOnly	DC_READONLY_MODE	Provided Domain Controller is set to Read-Only mode.	Terjadi jika pengontrol domain AD yang dikelola sendiri dalam ReadOnlyDC mode.	AD yang dikelola sendiri harus berupa pengontrol domain baca-tulis. Untuk informasi selengkapnya tentang jenis pengontrol domain, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Uji Konektivitas Port Jarak Jauh	testPortConnectivity	PORT_TEST_FAILED	Connection to <i>TargetDestination</i> failed for TCP ports [<i>failed TCP ports</i>]. UDP ports [<i>failed UDP ports</i>].	Terjadi jika port yang diperlukan pada AWS subnet Anda dan pengontrol domain AD yang dikelola sendiri tidak terbuka.	Pastikan semua port yang diperlukan terbuka antara AWS subnet Anda dan AD yang dikelola sendiri. Untuk informasi selengkapnya, lihat Persyaratan port jaringan .
Uji Replikasi	testReplication	REPLICATION_FAILED	Replication failed for [<i>failedDSASString</i>].	Terjadi jika replikasi pengontrol domain AD yang dikelola sendiri gagal.	Status replikasi pengontrol domain AD yang dikelola sendiri harus berhasil. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .
SMBV1Uji	testSMBV1	INSECURE_SETTING_SMB	SMBv1 is enabled on the system.	Terjadi jika AD yang dikelola sendiri saat ini digunakan SMBv1 untuk otentikasi.	SMBv1 diketahui tidak aman dan harus dinonaktifkan pada iklan yang dikelola sendiri. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
SSMUji Izin Pengguna	testSSMUserPermissions	INSUFFICIENT_PERMISSIONS	Systems Manager user does not have required elevated privileges.	Terjadi jika Windows pengguna yang digunakan oleh SSM memiliki hak istimewa yang tidak mencukupi.	Anda memerlukan izin Windows Administrator untuk agen Manajer AWS Sistem (SSM) di AD yang dikelola sendiri. Untuk informasi selengkapnya, lihat Akun AWS izin .
SysvolUji Replikasi	testSysvolReplication	DFSR_FAILURE_DETECTED	Failed DFSR event logs: <i>failedLog sString</i> .	Terjadi jika AD yang dikelola sendiri tidak memiliki metode sysvol replikasi (DFSR) yang benar, dan jika ada yang DCs gagal selama peristiwa DFSR replikasi.	Metode sysvol replikasi AD yang dikelola sendiri (DFSR) harus berhasil. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
GPOTes Tingkat Atas	testTopLevelEnforcedGPO	TOP_LEVEL_ENFORCED_GPO_FOUND	GroupPolicy cannot be set to Enforced at the Domain Root, Found GPOs: [<i>GposEnforced</i>] set as Enforced.	Terjadi jika AD yang dikelola sendiri memiliki Level Teratas yang GPOs ditetapkan sebagai Ditegakkan.	Pastikan domain AD yang dikelola sendiri Objek kebijakan grup Tingkat Atas (GPO) tidak disetel ke Ditegakkan. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .
Tes Jenis Kepercayaan	testTrustTypes	INVALID_TRUST_TYPE	Invalid trust types detected: [<i>InvalidTrustString</i>], only Uplevel (Microsoft AD) is currently supported.	Terjadi jika iklan yang dikelola sendiri memiliki jenis kepercayaan yang tidak didukung.	Uplevel adalah satu-satunya jenis kepercayaan yang didukung dengan direktori hybrid. AD yang dikelola sendiri tidak dapat memiliki jenis kepercayaan berikut: DCE, MIT, Downlevel. Untuk informasi selengkapnya tentang jenis kepercayaan, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode kesalahan	Pesan kesalahan	Deskripsi	Resolusi
Uji Pengontrol Domain yang Valid	testValidDC	COMPUTER_NOT_DC	Provided instance is not a domain controller.	Terjadi jika instans AD yang dikelola sendiri yang disediakan bukan pengontrol domain atau jika mereka sudah menjadi bagian dari direktori hybrid lain.	Menyediakan pengontrol domain AD yang dikelola sendiri yang unik untuk direktori hybrid ini. Coba lagi dengan direktori baru. Pastikan Anda telah menghapus direktori hybrid yang gagal dan semua yang ada AWS OU di AD yang dikelola sendiri.

Pesan peringatan Tes Penilaian

Tabel berikut menjelaskan pesan peringatan yang dapat terjadi selama tes penilaian. Peringatan ini mewakili rekomendasi untuk konfigurasi optimal tetapi tidak mencegah pengaturan direktori hybrid.

Nama uji	Nama pendek	Kode peringatan	Pesan peringatan	Deskripsi	Resolusi
Tes Kesehatan Domain	testDisabledStaleUserNumber	STALE_USERS_FOUND	<i>StaleUser Count</i> users were found to be stale, they have not logged	Terjadi jika ada akun pengguna di AD yang dikelola sendiri yang belum masuk untuk	Bersihkan akun pengguna basi.

Nama uji	Nama pendek	Kode peringatan	Pesan peringatan	Deskripsi	Resolusi
			in for <i>StaleThresholds</i> days.	waktu yang lama dan dapat dianggap basi atau tidak aktif.	
Uji Sumber Waktu Pengontrol Domain	testDCTimeSource	DC_BAD_TIME_SOURCE	Time sources not properly configured for PDC, should use an authoritative source. Time sources not properly configured for <i>dcHostName</i> , should use PDC as source	Terjadi jika AD yang dikelola sendiri memiliki pengaturan sumber waktu yang benar dan tidak ada kemiringan waktu yang besar jika dibandingkan dengan sumber waktu. AWS	Server waktu pengontrol domain utama Anda (PDC) diarahkan ke 169.254.169.123. Pengontrol domain non-primer Anda harus diarahkan ke PDC sebagai sumbernya. Untuk informasi selengkapnya, lihat Menjaga waktu dengan Amazon Time Sync Service .

Nama uji	Nama pendek	Kode peringatan	Pesan peringatan	Deskripsi	Resolusi
Uji Ruang Bebas	testFreeSpace	DISK_SPACE_EXCEEDED	Supported service max capacity of 7 GB exceeded; SysVol + NTDS is currently using: 24 GB)	Terjadi jika Gabungan AD yang dikelola sendiri NTDS dan Sysvol penggunaan di atas kuota yang didukung.	AD yang dikelola sendiri harus memiliki ruang disk 24 GB untuk direktori hybrid.
FSMO Roles Uji	testFSMORoles	FSMO_ROLE_TEST_FAILED	PDC Emulator (<i>dc1.example.com</i>) is not among the provided domain controllers. RID Master (<i>dc1.example.com</i>) is not among the provided domain controllers.	Terjadi jika peran FSMO (PDC Emulator dan RID Master) tidak termasuk di antara dua pengontrol domain yang disediakan saat Anda membuat direktori hybrid.	Direktori hybrid Anda harus memiliki peran FSMO (PDC Emulator dan RID Master) di antara dua pengontrol domain yang Anda berikan saat Anda membuat direktori hybrid. Untuk informasi selengkapnya, lihat Cara melihat dan mentransfer FSMO peran .

Nama uji	Nama pendek	Kode peringatan	Pesan peringatan	Deskripsi	Resolusi
SSPUji saluran S	testSchannelSSP	TLS_1_2_NOT_ENABLED	Disabled protocol <i>DisabledProtocol</i> is still enabled.	Terjadi jika AD yang dikelola sendiri tidak menggunakan TLS1.2 dan AES256 enkripsi.	AD yang dikelola sendiri harus digunakan TLS 1.2 dan AES256 untuk direktori hybrid.
Uji Korupsi Disk	testDiskCorruption	DISK_CORRUPTION	Disk corruption detected on <i>Drive</i> .	Terjadi jika ada kerusakan disk pada iklan yang dikelola sendiri.	Disk AD yang dikelola sendiri tidak boleh rusak.
Domain Controller Uji Spesifikasi	testDcSpecs	INSUFFICIENT_RESOURCES	<i>numAvailableCores</i> cores detected when <i>requiredCores</i> cores recommended. <i>gbAvailableRam</i> GB ram detected when <i>requiredRam</i> GB recommended.	Terjadi jika pengontrol domain AD yang dikelola sendiri tidak memenuhi spesifikasi yang diperlukan.	Pengontrol domain AD yang dikelola sendiri harus memiliki setidaknya 7 GB RAM dan 2 core CPU untuk direktori hybrid.

Nama uji	Nama pendek	Kode peringatan	Pesan peringatan	Deskripsi	Resolusi
DIIUji Plugin Tingkat Server	testServerLevelPluginDll	SERVER_LEVEL_PLUGIN_DLL_IS_SET	ServerLevelPluginDll registry configuration is not permitted.	Terjadi jika ServerLevelPluginDll disetel pada pengontrol domain AD yang dikelola sendiri.	Pengontrol domain AD yang dikelola sendiri seharusnya ServerLevelPluginDll tidak dikonfigurasi.
Izinkan Tes NT4 Crypto	testAllowNT4Crypto	NT4_CRYPTO_NOT_ALLOWED	Registry key AllowNt4Crypto is not allowed.	Terjadi jika AD yang dikelola sendiri memungkinkan NT4 Kriptografi.	AD yang dikelola sendiri tidak boleh menggunakan NT4 Kriptografi. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi.
Tes Pengguna Admin Yatim	testOrphanedAdminUsers	ORPHANED_ADMIN_USERS_FOUND	<i>OrphanedUsersCount</i> Orphaned Admin Users Found: [<i>OrphanedUserNames</i>].	Terjadi jika pengguna admin yatim piatu ada di iklan yang dikelola sendiri.	Hapus pengguna yatim piatu di iklan yang dikelola sendiri sebelum melanjutkan.

Nama uji	Nama pendek	Kode peringatan	Pesan peringatan	Deskripsi	Resolusi
Tes Hitungan Pengguna Istimewa	testPrivilegedUserCount	DOMAIN_ADMIN_COUNT_EXCEEDED	Number of Domain Admins (<i>daCount</i>) exceeded allowance of (<i>allowedDomainAdminCount</i>).	Terjadi jika jumlah total Admin Bawaan, Admin Domain, dan Admin Perusahaan pada iklan yang dikelola sendiri lebih besar dari 5.	Lingkungan iklan yang dikelola sendiri tidak boleh memiliki beberapa akun istimewa. Anda harus menghapus akun admin yang berlebihan sebelum melanjutkan.
Tes Hitungan Pengguna Istimewa	testPrivilegedUserCount	ENTERPRISE_ADMIN_COUNT_EXCEEDED	Number of Enterprise Admins (<i>eaCount</i>) exceeded allowance of (<i>allowedEnterpriseAdminCount</i>).	Terjadi jika jumlah total Admin Bawaan, Admin Domain, dan Admin Perusahaan pada iklan yang dikelola sendiri lebih besar dari 5.	Lingkungan iklan yang dikelola sendiri tidak boleh memiliki beberapa akun istimewa. Anda harus menghapus akun admin yang berlebihan sebelum melanjutkan.

Nama uji	Nama pendek	Kode peringatan	Pesan peringatan	Deskripsi	Resolusi
Tes Hitungan Pengguna Istimewa	testPrivilegedUserCount	BUILTIN_ADMIN_COUNT_EXCEEDED	Number of Built-in Admins (<i>baCount</i>) exceeded allowance of (<i>allowedAdminCount</i>).	Terjadi jika jumlah total Admin Bawaan, Admin Domain, dan Admin Perusahaan pada iklan yang dikelola sendiri lebih besar dari 5.	Lingkungan iklan yang dikelola sendiri tidak boleh memiliki beberapa akun istimewa. Anda harus menghapus akun admin yang berlebihan sebelum melanjutkan.
NTLMUji	testNTLM	INSECURE_SETTING_NTLM	NTLMv1 is enabled.	Terjadi jika NTLMv1 diaktifkan untuk otentikasi pada iklan yang dikelola sendiri.	NT LAN Managerversi 1 (NTLMv1) memiliki kerentanan keamanan yang diketahui dan tidak boleh digunakan. NTLMv1Non aktifkan iklan yang dikelola sendiri. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Nama uji	Nama pendek	Kode peringatan	Pesan peringatan	Deskripsi	Resolusi
Tes Seumur Hidup Tombstone	testTombstoneLifetime	TOMBSTONE _LIFETIME _ABOVE_LIFETIME MIT	Tombstone Lifetime is too long. DC Tombstone Lifetime is <i>Tombstone LifeTime</i> , AWS suggested number is <i>Tombstone Maximum</i> days.	Terjadi jika masa pakai Tombstone pada AD yang dikelola sendiri lebih dari 180 hari.	Masa pakai Tombstone adalah jumlah hari sebelum objek yang dihapus dihapus. AD Nilai seumur hidup Tombstone untuk AD yang dikelola sendiri harus 180 hari atau kurang. Untuk informasi lebih lanjut, lihat Microsoft dokumentasi .

Memulai dengan Microsoft AD yang AWS Dikelola

AWS Microsoft AD yang dikelola sepenuhnya menciptakan yang dikelola sepenuhnya, Microsoft Active Directory di AWS Cloud dan didukung oleh Windows Server 2019 dan beroperasi pada tingkat fungsional Hutan dan Domain R2 2012. Saat Anda membuat direktori dengan Microsoft AD AWS Terkelola, Directory Service buat dua pengontrol domain dan tambahkan layanan DNS atas nama Anda. Pengontrol domain dibuat dalam subnet yang berbeda di VPC Amazon, redundansi ini membantu memastikan bahwa direktori Anda tetap dapat diakses bahkan jika terjadi kegagalan. Jika Anda membutuhkan lebih banyak pengendali domain, Anda dapat menambahkannya nanti. Untuk informasi selengkapnya, lihat [Menerapkan pengontrol domain tambahan untuk AWS Microsoft AD yang Dikelola](#).

Untuk demo dan ikhtisar Microsoft AD yang AWS Dikelola, lihat YouTube video berikut.

[AWS Demo dan Ikhtisar Microsoft AD Terkelola](#)

Topik

- [Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS](#)
- [AWS IAM Identity Center prasyarat](#)
- [Prasyarat autentikasi multi-faktor](#)
- [Membuat Microsoft AD yang AWS Dikelola](#)
- [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#)
- [AWS Akun Administrator Microsoft AD yang dikelola dan izin grup](#)

Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS

Untuk membuat Direktori Aktif Microsoft AD AWS Terkelola, Anda memerlukan VPC Amazon dengan yang berikut ini:

- Setidaknya dua subnet. Masing-masing subnet harus berada di Availability Zone yang berbeda dan harus dari jenis jaringan yang sama.

Anda dapat menggunakan IPv6 untuk VPC Anda. Untuk informasi selengkapnya, lihat [IPv6 dukungan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.

- VPC harus memiliki penghunian perangkat keras default.
- Anda tidak dapat membuat iklan Microsoft AWS Terkelola di VPC menggunakan alamat di ruang alamat 198.18.0.0/15.

Jika Anda perlu mengintegrasikan domain Microsoft AD AWS Terkelola dengan domain Active Directory lokal yang ada, Anda harus memiliki tingkat fungsional Forest dan Domain untuk domain lokal yang disetel ke Windows Server 2003 atau yang lebih tinggi.

Directory Service menggunakan dua struktur VPC. Instans EC2 yang membentuk direktori Anda berjalan di luar AWS akun Anda, dan dikelola oleh AWS Mereka memiliki dua adaptor jaringan, ETH0 dan ETH1. ETH0 adalah adaptor pengelola, dan berada di luar akun Anda. ETH1 dibuat dalam akun Anda.

Rentang IP manajemen ETH0 jaringan direktori Anda adalah 198.18.0.0/15.

Untuk tutorial tentang cara membuat AWS lingkungan dan AWS Dikelola Microsoft AD, lihat [AWS Tutorial lab uji Microsoft AD yang dikelola](#).

AWS IAM Identity Center prasyarat

Jika Anda berencana untuk menggunakan Pusat Identitas IAM dengan Microsoft AD yang AWS Dikelola, Anda perlu memastikan bahwa berikut ini benar:

- Direktori Microsoft AD AWS Terkelola Anda disiapkan di akun manajemen AWS organisasi Anda.
- Instance Pusat Identitas IAM Anda berada di Wilayah yang sama tempat direktori Microsoft AD AWS Terkelola Anda disiapkan.

Untuk informasi selengkapnya, lihat [prasyarat Pusat Identitas IAM](#) di Panduan Pengguna AWS IAM Identity Center

Prasyarat autentikasi multi-faktor

Untuk mendukung autentikasi multi-faktor dengan direktori AWS Microsoft AD Terkelola, Anda harus mengonfigurasi server [Layanan Pengguna Dial-In \(RADIUS\) Autentikasi Jarak Jauh](#) (RADIUS) lokal atau berbasis Internet dengan cara berikut agar dapat menerima permintaan dari direktori Microsoft AD yang Dikelola di AWS

1. Di server RADIUS Anda, buat dua klien RADIUS untuk mewakili kedua pengontrol domain Microsoft AD AWS Terkelola (DCs) di AWS. Anda harus mengkonfigurasi kedua klien menggunakan parameter umum berikut (server RADIUS Anda dapat bervariasi):
 - Alamat (DNS atau IP): Ini adalah alamat DNS untuk salah satu iklan AWS Microsoft yang Dikelola. DCs Kedua alamat DNS dapat ditemukan di AWS Directory Service Console pada halaman Detail direktori Microsoft AD yang AWS dikelola tempat Anda berencana untuk menggunakan MFA. Alamat DNS yang ditampilkan mewakili alamat IP untuk kedua AD Microsoft AWS Terkelola DCs yang digunakan oleh AWS.

Note

Jika server RADIUS mendukung alamat DNS, Anda harus membuat hanya satu konfigurasi klien RADIUS. Jika tidak, Anda harus membuat satu konfigurasi klien RADIUS untuk setiap Microsoft AD DC yang AWS Dikelola.

- Angka port: Mengkonfigurasi nomor port yang server RADIUS Anda menerima koneksi klien RADIUS. Port RADIUS standar adalah 1812.

- **Rahasia bersama:** Ketik atau buat rahasia bersama yang server RADIUS akan gunakan untuk terhubung dengan klien RADIUS.
 - **Protokol:** Anda mungkin perlu mengonfigurasi protokol otentikasi antara Microsoft AD yang AWS Dikelola DCs dan server RADIUS. Protokol yang didukung adalah PAP, CHAP MS-CHAPv1, dan MS-. CHAPv2 MS- CHAPv2 direkomendasikan karena memberikan keamanan terkuat dari tiga opsi.
 - **Nama aplikasi:** Ini mungkin opsional di beberapa server RADIUS dan biasanya mengidentifikasi aplikasi dalam pesan atau laporan.
2. Konfigurasikan jaringan yang ada untuk mengizinkan lalu lintas masuk dari klien RADIUS (Alamat DCs DNS Microsoft AD yang AWS dikelola, lihat Langkah 1) ke port server RADIUS Anda.
 3. Tambahkan aturan ke grup keamanan Amazon EC2 di domain AWS Microsoft AD Terkelola yang memungkinkan lalu lintas masuk dari alamat DNS server RADIUS dan nomor port yang ditentukan sebelumnya. Untuk informasi selengkapnya, lihat [Menambahkan aturan ke sebuah grup keamanan](#) di Panduan Pengguna EC2.

Untuk informasi selengkapnya tentang menggunakan Microsoft AD yang AWS Dikelola dengan MFA, lihat. [Mengaktifkan otentikasi multi-faktor untuk Microsoft AD yang Dikelola AWS](#)

Membuat Microsoft AD yang AWS Dikelola

Untuk membuat Direktori Aktif Microsoft AD AWS Terkelola baru, lakukan langkah-langkah berikut. Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikan prasyarat yang diidentifikasi dalam [Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS](#).

Untuk membuat iklan Microsoft yang AWS Dikelola

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori, lalu pilih Atur direktori.
2. Di halaman Pilih jenis direktori, pilih Microsoft AD yang Dikelola AWS , lalu pilih Selanjutnya.
3. Di halaman Masukkan informasi direktori, berikan informasi berikut:

Edisi

Pilih dari Edisi Standar atau Edisi Perusahaan dari Microsoft AD yang AWS Dikelola. Untuk informasi selengkapnya tentang edisi, lihat [Directory Service AWS untuk Microsoft Active Directory](#).

Nama DNS direktori

Nama berkualifikasi penuh untuk direktori, seperti `corp.example.com`.

Note

Jika Anda berencana menggunakan Amazon Route 53 untuk DNS, nama domain Microsoft AD yang AWS Dikelola harus berbeda dengan nama domain Route 53 Anda. Masalah resolusi DNS dapat terjadi jika Route 53 dan Microsoft AD yang AWS dikelola berbagi nama domain yang sama.

Direktori nama NetBIOS

Nama singkat untuk direktori, seperti `CORP`.

Deskripsi direktori

Deskripsi opsional untuk direktori. Deskripsi ini dapat diubah setelah membuat iklan Microsoft AWS Terkelola Anda.

Kata sandi admin

Kata sandi administrator direktori. Proses pembuatan direktori menciptakan akun administrator dengan nama pengguna Admin dan kata sandi ini. Anda dapat mengubah kata sandi Admin setelah membuat iklan Microsoft AWS Terkelola.

Kata sandi tidak dapat menyertakan kata "admin."

Kata sandi administrator direktori peka akan huruf besar kecil dan harus terdiri dari 8 sampai 64 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:

- Huruf kecil (a-z)
- Huruf besar (A-Z)
- Angka (0-9)
- Karakter non-alfanumerik (~!@#\$%^&* _-+=`|()\{}[];:'"<>,.?/)

Konfirmasikan kata sandi

Ketik ulang kata sandi administrator.

(Optional) Manajemen pengguna dan grup

Untuk mengaktifkan AWS pengelolaan pengguna dan grup Microsoft AD Terkelola dari Konsol Manajemen AWS, pilih Kelola pengguna dan manajemen grup di Konsol Manajemen AWS. Untuk informasi selengkapnya tentang cara menggunakan manajemen pengguna dan grup, lihat [the section called “Kelola pengguna dan grup dengan konsol, CLI, atau PowerShell”](#).

4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.

VPC

Pilih VPC untuk direktori.

Jenis jaringan

Sistem pengalamatan Internet Protocol (IP) yang terkait dengan VPC dan subnet Anda.

Pilih blok CIDR yang terkait dengan VPC Anda yang ada. Sumber daya di subnet Anda dapat dikonfigurasi untuk IPv4 hanya menggunakan, IPv6 hanya, atau keduanya IPv4 dan IPv6 (dual-stack). Untuk informasi selengkapnya, lihat [Bandingkan IPv4 dan IPv6](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Subnet

Pilih subnet untuk pengontrol domain. Kedua subnet harus berada di Zona Ketersediaan yang berbeda.

5. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Membuat direktori membutuhkan waktu 20 sampai 40 menit. Setelah dibuat, nilai Status berubah ke Aktif.

Untuk informasi selengkapnya tentang apa yang dibuat dengan Microsoft AD yang AWS Dikelola, lihat berikut ini:

- [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#)
- [AWS Akun Administrator Microsoft AD yang dikelola dan izin grup](#)

Artikel blog AWS Keamanan Terkait

- [Cara mendelegasikan administrasi direktori Microsoft AD AWS Terkelola ke pengguna Active Directory lokal](#)
- [Cara mengonfigurasi kebijakan kata sandi yang lebih kuat untuk membantu memenuhi standar keamanan Anda dengan menggunakan Directory Service untuk Microsoft AD yang AWS Dikelola](#)
- [Cara meningkatkan redundansi dan kinerja Anda Directory Service untuk AWS Microsoft AD yang Dikelola dengan menambahkan pengontrol Domain](#)
- [Cara mengaktifkan penggunaan desktop jarak jauh dengan menerapkan manajer lisensi desktop Microsoft jarak jauh di Microsoft AD yang Dikelola AWS](#)
- [Cara mengakses iklan Microsoft yang Konsol Manajemen AWSAWS Dikelola dan kredensial lokal Anda](#)
- [Cara mengaktifkan autentikasi multi-faktor untuk AWS layanan dengan menggunakan Managed AWS Microsoft AD dan kredensial lokal](#)
- [Cara mudah masuk ke AWS layanan dengan menggunakan Active Directory lokal](#)

Apa yang dibuat dengan Microsoft AD yang AWS Dikelola

Saat Anda membuat Direktori Aktif dengan Microsoft AD yang AWS Dikelola, Directory Service lakukan tugas berikut atas nama Anda:

- Secara otomatis membuat dan mengasosiasikan antarmuka jaringan elastis (ENI) dengan masing-masing pengendali domain Anda. Masing-masing ENIs penting untuk konektivitas antara VPC dan pengontrol Directory Service domain Anda dan tidak boleh dihapus. Anda dapat mengidentifikasi semua antarmuka jaringan yang dicadangkan untuk digunakan Directory Service dengan deskripsi: "AWS menciptakan antarmuka jaringan untuk direktori-id direktori". Untuk informasi selengkapnya, lihat [Antarmuka Jaringan Elastis](#) di Panduan Pengguna Amazon EC2. Server DNS default dari Direktori Aktif Microsoft AD yang AWS Dikelola adalah server DNS VPC di Classless Inter-Domain Routing (CIDR) +2. Untuk informasi selengkapnya, lihat [Server DNS](#) Amazon di Panduan Pengguna Amazon VPC.

Note

Pengontrol domain diterapkan di dua Availability Zone di suatu wilayah secara default dan terhubung ke Amazon VPC (VPC) Anda. Pencadangan diambil secara otomatis sekali sehari, dan volume Amazon EBS (EBS) dienkripsi untuk memastikan bahwa data diamankan saat istirahat. Pengendali domain yang gagal secara otomatis diganti di

Availability Zone yang sama menggunakan alamat IP yang sama, dan pemulihan bencana penuh dapat dilakukan dengan menggunakan backup terbaru.

- Persediaan Direktori Aktif dalam VPC Anda menggunakan dua pengendali domain untuk toleransi kesalahan dan ketersediaan tinggi. Pengendali domain yang lebih dapat disediakan untuk ketahanan yang lebih tinggi dan performa setelah direktori telah berhasil dibuat dan [Aktif](#). Untuk informasi selengkapnya, lihat [Menerapkan pengontrol domain tambahan untuk AWS Microsoft AD yang Dikelola](#).

 Note

AWS tidak mengizinkan penginstalan agen pemantauan pada pengontrol domain Microsoft AD AWS Terkelola.

- Membuat [grup AWS Keamanan](#) `sg-1234567890abcdef0` yang menetapkan aturan jaringan untuk lalu lintas masuk dan keluar dari pengontrol domain Anda. Aturan keluar default mengizinkan semua lalu lintas ke semua IPv4 alamat. Aturan masuk default hanya mengizinkan lalu lintas melalui port yang diperlukan oleh Active Directory dari blok IPv4 CIDR utama yang terkait dengan hosting VPC untuk iklan Microsoft Terkelola AWS Anda. Untuk keamanan tambahan, ENIs yang dibuat tidak memiliki Elastic yang IPs melekat padanya dan Anda tidak memiliki izin untuk melampirkan IP Elastis ke IP tersebut ENIs. Oleh karena itu secara default, satu-satunya lalu lintas masuk yang dapat berkomunikasi dengan Microsoft AD yang AWS Dikelola adalah VPC lokal. Anda dapat mengubah aturan grup keamanan untuk mengizinkan sumber lalu lintas tambahan, misalnya dari peered lain VPCs atau CIDRs dapat dijangkau melalui VPN. Gunakan sangat hati-hati jika Anda mencoba untuk mengubah aturan-aturan ini karena mungkin dapat merusak kemampuan Anda untuk berkomunikasi dengan pengendali domain Anda. Untuk informasi selengkapnya, lihat [AWS Praktik terbaik Microsoft AD yang dikelola](#) dan [Meningkatkan konfigurasi keamanan jaringan Microsoft AD AWS Terkelola](#).

Anda dapat menggunakan [daftar awalan](#) untuk mengelola blok CIDR Anda dalam aturan grup keamanan. Daftar awalan memudahkan untuk mengelola dan mengkonfigurasi grup keamanan dan tabel rute. Anda dapat mengkonsolidasikan beberapa blok CIDR dengan port dan protokol yang sama untuk menskalakan lalu lintas jaringan Anda.

- Dalam suatu Windows lingkungan, klien sering berkomunikasi melalui [Server Message Block \(SMB\)](#) atau port 445. Protokol ini memfasilitasi berbagai tindakan seperti berbagi file dan printer dan komunikasi jaringan umum. Anda akan melihat lalu lintas klien pada port 445 ke antarmuka manajemen pengontrol domain AWS Microsoft AD Terkelola Anda.

Lalu lintas ini terjadi karena klien SMB mengandalkan resolusi nama DNS (port 53) dan NetBIOS (port 138) untuk menemukan sumber daya domain AWS Microsoft AD Terkelola Anda. Klien ini diarahkan ke antarmuka yang tersedia pada pengontrol domain saat menemukan sumber daya domain. Perilaku ini diharapkan dan sering terjadi di lingkungan dengan beberapa adaptor jaringan dan di mana [SMB Multichannel](#) memungkinkan klien untuk membuat koneksi di berbagai antarmuka untuk meningkatkan kinerja dan redundansi.

Aturan grup AWS Keamanan berikut dibuat secara default:

Aturan Masuk

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
ICMP	N/A	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	Ping	LDAP Tetap Hidup, DFS
TCP & UDP	53	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan
TCP & UDP	88	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	389	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	LDAP	Direktori , replikasi , kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP & UDP	445	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	SMB / CIFS	Replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
TCP & UDP	464	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentikasi komputer, kepercayaan
TCP	135	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	Replikasi	RPC, EPM
TCP	636	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	LDAP SSL	Direktori , replikasi , pengguna dan autentikasi komputer, kebijakan grup, kepercayaan

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	1024 - 65535	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	RPC	Replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	LDAP GC & LDAP GC SSL	Direktori, replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
UDP	123	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	Waktu Windows	Waktu Windows, kepercayaan
UDP	138	AWS Microsoft AD IPv4 VPC CIDR yang dikelola	DFSN & NetLogon	DFS, kebijakan grup
Semua	Semua	AWS membuat grup keamanan untuk pengontrol domain () <i>sg-123456</i> <i>7890abcde</i> <i>f0</i>	Semua Lalu Lintas	

Aturan Keluar

Protokol	Rentang Port	Destinasi	Jenis lalu lintas	Penggunaan Direktori Aktif
Semua	Semua	0.0.0.0/0	Semua Lalu Lintas	

- Untuk informasi selengkapnya tentang port dan protokol yang digunakan oleh Active Directory, lihat [Ringkasan layanan dan persyaratan port jaringan untuk Windows dalam Microsoft dokumentasi](#).
- Membuat akun administrator direktori dengan nama pengguna Admin dan kata sandi yang ditentukan. Akun ini terletak di bawah Users OU (Misalnya, Corp > Pengguna). Anda menggunakan akun ini untuk mengelola direktori Anda di AWS Cloud. Untuk informasi selengkapnya, lihat [AWS Akun Administrator Microsoft AD yang dikelola dan izin grup](#).

Important

Pastikan untuk menyimpan kata sandi ini. Directory Service tidak menyimpan kata sandi ini, dan tidak dapat diambil. Namun, Anda dapat mengatur ulang kata sandi dari Directory Service konsol atau dengan menggunakan [ResetUserPasswordAPI](#).

- Menciptakan tiga unit organisasi berikut (OUs) di bawah root domain:

Nama OU	Deskripsi
AWS Delegated Groups	Menyimpan semua grup yang dapat Anda gunakan untuk mendelegasikan izin AWS tertentu kepada pengguna Anda.
AWS Reserved	Menyimpan semua akun khusus AWS manajemen.
<yourdomainname>	Nama OU ini didasarkan dari nama NetBIOS yang Anda ketik saat membuat direktori. Jika Anda tidak menentukan nama NetBIOS, nama itu akan default ke bagian pertama dari nama DNS direktori Anda (misalnya, dalam kasus corp.example.com, nama NetBIOS adalah corp). OU ini dimiliki oleh AWS dan berisi

Nama OU	Deskripsi
	semua objek direktori AWS terkait Anda, yang Anda diberikan Kontrol Penuh atas. Dua anak OUs ada di bawah OU ini secara default; Komputer dan Pengguna. Contoh: • Corp • Komputer • Pengguna

- Membuat grup berikut diAWS Delegated Groups OU:

Nama grup	Deskripsi
AWS Delegated Account Operators	Anggota grup keamanan ini memiliki kemampuan manajemen akun terbatas seperti pengaturan ulang kata sandi
AWS Delegated Active Directory Based Activation Administrators	Anggota grup keamanan ini dapat membuat objek aktivasi lisensi volume Directory Aktif, yang memungkinkan korporasi untuk mengaktifkan komputer melalui sambungan ke domain mereka.
AWS Delegated Add Workstations To Domain Users	Anggota grup keamanan ini dapat menggabungkan 10 komputer ke sebuah domain.
AWS Delegated Administrators	Anggota grup keamanan ini dapat AWS mengelola Microsoft AD yang Dikelola, memiliki kontrol penuh atas semua objek di OU Anda dan dapat mengelola grup yang terdapat dalamAWS Delegated Groups OU.
AWS Delegated Allowed to Authenticate Objects	Anggota grup keamanan ini diberikan kemampuan untuk mengautentikasi ke sumber daya komputer di AWS Reserved OU

Nama grup	Deskripsi
	(Hanya diperlukan untuk objek lokal dengan Trusts yang diaktifkan Otentikasi Selektif).
AWS Delegated Allowed to Authenticate to Domain Controllers	Anggota grup keamanan ini diberikan kemampuan untuk mengautentikasi ke sumber daya komputer di Domain Controllers OU (Hanya diperlukan untuk objek lokal dengan Trusts yang diaktifkan Otentikasi Selektif).
AWS Delegated Deleted Object Lifetime Administrators	Anggota grup keamanan ini dapat memodifikasi msDS-DeletedObjectLifetime objek, yang menentukan berapa lama objek yang dihapus akan tersedia untuk dipulihkan dari Tempat Sampah AD.
AWS Delegated Distributed File System Administrators	Anggota grup keamanan ini dapat menambah dan menghapus FRS, DFS-R, dan ruang nama DFS.
AWS Delegated Domain Name System Administrators	Anggota grup keamanan ini dapat mengelola DNS terintegrasi Direktori Aktif.
AWS Delegated Dynamic Host Configuration Protocol Administrators	Anggota grup keamanan ini dapat mengotorisasi server Windows DHCP di korporasi.
AWS Delegated Enterprise Certificate Authority Administrators	Anggota grup keamanan ini dapat men-deploy dan mengelola infrastruktur Otoritas Sertifikat Microsoft Enterprise.
AWS Delegated Fine Grained Password Policy Administrators	Anggota grup keamanan ini dapat memodifikasi kebijakan kata sandi terperinci yang telah dibuat sebelumnya.
AWS Delegated FSx Administrators	Anggota grup keamanan ini diberikan kemampuan untuk mengelola FSx sumber daya Amazon.

Nama grup	Deskripsi
AWS Delegated Group Policy Administrators	Anggota grup keamanan ini dapat melakukan tugas manajemen kebijakan grup (membuat, mengedit, menghapus, tautan).
AWS Delegated Kerberos Delegation Administrators	Anggota grup keamanan ini dapat mengaktifkan delegasi pada komputer dan objek akun pengguna.
AWS Delegated Managed Service Account Administrators	Anggota grup keamanan ini dapat membuat dan menghapus Akun Layanan Terkelola.
AWS Delegated MS-NPRC Non-Compliant Devices	Anggota grup keamanan ini akan diberikan pengecualian dari memerlukan komunikasi saluran aman dengan pengendali domain. Grup ini adalah untuk akun komputer.
AWS Delegated Remote Access Service Administrators	Anggota grup keamanan ini dapat menambah dan menghapus server RAS dari grup Server RAS dan IAS.
AWS Delegated Replicate Directory Changes Administrators	Anggota grup keamanan ini dapat menyinkronkan informasi profil di Active Directory dengan SharePoint Server.
AWS Delegated Server Administrators	Anggota grup keamanan ini termasuk dalam grup administrator lokal pada semua komputer yang tergabung di domain.
AWS Delegated Sites and Services Administrators	Anggota grup keamanan ini dapat mengganti nama Default-First-Site-Name objek di Situs dan Layanan Direktori Aktif.
AWS Delegated System Management Administrators	Anggota grup keamanan ini dapat membuat dan mengelola objek dalam kontainer pengelolaan sistem.

Nama grup	Deskripsi
AWS Delegated Terminal Server Licensing Administrators	Anggota grup keamanan ini dapat menambah dan menghapus Server Lisensi Server Terminal dari grup Server Lisensi Server Terminal.
AWS Delegated User Principal Name Suffix Administrators	Anggota grup keamanan ini dapat menambah dan menghapus akhiran nama utama pengguna.

 Note

Anda dapat menambahkan ini AWS Delegated Groups.

- Membuat dan menerapkan Objek Kebijakan Grup berikut (GPOs):

 Note

Anda tidak memiliki izin untuk menghapus, memodifikasi, atau memutuskan tautan ini. GPOs Ini adalah desain karena mereka dicadangkan untuk AWS digunakan. Anda dapat menautkannya ke OUs yang Anda kendalikan jika diperlukan.

Nama kebijakan grup	Berlaku untuk	Deskripsi
Default Domain Policy	Domain	Termasuk kebijakan kata sandi domain dan Kerberos.
ServerAdmins	Semua akun komputer pengendali non domain	Menambahkan 'AWS Delegated Server Administrators' sebagai anggota BU ILTIN\Administrators Group.
AWS Reserved Policy:User	AWS Reserved user accounts	Menetapkan pengaturan keamanan yang disarankan

Nama kebijakan grup	Berlaku untuk	Deskripsi
		pada semua akun pengguna diAWS Reserved OU.
AWS Managed Active Directory Policy	Semua pengendali domain	Atur pengaturan keamanan yang direkomendasikan pada semua pengendali domain.
TimePolicyNT5DS	Semua pengontrol non PDCE domain	Menetapkan semua kebijakan waktu pengontrol non PDCE domain untuk menggunakan Windows Time (NT5DS).
TimePolicyPDC	Pengontrol PDCE domain	Menetapkan kebijakan waktu pengontrol PDCE domain untuk menggunakan Network Time Protocol (NTP).
Default Domain Controllers Policy	Tidak digunakan	Disediakan selama pembuatan domain, Kebijakan Direktori Aktif AWS Terkelola digunakan sebagai gantinya.

Jika Anda ingin melihat pengaturan dari setiap GPO, Anda dapat melihat mereka dari instans Windows yang tergabung domain misalnya dengan [Konsol Manajemen kebijakan grup \(GPMC\)](#) diaktifkan.

- Membuat hal berikut default local accounts untuk manajemen Microsoft AD yang AWS Dikelola:

Important

Pastikan untuk menyimpan kata sandi admin. Directory Service tidak menyimpan kata sandi ini, dan tidak dapat diambil. Namun, Anda [dapat mengatur ulang kata sandi dari Directory Service konsol](#) atau dengan menggunakan [ResetUserPasswordAPI](#).

Admin

AdminIni adalah yang directory administrator account dibuat ketika AD Microsoft yang AWS Dikelola pertama kali dibuat. Anda memberikan kata sandi untuk akun ini saat membuat iklan Microsoft AWS Terkelola. Akun ini terletak di bawah Users OU (Misalnya, Corp > Pengguna). Anda menggunakan akun ini untuk mengelola Direktori Aktif Anda di AWS. Untuk informasi selengkapnya, lihat [AWS Akun Administrator Microsoft AD yang dikelola dan izin grup](#).

AWS_1111111111

Setiap nama akun yang dimulai dengan AWS diikuti dengan garis bawah dan terletak di AWS Reserved OU adalah akun yang dikelola layanan. Akun yang dikelola layanan ini digunakan oleh AWS untuk berinteraksi dengan Active Directory. Akun-akun ini dibuat ketika AWS Directory Service Data diaktifkan dan dengan setiap AWS aplikasi baru yang diotorisasi di Active Directory. Akun ini hanya dapat diakses oleh AWS layanan.

krbtgt account

Ini krbtgt account memainkan peran penting dalam pertukaran tiket Kerberos yang digunakan oleh AWS Microsoft AD Terkelola Anda. krbtgt accountIni adalah akun khusus yang digunakan untuk enkripsi tiket pemberian tiket Kerberos (TGT), dan memainkan peran penting dalam keamanan protokol otentikasi Kerberos. Untuk informasi selengkapnya, lihat [dokumentasi Microsoft](#).

AWS secara otomatis memutar krbtgt account kata sandi untuk Microsoft AD AWS Terkelola Anda dua kali setiap 90 hari. Ada masa tunggu 24 jam antara dua rotasi berturut-turut setiap 90 hari.

Untuk informasi selengkapnya tentang akun admin dan akun lain yang dibuat oleh Active Directory, lihat [Microsoftdokumentasi](#).

AWS Akun Administrator Microsoft AD yang dikelola dan izin grup

Saat Anda membuat AWS direktori Directory Service untuk Microsoft Active Directory, AWS buat unit organisasi (OU) untuk menyimpan semua grup dan akun AWS terkait. Untuk informasi selengkapnya tentang OU ini, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#). Ini termasuk akun Admin. Akun Admin memiliki izin untuk melakukan aktivitas administratif umum berikut untuk OU Anda:

- Menambahkan, memperbarui, atau menghapus pengguna, grup, dan komputer. Untuk informasi selengkapnya, lihat [Manajemen pengguna dan grup di Microsoft AD yang AWS Dikelola](#).
- Menambahkan sumber daya ke domain Anda seperti server file atau cetak, kemudian berikan izin untuk sumber daya tersebut ke pengguna dan grup di OU Anda.
- Buat tambahan OUs dan wadah.
- Mendelegasikan wewenang tambahan OUs dan kontainer. Untuk informasi selengkapnya, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).
- Membuat dan menautkan kebijakan grup.
- Memulihkan objek yang dihapus dari Keranjang Sampah Directory Active.
- Jalankan PowerShell modul Active Directory dan DNS di Active Directory Web Service.
- Buat dan konfigurasi Akun Layanan Terkelola grup. Untuk informasi selengkapnya, lihat [Akun Layanan yang Dikelola Grup](#).
- Mengkonfigurasi delegasi terbatas Kerberos. Untuk informasi selengkapnya, lihat [Delegasi terbatas Kerberos](#).

Akun Admin juga memiliki hak untuk melakukan aktivitas di seluruh domain berikut:

- Mengelola konfigurasi DNS (menambahkan, menghapus, atau memperbarui catatan, zona, dan penerus)
- Melihat log peristiwa DNS
- Melihat log peristiwa keamanan

Hanya tindakan yang tercantum di sini yang diizinkan untuk akun Admin. Akun Admin juga tidak memiliki izin untuk setiap tindakan terkait direktori di luar OU spesifik Anda, seperti pada OU induk.

Pertimbangan-pertimbangan

- AWS Administrator Domain memiliki akses administratif penuh ke semua domain yang di-host. AWS Lihat perjanjian Anda AWS dan [FAQ perlindungan AWS data](#) untuk informasi selengkapnya tentang cara AWS menangani konten, termasuk informasi direktori, yang Anda simpan di AWS sistem.
- Kami merekomendasikan agar Anda tidak menghapus atau mengubah nama akun ini. Jika Anda tidak lagi ingin menggunakan akun, kami sarankan Anda menetapkan kata sandi yang panjang (paling banyak 64 karakter acak) dan kemudian nonaktifkan akun.

 Note

AWS memiliki kontrol eksklusif atas pengguna dan grup istimewa Administrator Domain dan Administrator Perusahaan. Hal ini memungkinkan AWS untuk melakukan manajemen operasional direktori Anda.

Akun istimewa administrator korporasi dan domain

AWS secara otomatis memutar kata sandi Administrator bawaan ke kata sandi acak setiap 90 hari. Kapan saja kata sandi Administrator bawaan diminta untuk penggunaan manusia, AWS tiket dibuat dan dicatat dengan Directory Service tim. Kredensial akun dienkripsi dan ditangani melalui saluran aman. Juga kredensi akun Administrator hanya dapat diminta oleh tim Directory Service manajemen.

Untuk melakukan manajemen operasional direktori Anda, AWS memiliki kontrol eksklusif atas akun dengan hak istimewa Administrator Perusahaan dan Administrator Domain. Ini termasuk kontrol eksklusif akun administrator Direktori Aktif. AWS melindungi akun ini dengan mengotomatiskan manajemen kata sandi melalui penggunaan brankas kata sandi. Selama rotasi otomatis kata sandi administrator, AWS buat akun pengguna sementara dan berikan hak istimewa Administrator Domain. Akun sementara ini digunakan sebagai back-up jika terjadi kegagalan rotasi kata sandi pada akun administrator. Setelah AWS berhasil memutar kata sandi administrator, AWS menghapus akun administrator sementara.

Biasanya AWS mengoperasikan direktori sepenuhnya melalui otomatisasi. Jika proses otomatisasi tidak dapat menyelesaikan masalah operasional, AWS mungkin perlu meminta insinyur dukungan masuk ke pengontrol domain (DC) Anda untuk melakukan diagnosis. Dalam kasus yang jarang terjadi ini, AWS menerapkan request/notification sistem untuk memberikan akses. Dalam proses ini, AWS otomatisasi membuat akun pengguna terbatas waktu di direktori Anda yang memiliki izin Administrator Domain. AWS mengaitkan akun pengguna dengan insinyur yang ditugaskan untuk bekerja di direktori Anda. AWS mencatat asosiasi ini dalam sistem log kami dan memberikan insinyur dengan kredensi untuk digunakan. Semua tindakan yang diambil oleh teknisi dicatat dalam log peristiwa Windows. Ketika waktu yang dialokasikan berlalu, otomatisasi menghapus akun pengguna.

Anda dapat memantau tindakan akun administratif dengan menggunakan fitur penerusan log direktori Anda. Fitur ini memungkinkan Anda untuk meneruskan peristiwa Keamanan AD ke CloudWatch sistem Anda di mana Anda dapat menerapkan solusi pemantauan. Untuk informasi selengkapnya, lihat [Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS](#).

Peristiwa Keamanan IDs 4624, 4672 dan 4648 semuanya dicatat ketika seseorang masuk ke DC secara interaktif. Anda dapat melihat setiap log peristiwa Windows Security DC menggunakan Event Viewer Microsoft Management Console (MMC) dari domain yang bergabung dengan komputer Windows. Anda juga dapat [Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS](#) mengirim semua log peristiwa Keamanan ke CloudWatch Log di akun Anda.

Anda mungkin sesekali melihat pengguna yang dibuat dan dihapus dalam OU AWS Cadangan. AWS bertanggung jawab atas pengelolaan dan keamanan semua objek di OU ini dan OU atau wadah lainnya di mana kami belum mendelegasikan izin bagi Anda untuk mengakses dan mengelola. Anda mungkin melihat pembuatan dan penghapusan di OU tersebut. Ini karena Directory Service menggunakan otomatisasi untuk memutar kata sandi Administrator Domain secara teratur. Ketika kata sandi dirotasi, backup dibuat pada peristiwa rotasi yang gagal. Setelah rotasi berhasil, akun backup akan dihapus secara otomatis. Juga dalam hal langka bahwa akses interaktif diperlukan pada DCs untuk tujuan pemecahan masalah, akun pengguna sementara dibuat untuk seorang Directory Service insinyur untuk digunakan. Setelah teknisi menyelesaikan pekerjaan mereka, akun pengguna sementara akan dihapus. Perhatikan bahwa setiap kali kredensi interaktif diminta untuk direktori, tim Directory Service manajemen akan diberi tahu.

Konsep kunci dan praktik terbaik untuk Microsoft AD yang AWS Dikelola

Anda bisa mendapatkan lebih banyak dari Microsoft AD yang AWS Dikelola dengan menjadi akrab dengan konsep-konsep utama dan praktik terbaik. Konsep utama membantu Anda memahami cara kerja Microsoft AD yang AWS Dikelola. Konsep utama termasuk mempelajari lebih lanjut tentang skema Direktori Aktif, jadwal penambalan, dan Akun Layanan Terkelola Grup. Skema Active Directory mencakup elemen seperti atribut, kelas, dan objek yang membentuk Microsoft AD yang AWS Dikelola. AWS menambal pengontrol domain Microsoft AD AWS Terkelola Anda dengan Microsoft pembaruan atas nama Anda. Anda juga dapat mempelajari selengkapnya tentang grup Akun Layanan Terkelola (gMSAs) dan menggunakannya dengan iklan Microsoft AWS Terkelola.

Anda dapat menghindari masalah dengan Microsoft AD yang AWS Dikelola dengan mempertimbangkan praktik terbaik. Beberapa praktik terbaik ini meliputi:

- Saat menyiapkan iklan Microsoft AWS Terkelola, mengonfigurasi grup keamanan untuk memenuhi kebutuhan Anda, mengingat ID dan kata sandi akun administrator Anda, dan aktifkan pengaturan penerusan bersyarat.

- Saat menggunakan iklan Microsoft AWS Terkelola, jangan ubah unit organisasi yang AWS dibuat saat direktori dibuat, pantau performa dengan alat seperti Amazon CloudWatch dan Amazon SNS, dan gunakan klien SMB 2.x.
- Saat memprogram aplikasi untuk bekerja dengan Microsoft AD yang AWS Dikelola, gunakan layanan pencari lokasi Windows DC, uji beban berubah sebelum meluncurkannya ke lingkungan produksi, dan gunakan kueri LDAP yang efisien untuk menghindari siklus CPU yang signifikan dalam pengontrol domain.

Topik

- [AWS Konsep kunci Microsoft AD yang dikelola](#)
- [AWS Praktik terbaik Microsoft AD yang dikelola](#)

AWS Konsep kunci Microsoft AD yang dikelola

Anda akan mendapatkan lebih banyak dari Microsoft AD yang AWS Dikelola jika Anda terbiasa dengan konsep-konsep kunci berikut.

Topik

- [Skema Direktori Aktif](#)
- [Penambalan dan pemeliharaan untuk Microsoft AD yang AWS Dikelola](#)
- [Akun Layanan yang Dikelola Grup](#)
- [Delegasi terbatas Kerberos](#)

Skema Direktori Aktif

Skema adalah definisi atribut dan kelas yang merupakan bagian dari direktori terdistribusi dan mirip dengan bidang dan tabel dalam basis data. Skema termasuk seperangkat aturan yang menentukan jenis dan format data yang dapat ditambahkan atau disertakan dalam basis data. Kelas Pengguna adalah salah satu contoh dari kelas yang disimpan dalam basis data. Beberapa contoh atribut kelas Pengguna dapat mencakup nama depan pengguna, nama belakang, nomor telepon, dan sebagainya.

Elemen skema

Atribut, kelas dan objek adalah elemen dasar yang digunakan untuk membangun definisi objek dalam skema. Berikut ini memberikan rincian tentang elemen skema yang penting untuk diketahui sebelum Anda memulai proses untuk memperluas skema AD Microsoft AWS Terkelola Anda.

Atribut

Setiap atribut skema, yang mirip dengan bidang dalam basis data, memiliki beberapa properti yang menentukan karakteristik atribut. Misalnya, properti yang digunakan oleh klien LDAP untuk membaca dan menulis atribut `LDAPDisplayName`. Properti `LDAPDisplayName` harus unik di semua atribut dan kelas. Untuk daftar lengkap karakteristik atribut, lihat [Karakteristik Atribut](#) pada situs web MSDN. Untuk pedoman tambahan tentang cara membuat atribut baru, lihat [Menentukan Atribut Baru](#) pada situs web MSDN.

Kelas

Kelas-kelas adalah analog dengan tabel dalam database dan juga memiliki beberapa sifat untuk ditentukan. Misalnya, `objectClassCategory` menentukan kategori kelas. Untuk daftar lengkap karakteristik atribut, lihat [Karakteristik Atribut](#) pada situs web MSDN. Untuk informasi selengkapnya tentang cara membuat kelas baru, lihat [Menentukan Kelas Baru](#) pada situs web MSDN.

Pengenal objek (OID)

Setiap kelas dan atribut harus memiliki OID yang unik untuk semua objek Anda. Vendor perangkat lunak harus mendapatkan OID mereka sendiri untuk memastikan keunikan. Keunikan menghindari konflik ketika atribut yang sama digunakan oleh lebih dari satu aplikasi untuk tujuan yang berbeda. Untuk memastikan keunikan, Anda dapat memperoleh OID root dari Otoritas Pendaftaran Nama ISO. Atau, Anda dapat memperoleh dasar OID dari Microsoft. Untuk informasi selengkapnya tentang OIDs dan cara mendapatkannya, lihat [Pengenal Objek di situs](#) web MSDN.

Atribut terkait skema

Beberapa atribut dihubungkan antara dua kelas dengan tautan terusan dan kembali. Contoh terbaik adalah grup. Ketika Anda melihat grup itu menunjukkan kepada Anda anggota grup; jika Anda melihat pengguna Anda dapat melihat grup apa yang menjadi miliknya. Ketika Anda menambahkan pengguna ke grup, Direktori Aktif membuat tautan terusan ke grup. Kemudian Direktori Aktif menambahkan tautan kembali dari grup ke pengguna. ID tautan unik harus dibuat saat membuat atribut yang akan ditautkan. Untuk informasi selengkapnya, lihat [Atribut Tertaut](#) pada situs web MSDN.

Topik terkait

- [Kapan harus memperpanjang skema AD Microsoft AWS Terkelola](#)
- [Tutorial: Memperluas skema AD Microsoft AWS Terkelola Anda](#)

Penambalan dan pemeliharaan untuk Microsoft AD yang AWS Dikelola

AWS Directory Service untuk Microsoft Active Directory, juga dikenal sebagai AWS DS untuk Microsoft AD yang AWS dikelola, sebenarnya adalah Microsoft Active Directory Domain Services (AD DS), disampaikan sebagai layanan terkelola. Sistem ini menggunakan Microsoft Windows Server 2019 untuk pengontrol domain (DCs), dan AWS menambahkan perangkat lunak ke DCs untuk tujuan manajemen layanan. AWS pembaruan (tambalan) DCs untuk menambahkan fungsionalitas baru dan menjaga perangkat lunak Microsoft Windows Server tetap terkini. Selama proses patch, direktori Anda tetap tersedia untuk digunakan.

Memastikan ketersediaan

Secara default setiap direktori terdiri dari dua DCs, masing-masing diinstal di Availability Zone yang berbeda. Sesuai pilihan Anda, Anda dapat DCs menambah ketersediaan lebih lanjut. Untuk lingkungan kritis yang membutuhkan ketersediaan tinggi dan toleransi kesalahan, sebaiknya gunakan tambahan. DCs AWS menambal DCs secara berurutan, selama waktu itu DC yang secara aktif menambal AWS tidak tersedia. Jika satu atau lebih dari Anda sementara DCs tidak berfungsi, tunda AWS patching sampai direktori Anda memiliki setidaknya dua operasional. DCs Ini memungkinkan Anda menggunakan operasi lain DCs selama proses patch, yang biasanya memakan waktu 30 hingga 45 menit per DC, meskipun waktu ini dapat bervariasi. Untuk memastikan aplikasi Anda dapat mencapai DC yang beroperasi jika satu atau lebih tidak DCs tersedia karena alasan apa pun, termasuk penambalan, aplikasi Anda harus menggunakan layanan pencari lokasi Windows DC dan tidak menggunakan alamat DC statis.

Memahami jadwal patching

Untuk menjaga agar perangkat lunak Microsoft Windows Server tetap terkini pada Anda DCs, AWS gunakan pembaruan Microsoft. Karena Microsoft membuat patch rollup bulanan tersedia untuk Windows Server, AWS melakukan upaya terbaik untuk menguji dan menerapkan rollup ke semua pelanggan DCs dalam waktu tiga minggu kalender. Selain itu, AWS meninjau pembaruan yang dirilis Microsoft di luar rollup bulanan berdasarkan penerapan dan urgensi. DCs Untuk patch keamanan yang menurut Microsoft sebagai Penting atau Penting, dan yang relevan dengannya DCs, AWS melakukan segala upaya untuk menguji dan menyebarkan patch dalam waktu lima hari.

Akun Layanan yang Dikelola Grup

Dengan Windows Server 2012, Microsoft memperkenalkan metode baru yang dapat digunakan administrator untuk mengelola akun layanan yang disebut grup Akun Layanan Terkelola (gMSAs). Menggunakan gMSAs, administrator layanan tidak lagi perlu mengelola sinkronisasi kata sandi secara manual antar instance layanan. Sebaliknya, administrator hanya dapat membuat gMSA di Direktori Aktif dan kemudian mengkonfigurasi beberapa instans layanan untuk menggunakan gMSA tunggal.

Untuk memberikan izin agar pengguna di Microsoft AD yang AWS Dikelola dapat membuat GMSA, Anda harus menambahkan akun mereka sebagai anggota grup keamanan Administrator Akun Layanan Terkelola AWS yang Delegasi. Secara default, akun Admin adalah anggota grup ini. Untuk informasi selengkapnya tentang gMSAs, lihat [Ringkasan Akun Layanan Terkelola Grup](#) di TechNet situs web Microsoft.

Posting Blog AWS Keamanan Terkait

- [Bagaimana Microsoft AD yang AWS Dikelola Membantu Menyederhanakan Penyebaran dan Meningkatkan Keamanan Aplikasi .NET Terintegrasi Direktori Aktif](#)

Delegasi terbatas Kerberos

Kerberos constrained delegation adalah sebuah fitur di Windows Server. Fitur ini memberi administrator layanan kemampuan untuk menentukan dan menegakkan batasan kepercayaan aplikasi dengan membatasi ruang lingkup di mana layanan aplikasi dapat bertindak atas nama pengguna. Hal ini dapat berguna ketika Anda perlu mengkonfigurasi akun layanan front-end yang dapat mendelegasikan ke layanan backend mereka. Kerberos constrained delegation juga mencegah gMSA Anda untuk menghubungkan ke setiap dan semua layanan atas nama pengguna Direktori Aktif Anda, menghindari potensi penyalahgunaan oleh developer nakal.

Misalnya, katakanlah pengguna jsmith masuk ke aplikasi HR. Anda ingin SQL Server menerapkan izin database jsmith. Namun, secara default SQL Server membuka koneksi database menggunakan kredensial akun layanan yang menerapkan hr-app-service izin alih-alih izin yang dikonfigurasi jsmith. Anda harus memungkinkan aplikasi penggajian SDM untuk mengakses database SQL Server menggunakan kredensial jsmith. Untuk melakukannya, Anda mengaktifkan delegasi terbatas Kerberos untuk akun hr-app-service layanan di direktori AWS Microsoft AD Terkelola di. AWS Ketika jsmith masuk, Direktori Aktif menyediakan tiket Kerberos yang secara otomatis Windows gunakan ketika jsmith mencoba untuk mengakses layanan lain dalam jaringan. Delegasi

Kerberos memungkinkan hr-app-service akun untuk menggunakan kembali tiket jsmith Kerberos saat mengakses database, sehingga menerapkan izin khusus untuk jsmith saat membuka koneksi database.

Untuk memberikan izin yang memungkinkan pengguna di Microsoft AD yang AWS Dikelola mengonfigurasi delegasi terbatas Kerberos, Anda harus menambahkan akun mereka sebagai anggota grup keamanan Administrator Delegasi Kerberos yang AWS Delegasi. Secara default, akun Admin adalah anggota grup ini. Untuk informasi selengkapnya tentang delegasi terbatas Kerberos, lihat Ikhtisar Delegasi Terbatas [Kerberos](#) di situs web Microsoft. TechNet

[Delegasi terbatas berbasis sumber daya](#) diperkenalkan dengan Windows Server 2012. Ini menyediakan layanan back-end administrator kemampuan untuk mengkonfigurasi delegasi terbatas untuk layanan.

AWS Praktik terbaik Microsoft AD yang dikelola

Berikut adalah beberapa saran dan panduan yang harus Anda pertimbangkan untuk menghindari masalah dan mendapatkan hasil maksimal dari Microsoft AD yang AWS Dikelola.

Topik

- [Praktik terbaik untuk menyiapkan iklan Microsoft yang AWS Dikelola](#)
- [Praktik terbaik saat menggunakan direktori Microsoft AD yang AWS Dikelola](#)
- [Praktik terbaik saat memprogram aplikasi Anda untuk Microsoft AD yang AWS Dikelola](#)

Praktik terbaik untuk menyiapkan iklan Microsoft yang AWS Dikelola

Berikut adalah beberapa saran dan pedoman saat menyiapkan iklan Microsoft AWS Terkelola:

Topik

- [Prasyarat](#)
- [Membuat Microsoft AD yang AWS Dikelola](#)

Prasyarat

Pertimbangkan panduan ini sebelum membuat direktori Anda.

Verifikasikan Anda memiliki jenis direktori yang tepat

Directory Service menyediakan berbagai cara untuk digunakan Microsoft Active Directory dengan AWS layanan lain. Anda dapat memilih directory service dengan fitur yang Anda butuhkan dengan biaya yang sesuai dengan anggaran Anda:

- AWS Directory Service untuk Microsoft Active Directory adalah pengelola kaya fitur yang Microsoft Active Directory dihosting di cloud. AWS AWS Microsoft AD yang dikelola adalah pilihan terbaik Anda jika Anda memiliki lebih dari 5.000 pengguna dan memerlukan hubungan kepercayaan yang disiapkan antara direktori yang AWS dihosting dan direktori lokal Anda.
- AD Connector cukup menghubungkan Active Directory lokal Anda yang ada. AWS AD Connector adalah pilihan terbaik Anda saat Anda ingin menggunakan direktori on-premise Anda yang sudah ada dengan layanan AWS .
- Simple AD adalah direktori berskala rendah dan berbiaya rendah dengan kompatibilitas Active Directory dasar. Ini mendukung 5.000 atau lebih sedikit pengguna, aplikasi yang kompatibel dengan Samba 4, dan kompatibilitas LDAP untuk aplikasi sadar LDAP.

Untuk perbandingan Directory Service opsi yang lebih rinci, lihat [Mana yang harus dipilih](#).

Pastikan Anda VPCs dan instans dikonfigurasi dengan benar

Untuk terhubung ke, mengelola, dan menggunakan direktori Anda, Anda harus mengonfigurasi dengan benar VPCs bahwa direktori terkait. Lihat [Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS](#), [Prasyarat AD Connector](#), atau [Prasyarat Simple AD](#) untuk informasi tentang persyaratan keamanan dan jaringan VPC.

Jika Anda menambahkan instans ke domain Anda, pastikan bahwa Anda memiliki konektivitas dan akses jarak jauh ke instans Anda seperti yang dijelaskan di [Cara untuk bergabung dengan instans Amazon EC2 ke AWS Microsoft AD yang Dikelola](#).

Ketahui batasan Anda

Pelajari tentang berbagai batasan untuk jenis direktori spesifik Anda. Penyimpanan yang tersedia dan ukuran agregat objek Anda adalah satu-satunya keterbatasan terkait jumlah objek yang dapat Anda simpan dalam direktori Anda. Lihat [AWS Kuota Microsoft AD yang dikelola](#), [Kuota AD Connector](#), atau [Kuota Simple AD](#) untuk detail tentang direktori pilihan Anda.

Memahami konfigurasi dan penggunaan grup AWS keamanan direktori Anda

AWS membuat [grup keamanan](#) dan melampirkannya ke [antarmuka jaringan elastis](#) pengontrol domain direktori Anda. Grup keamanan ini memblokir lalu lintas yang tidak perlu ke pengontrol domain dan memungkinkan lalu lintas yang diperlukan untuk komunikasi Active Directory. AWS mengkonfigurasi grup keamanan untuk membuka hanya port yang diperlukan untuk komunikasi Active Directory. Dalam konfigurasi default, grup keamanan menerima lalu lintas ke port ini dari alamat CIDR IPv4 VPC AD Microsoft AD yang AWS Dikelola. AWS melampirkan grup keamanan ke antarmuka pengontrol domain Anda yang dapat diakses dari dalam peered atau diubah ukurannya. [VPCs](#) Antarmuka ini tidak dapat diakses dari internet bahkan jika Anda mengubah tabel perutean, mengubah koneksi jaringan ke VPC Anda, dan mengkonfigurasi [layanan NAT Gateway](#). Dengan demikian, hanya instans dan komputer yang memiliki jalur jaringan ke VPC dapat mengakses direktori. Ini menyederhanakan pengaturan dengan menghilangkan persyaratan bagi Anda untuk mengkonfigurasi rentang alamat tertentu. Sebaliknya, Anda mengkonfigurasi rute dan grup keamanan ke VPC yang mengizinkan lalu lintas hanya dari instans dan komputer terpercaya.

Memodifikasi grup keamanan direktori

Jika Anda ingin meningkatkan keamanan grup keamanan direktori Anda, Anda dapat memodifikasinya untuk menerima lalu lintas dari daftar alamat IP yang lebih ketat. Misalnya, Anda dapat mengubah alamat yang diterima dari rentang IPv4 CIDR VPC Anda ke rentang CIDR yang khusus untuk satu subnet atau komputer. Demikian pula, Anda dapat memilih untuk membatasi alamat tujuan yang di mana pengendali domain Anda bisa berkomunikasi. Hanya buat perubahan tersebut jika Anda sepenuhnya memahami cara kerja filter grup keamanan. Untuk informasi selengkapnya, lihat [Grup Keamanan Amazon EC2 untuk instans Linux](#) di Panduan Pengguna Amazon EC2. Perubahan yang tidak tepat dapat mengakibatkan hilangnya komunikasi ke komputer dan instance yang dituju. AWS merekomendasikan agar Anda tidak mencoba membuka port tambahan ke pengontrol domain karena ini mengurangi keamanan direktori Anda. Harap tinjau dengan seksama [Model Tanggung Jawab Bersama AWS](#).

Warning

Hal itu mungkin secara teknis untuk Anda dapat mengasosiasikan grup keamanan direktori dengan instans EC2 lain yang Anda buat. Namun, AWS merekomendasikan untuk tidak melakukan praktik ini. AWS mungkin memiliki alasan untuk memodifikasi grup keamanan tanpa pemberitahuan untuk mengatasi kebutuhan fungsional atau keamanan direktori terkelola. Perubahan tersebut mempengaruhi setiap instans yang Anda asosiasikan dengan grup keamanan direktori. Selain itu, mengasosiasikan grup keamanan direktori dengan

instans EC2 Anda dapat menciptakan risiko keamanan potensial untuk instans EC2 Anda. Grup keamanan direktori menerima lalu lintas pada port Direktori Aktif yang diperlukan dari alamat Microsoft AD VPC IPv4 CIDR yang AWS Dikelola. Jika Anda mengasosiasikan grup keamanan ini dengan instans EC2 yang memiliki alamat IP publik yang terpasang ke internet, maka setiap komputer di internet dapat berkomunikasi dengan Anda instans EC2 pada port-port yang terbuka.

Membuat Microsoft AD yang AWS Dikelola

Berikut adalah beberapa saran untuk dipertimbangkan saat Anda membuat iklan Microsoft AWS Terkelola.

Topik

- [Ingat ID dan kata sandi administrator Anda](#)
- [Buat set opsi DHCP](#)
- [Aktifkan Pengaturan Forwarder Bersyarat](#)
- [Men-deploy pengendali domain tambahan](#)
- [Memahami batasan nama pengguna untuk AWS aplikasi](#)

Ingat ID dan kata sandi administrator Anda

Saat mengatur direktori Anda, Anda memberikan kata sandi untuk akun administrator. ID akun tersebut adalah Admin untuk Microsoft AD yang AWS Dikelola. Ingat kata sandi yang Anda buat untuk akun ini; jika tidak, Anda tidak akan dapat menambahkan objek ke direktori Anda.

Buat set opsi DHCP

Kami menyarankan Anda membuat opsi DHCP yang ditetapkan untuk Directory Service direktori Anda dan menetapkan opsi DHCP yang disetel ke VPC tempat direktori Anda berada. Dengan cara itu setiap instans dalam VPC dapat menunjuk ke domain tertentu, dan server DNS dapat menyelesaikan nama domain mereka.

Untuk informasi selengkapnya tentang set pilihan DHCP, lihat [Membuat atau mengubah opsi DHCP yang disetel untuk Microsoft AD yang AWS Dikelola](#).

Aktifkan Pengaturan Forwarder Bersyarat

Pengaturan penerusan bersyarat berikut Simpan forwarder bersyarat ini di Active Directory, replikasi sebagai berikut: harus diaktifkan. Mengaktifkan pengaturan ini akan memastikan pengaturan forwarder bersyarat persisten ketika node diganti karena kegagalan infrastruktur atau kegagalan kelebihan beban.

Forwarder bersyarat harus dibuat pada satu Domain Controller dengan pengaturan sebelumnya diaktifkan. Ini akan memungkinkan replikasi ke Pengontrol Domain lainnya.

Men-deploy pengendali domain tambahan

Secara default, AWS buat dua pengontrol domain yang ada di Availability Zone terpisah. Hal ini memberikan ketahanan kesalahan selama patch perangkat lunak dan peristiwa lain yang dapat membuat satu pengendali domain tidak terjangkau atau tidak tersedia. Kami merekomendasikan Anda [men-deploy pengendali domain tambahan](#) untuk lebih meningkatkan ketahanan dan memastikan performa menskalakan keluar dalam peristiwa dari peristiwa jangka panjang yang mempengaruhi akses ke pengendali domain atau Availability Zone.

Untuk informasi selengkapnya, lihat [Gunakan layanan pencari lokasi Windows DC](#).

Memahami batasan nama pengguna untuk AWS aplikasi

Directory Service memberikan dukungan untuk sebagian besar format karakter yang dapat digunakan dalam pembangunan nama pengguna. Namun, ada batasan karakter yang diberlakukan pada nama pengguna yang akan digunakan untuk masuk ke AWS aplikasi, seperti, WorkDocs Amazon WorkSpaces WorkMail, atau Quick. Pembatasan ini mengharuskan karakter berikut tidak digunakan:

- Spasi
- Karakter multibyte
- !"#\$%&'()*+,-./:;<=>?@[\\]^_{|}~

Note

Simbol @ diperbolehkan selama itu mendahului akhiran UPN.

Praktik terbaik saat menggunakan direktori Microsoft AD yang AWS Dikelola

Berikut adalah beberapa saran yang perlu diingat saat menggunakan iklan Microsoft AWS Terkelola Anda.

Topik

- [Jangan mengubah pengguna, grup, dan unit organisasi yang telah ditetapkan](#)
- [Gabung domain secara otomatis](#)
- [Atur kepercayaan dengan benar](#)
- [Lacak kinerja pengontrol domain Anda](#)
- [Berhati-hati merancang ekstensi skema](#)
- [Tentang penyeimbang beban](#)
- [Buat backup instans Anda](#)
- [Mengatur olahpesan SNS](#)
- [Terapkan pengaturan layanan direktori](#)
- [Hapus aplikasi Amazon Enterprise sebelum menghapus direktori](#)
- [Menggunakan klien SMB 2.x saat mengakses saham SYSVOL dan NETLOGON](#)

Jangan mengubah pengguna, grup, dan unit organisasi yang telah ditetapkan

Saat Anda menggunakan Directory Service untuk meluncurkan direktori, AWS buat unit organisasi (OU) yang berisi semua objek direktori Anda. OU ini, yang memiliki nama NetBIOS yang Anda ketik saat membuat direktori Anda, terletak di root domain. Root domain dimiliki dan dikelola oleh AWS. Beberapa grup dan pengguna administratif juga dibuat.

Jangan memindahkan, menghapus atau dengan cara lain mengubah objek yang telah ditetapkan. Melakukannya dapat membuat direktori Anda tidak dapat diakses oleh Anda dan AWS. Untuk informasi selengkapnya, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).

Gabung domain secara otomatis

Saat meluncurkan instance Windows yang akan menjadi bagian dari Directory Service domain, seringkali paling mudah untuk bergabung dengan domain sebagai bagian dari proses pembuatan instance daripada menambahkan instance secara manual nanti. Untuk menggabungkan domain secara otomatis, cukup pilih direktori yang benar untuk Direktori penggabungan domain saat

meluncurkan instans baru. Anda dapat menemukan detailnya di [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#).

Atur kepercayaan dengan benar

Saat menyiapkan hubungan kepercayaan antara direktori Microsoft AD AWS Terkelola dan direktori lain, perhatikan panduan ini:

- Jenis kepercayaan harus cocok di kedua sisi (Forest atau Eksternal)
- Pastikan arah kepercayaan diatur dengan benar jika menggunakan kepercayaan satu arah (Keluar pada domain terpercaya, Masuk pada domain terpercaya)
- Baik nama domain yang memenuhi syarat (FQDNs) dan nama NetBIOS harus unik antara hutan/domain

Untuk detail selengkapnya dan petunjuk spesifik tentang cara mengatur hubungan kepercayaan, lihat [Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri](#).

Lacak kinerja pengontrol domain Anda

Untuk membantu mengoptimalkan keputusan penskalaan dan meningkatkan ketahanan dan kinerja direktori, sebaiknya gunakan metrik. CloudWatch Untuk informasi selengkapnya, lihat [Menggunakan CloudWatch untuk memantau kinerja pengontrol domain Microsoft AD yang AWS Dikelola](#).

Untuk petunjuk tentang cara mengatur metrik pengontrol domain menggunakan CloudWatch konsol, lihat [Cara mengotomatiskan penskalaan AWS Microsoft AD Terkelola berdasarkan metrik pemanfaatan di Blog Keamanan. AWS](#)

Berhati-hati merancang ekstensi skema

Terapkan ekstensi skema dengan cermat untuk mengindeks direktori Anda untuk kueri yang penting dan sering. Berhati-hati untuk tidak over-indeks direktori karena indeks mengkonsumsi ruang direktori dan dengan cepat mengubah nilai-nilai yang diindeks dapat mengakibatkan masalah performa. Untuk menambahkan indeks, Anda harus membuat file Lightweight Directory Access Protocol (LDAP) Directory Interchange Format (LDIF) dan memperpanjang perubahan skema Anda. Untuk informasi selengkapnya, lihat [Perluas skema AD Microsoft AWS Terkelola Anda](#).

Tentang penyeimbang beban

Jangan gunakan penyeimbang beban di depan titik akhir Microsoft AD yang AWS Dikelola. Microsoft dirancang Active Directory (AD) untuk digunakan dengan algoritma penemuan pengontrol domain (DC) yang menemukan DC operasional paling responsif tanpa penyeimbangan beban eksternal. Penyeimbang beban jaringan eksternal mendeteksi aktif secara tidak akurat DCs dan dapat mengakibatkan aplikasi Anda dikirim ke DC yang muncul tetapi tidak siap untuk digunakan. Untuk informasi selengkapnya, lihat [Load balancer dan Active Directory](#) di Microsoft TechNet yang merekomendasikan untuk memperbaiki aplikasi agar menggunakan Active Directory dengan benar daripada menerapkan penyeimbang beban eksternal.

Buat backup instans Anda

Jika Anda memutuskan untuk menambahkan instance secara manual ke Directory Service domain yang ada, buat cadangan atau ambil snapshot dari instance tersebut terlebih dahulu. Hal ini sangat penting ketika menggabungkan instans Linux. Beberapa prosedur digunakan untuk menambahkan instans, jika tidak dilakukan dengan benar, dapat membuat instans Anda tidak terjangkau atau tidak dapat digunakan. Untuk informasi selengkapnya, lihat [Memulihkan iklan Microsoft AWS Terkelola Anda dengan snapshot](#).

Mengatur olahpesan SNS

Dengan Amazon Simple Notification Service (Amazon SNS), Anda dapat menerima pesan email atau teks (SMS) ketika status direktori Anda berubah. Anda akan diberi tahu jika direktori Anda berjalan dari status Aktif ke status Gangguan atau Tidak bisa dioperasi. Anda juga menerima notifikasi ketika direktori kembali ke status Aktif.

Juga ingat bahwa jika Anda memiliki topik SNS yang menerima pesan dari Directory Service, sebelum menghapus topik itu dari konsol Amazon SNS, Anda harus mengaitkan direktori Anda dengan topik SNS yang berbeda. Jika tidak, Anda berisiko kehilangan pesan status direktori penting. Untuk informasi tentang cara mengatur Amazon SNS, lihat [Mengaktifkan pemberitahuan status direktori Microsoft AD AWS Terkelola dengan Amazon Simple Notification Service](#).

Terapkan pengaturan layanan direktori

AWS Microsoft AD yang dikelola memungkinkan Anda menyesuaikan konfigurasi keamanan untuk memenuhi persyaratan kepatuhan dan keamanan Anda. AWS Microsoft AD yang dikelola menyebarkan dan memelihara konfigurasi ke semua pengontrol domain di direktori Anda, termasuk saat menambahkan wilayah baru atau pengontrol domain tambahan. Anda dapat mengonfigurasi dan

menerapkan pengaturan keamanan ini untuk semua direktori baru dan yang sudah ada. Anda dapat melakukan ini di konsol dengan mengikuti langkah-langkah di dalam [Edit pengaturan keamanan direktori](#) atau melalui [UpdateSettingsAPI](#).

Untuk informasi selengkapnya, lihat [Mengedit pengaturan keamanan direktori Microsoft AD yang AWS Dikelola](#).

Hapus aplikasi Amazon Enterprise sebelum menghapus direktori

Sebelum menghapus direktori yang terkait dengan satu atau beberapa Aplikasi Amazon Enterprise seperti,, Amazon WorkSpaces Application Manager WorkSpaces, Amazon, WorkDocs WorkMail Konsol Manajemen AWS, atau Amazon Relational Database Service (Amazon RDS), Anda harus terlebih dahulu menghapus setiap aplikasi. Untuk informasi selengkapnya untuk cara menghapus aplikasi ini, lihat [Menghapus iklan Microsoft yang AWS Dikelola](#).

Menggunakan klien SMB 2.x saat mengakses saham SYSVOL dan NETLOGON

Komputer klien menggunakan Blok Pesan Server (SMB) untuk mengakses saham SYSVOL dan NETLOGON pada pengontrol domain AWS Microsoft AD Terkelola untuk Kebijakan Grup, skrip login, dan file lainnya. AWS Microsoft AD yang dikelola hanya mendukung SMB versi 2.0 (SMBv2) dan yang lebih baru.

Protokol versi yang lebih baru menambahkan sejumlah fitur yang meningkatkan kinerja klien dan meningkatkan keamanan pengontrol domain dan klien Anda. SMBv2 Perubahan ini mengikuti rekomendasi oleh Tim [Kesiapan Darurat Komputer Amerika Serikat](#) dan [Microsoft](#) untuk SMBv1 menonaktifkan.

Important

Jika saat ini Anda menggunakan SMBv1 klien untuk mengakses saham SYSVOL dan NETLOGON dari pengontrol domain Anda, Anda harus memperbarui klien tersebut untuk digunakan atau yang lebih baru. SMBv2 Direktori Anda akan berfungsi dengan benar tetapi SMBv1 klien Anda akan gagal terhubung ke saham SYSVOL dan NETLOGON dari pengontrol domain AWS Microsoft AD Terkelola Anda, dan juga tidak akan dapat memproses Kebijakan Grup.

SMBv1 klien akan bekerja dengan server file SMBv1 kompatibel lainnya yang Anda miliki. Namun, AWS merekomendasikan agar Anda memperbarui semua server dan klien SMB Anda ke SMBv2

atau yang lebih baru. [Untuk mempelajari selengkapnya tentang menonaktifkan SMBv1 dan memperbaruinya ke versi SMB yang lebih baru di sistem Anda, lihat postingan ini di Microsoft dan Dokumentasi. TechNet Microsoft](#)

Melacak Koneksi SMBv1 Jarak Jauh

Anda dapat meninjau log Peristiwa Microsoft Windows- SMBServer /Audit Windows dari jarak jauh yang menghubungkan ke pengontrol domain AWS Microsoft AD Terkelola, setiap peristiwa dalam log ini menunjukkan koneksi. SMBv1 Berikut adalah contoh informasi yang mungkin Anda lihat di salah satu log berikut:

SMB1 akses

Alamat Klien: ###.#####. ###

Bimbingan:

Peristiwa ini menunjukkan bahwa klien mencoba mengakses server menggunakan SMB1. Untuk menghentikan SMB1 akses audit, gunakan PowerShell cmdlet Set-. SmbServerConfiguration

Praktik terbaik saat memprogram aplikasi Anda untuk Microsoft AD yang AWS Dikelola

Sebelum Anda memprogram aplikasi agar berfungsi dengan Microsoft AD yang AWS Dikelola, pertimbangkan hal berikut:

Topik

- [Gunakan layanan pencari lokasi Windows DC](#)
- [Muat tes sebelum diluncurkan ke produksi](#)
- [Gunakan kueri LDAP yang efisien](#)

Gunakan layanan pencari lokasi Windows DC

Saat mengembangkan aplikasi, gunakan layanan pencari lokasi Windows DC atau gunakan layanan Dynamic DNS (DDNS) dari AWS Microsoft AD yang Dikelola untuk menemukan pengontrol domain (). DCs Jangan hard code aplikasi dengan alamat DC. Layanan locator DC membantu memastikan beban direktori didistribusikan dan memungkinkan Anda untuk mengambil keuntungan dari penskalaan horizontal dengan menambahkan pengendali domain untuk deployment Anda. Jika Anda mengikat aplikasi Anda ke DC tetap dan DC mengalami penambalan atau pemulihan, aplikasi

Anda akan kehilangan akses ke DC alih-alih menggunakan salah satu yang tersisa. DCs Selain itu, hard coding DC dapat mengakibatkan hot spotting pada DC tunggal. Pada kasus yang parah, hot spotting dapat menyebabkan DC Anda menjadi tidak responsif. Kasus seperti itu juga dapat menyebabkan otomatisasi AWS direktori menandai direktori sebagai terganggu dan dapat memicu proses pemulihan yang menggantikan DC yang tidak responsif.

Muat tes sebelum diluncurkan ke produksi

Pastikan untuk melakukan pengujian laboratorium dengan aplikasi dan permintaan yang mewakili beban kerja produksi Anda untuk mengonfirmasi bahwa direktori menskalakan ke beban aplikasi Anda. Jika Anda memerlukan kapasitas tambahan, uji dengan tambahan DCs saat mendistribusikan permintaan di antara. DCs Untuk informasi selengkapnya, lihat [Menerapkan pengontrol domain tambahan untuk AWS Microsoft AD yang Dikelola](#).

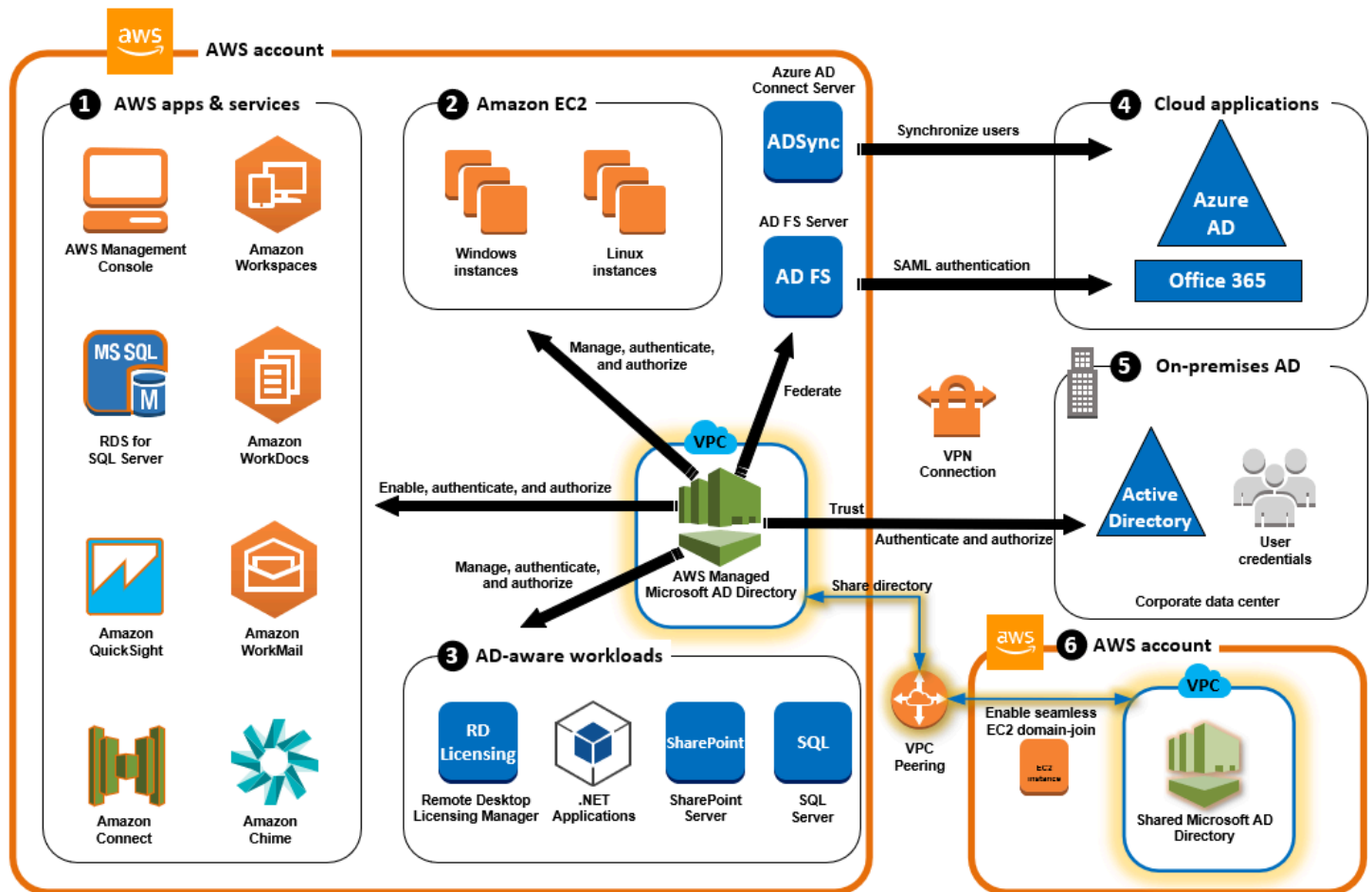
Gunakan kueri LDAP yang efisien

Kueri LDAP luas ke pengendali domain pada puluhan ribu objek dapat mengkonsumsi siklus CPU yang signifikan dalam DC tunggal, mengakibatkan hot spotting. Hal ini dapat mempengaruhi aplikasi yang berbagi DC yang sama selama kueri.

Kasus penggunaan untuk Microsoft AD yang AWS Dikelola

Dengan Microsoft AD yang AWS Dikelola, Anda dapat berbagi satu direktori untuk beberapa kasus penggunaan. Misalnya, Anda dapat berbagi direktori untuk mengautentikasi dan mengotorisasi akses untuk aplikasi .NET, [Amazon RDS for SQL Server](#) dengan [Autentikasi Windows](#) diaktifkan, dan [Amazon Chime](#) untuk olahpesan dan konferensi video.

Diagram berikut menunjukkan beberapa kasus penggunaan untuk direktori Microsoft AD AWS Terkelola Anda. Ini termasuk kemampuan untuk memberikan pengguna Anda akses ke aplikasi cloud eksternal dan memungkinkan pengguna Active Directory lokal untuk mengelola dan memiliki akses ke sumber daya di AWS Cloud.



Gunakan Microsoft AD yang AWS Dikelola untuk salah satu kasus penggunaan bisnis berikut.

Topik

- [Kasus Penggunaan 1: Masuk ke AWS aplikasi dan layanan dengan kredensial Active Directory](#)
- [Kasus Penggunaan 2: Mengelola instans Amazon EC2](#)
- [Kasus Penggunaan 3: Menyediakan layanan direktori ke beban kerja sadar Direktori Aktif Anda](#)
- [Kasus Penggunaan 4: AWS IAM Identity Center ke Office 365 dan aplikasi cloud lainnya](#)
- [Kasus Penggunaan 5: Perluas Direktori Aktif lokal Anda ke AWS Cloud](#)
- [Kasus Penggunaan 6: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 dengan mulus ke domain di seluruh akun AWS](#)

Kasus Penggunaan 1: Masuk ke AWS aplikasi dan layanan dengan kredensial Active Directory

Anda dapat mengaktifkan beberapa AWS aplikasi dan layanan seperti [AWS Client VPN](#), [Konsol Manajemen AWS](#), [Amazon Chime AWS IAM Identity Center](#), [Amazon Connect](#), [Amazon FSx](#), [Amazon RDS for SQL Server](#) [WorkDocs](#), WorkMail Amazon [WorkSpaces](#), dan menggunakan direktori AD Microsoft Terkelola AWS Anda. Ketika Anda mengaktifkan AWS aplikasi atau layanan di direktori Anda, pengguna Anda dapat mengakses aplikasi atau layanan dengan kredensi Direktori Aktif mereka.

Misalnya, Anda dapat mengaktifkan pengguna Anda [untuk masuk Konsol Manajemen AWS dengan kredensial Direktori Aktif mereka](#). Untuk melakukan ini, Anda mengaktifkan Konsol Manajemen AWS sebagai aplikasi di direktori Anda, dan kemudian menetapkan pengguna dan grup Direktori Aktif Anda ke peran IAM. Saat pengguna Anda masuk ke Konsol Manajemen AWS, mereka mengambil peran IAM untuk mengelola AWS sumber daya. Hal ini memudahkan Anda untuk memberikan pengguna Anda akses ke Konsol Manajemen AWS tanpa perlu mengkonfigurasi dan mengelola infrastruktur SAML yang terpisah.

Untuk lebih meningkatkan pengalaman pengguna akhir, Anda dapat mengaktifkan kemampuan [masuk tunggal](#) WorkDocs, yang memberi pengguna Anda kemampuan untuk mengakses WorkDocs dari komputer yang bergabung ke direktori tanpa harus memasukkan kredensialnya secara terpisah.

Anda dapat memberikan akses ke akun pengguna di direktori Anda atau di Active Directory lokal, sehingga mereka dapat masuk ke Konsol Manajemen AWS atau melalui AWS CLI menggunakan kredensial dan izin yang ada untuk mengelola AWS sumber daya dengan menetapkan peran IAM langsung ke akun pengguna yang ada.

FSx untuk integrasi Windows File Server dengan Microsoft AD yang AWS Dikelola

Mengintegrasikan FSx untuk Windows File Server dengan Microsoft AD yang AWS Dikelola menyediakan sistem file protokol Server Message Block (SMB) berbasis Microsoft Windows asli yang dikelola sepenuhnya yang memungkinkan Anda untuk dengan mudah memindahkan aplikasi dan klien berbasis Windows Anda (yang memanfaatkan penyimpanan file bersama) ke AWS. Meskipun FSx untuk Windows File Server dapat diintegrasikan dengan Microsoft Active Directory yang dikelola sendiri, kami tidak membahas skenario itu di sini.

Kasus FSx penggunaan dan sumber daya Amazon yang umum

Bagian ini memberikan referensi ke sumber daya umum FSx untuk integrasi Windows File Server dengan kasus penggunaan Microsoft AD yang AWS Dikelola. Setiap kasus penggunaan di bagian ini dimulai dengan konfigurasi Microsoft AD yang AWS dikelola dasar dan FSx untuk Windows File Server. Untuk informasi selengkapnya tentang cara membuat konfigurasi ini, lihat:

- [Memulai dengan Microsoft AD yang AWS Dikelola](#)
- [Memulai dengan Amazon FSx](#)

FSx untuk Windows File Server sebagai penyimpanan persisten pada wadah Windows

[Amazon Elastic Container Service \(ECS\)](#) mendukung kontainer Windows pada instans kontainer yang diluncurkan dengan Windows AMI yang dioptimalkan Amazon ECS. Instans kontainer Windows menggunakan versi dari agen kontainer Amazon ECS miliknya sendiri. Pada Windows AMI yang dioptimalkan Amazon ECS, agen kontainer Amazon ECS berjalan sebagai layanan pada host.

Amazon ECS mendukung autentikasi Direktori Aktif untuk kontainer Windows melalui akun layanan khusus yang disebut group Managed Service Account (gMSA). Karena kontainer Windows tidak dapat tergabung domain, Anda harus mengonfigurasi kontainer Windows untuk berjalan dengan gMSA.

Item Terkait

- [Menggunakan FSx untuk Windows File Server sebagai penyimpanan persisten pada Windows Container](#)
- [Akun Layanan Terkelola Grup](#)

Dukungan Amazon AppStream 2.0

[Amazon AppStream 2.0](#) adalah layanan streaming aplikasi yang dikelola sepenuhnya. Ini menyediakan berbagai solusi bagi pengguna untuk menyimpan dan mengakses data melalui aplikasi mereka. Amazon FSx dengan WorkSpaces Aplikasi menyediakan drive penyimpanan persisten pribadi menggunakan Amazon FSx dan dapat dikonfigurasi untuk menyediakan folder bersama untuk mengakses file umum.

Item Terkait

- [Panduan 4: Menggunakan Amazon dengan FSx Amazon 2.0 AppStream](#)

- [Menggunakan Amazon FSx dengan Amazon AppStream 2.0](#)
- [Menggunakan Active Directory dengan WorkSpaces Aplikasi](#)

Dukungan Microsoft SQL Server

FSx untuk Windows File Server dapat digunakan sebagai opsi penyimpanan untuk Microsoft SQL Server 2012 (dimulai dengan 2012 versi 11.x) dan database sistem yang lebih baru (termasuk Master, Model, MSDB, dan TempDB), dan untuk database pengguna Database Engine.

Item Terkait

- [Instal SQL Server dengan penyimpanan fileshare SMB](#)
- [Sederhanakan penerapan ketersediaan tinggi Microsoft SQL Server Anda menggunakan FSx Windows File Server](#)
- [Akun Layanan Terkelola Grup](#)

Folder rumah dan dukungan profil pengguna roaming

FSx untuk Windows File Server dapat digunakan untuk menyimpan data dari folder rumah pengguna Active Directory dan My Documents di lokasi pusat. FSx untuk Windows File Server juga dapat digunakan untuk menyimpan data dari Profil Pengguna Roaming.

Item terkait

- [Direktori rumah Windows menjadi mudah dengan Amazon FSx](#)
- [Menyebarkan profil pengguna roaming](#)
- [Menggunakan FSx untuk Windows File Server dengan WorkSpaces](#)

Dukungan berbagi file jaringan

FSx Berbagi file jaringan pada Windows File Server menyediakan solusi berbagi file yang dikelola dan dapat diskalakan. Satu kasus penggunaan dipetakan drive untuk klien yang dapat dibuat secara manual atau melalui Kebijakan Grup.

Item terkait

- [Walkthrough 6: Meningkatkan kinerja dengan Shards](#)
- [Pemetaan drive](#)

- [Menggunakan FSx untuk Windows File Server dengan WorkSpaces](#)

Dukungan instalasi perangkat lunak kebijakan grup

Karena ukuran dan performa folder SYSVOL terbatas, sebagai praktik terbaik harus, menghindari menyimpan data seperti file instalasi perangkat lunak dalam folder tersebut. Sebagai solusi yang mungkin untuk ini, FSx untuk Windows File Server dapat dikonfigurasi untuk menyimpan semua file perangkat lunak yang diinstal menggunakan Kebijakan Grup.

Item terkait

- [Gunakan Kebijakan Grup untuk menginstal perangkat lunak dari jarak jauh](#)

Dukungan target Backup Server Windows

FSx untuk Windows File Server dapat dikonfigurasi sebagai drive target di Windows Server Backup menggunakan berbagi file UNC. Dalam hal ini, Anda akan menentukan jalur UNC ke Server File Windows Anda FSx alih-alih ke volume EBS terlampir.

Item Terkait

- [Lakukan pemulihan status sistem server Anda](#)

Amazon FSx juga mendukung Berbagi Direktori Microsoft AD yang AWS Dikelola. Untuk informasi lebih lanjut, lihat:

- [Bagikan iklan Microsoft yang AWS Dikelola](#)
- [Menggunakan Amazon FSx dengan Microsoft AD yang AWS Dikelola di VPC atau akun yang berbeda](#)

Integrasi Amazon RDS dengan Microsoft AD yang AWS Dikelola

Amazon RDS mendukung autentikasi eksternal pengguna basis data menggunakan Kerberos dan Microsoft Active Directory. Kerberos adalah protokol autentikasi jaringan yang menggunakan tiket dan kriptografi kunci-simetris untuk menghilangkan kebutuhan untuk mentransmisikan kata sandi melalui jaringan. Dukungan Amazon RDS untuk Kerberos dan Direktori Aktif menyediakan keuntungan dari sign-on tunggal dan autentikasi terpusat dari pengguna basis data sehingga Anda dapat menyimpan kredensial pengguna Anda di Direktori Aktif.

Untuk memulai kasus penggunaan ini, Anda harus terlebih dahulu menyiapkan konfigurasi Microsoft AD dan Amazon RDS yang AWS Dikelola dasar.

- [Memulai dengan Microsoft AD yang AWS Dikelola](#)
- [Memulai dengan Amazon RDS](#)

Semua kasus penggunaan yang dirujuk di bawah ini akan dimulai dengan basis Microsoft AD dan Amazon RDS yang AWS dikelola dan mencakup cara mengintegrasikan Amazon RDS dengan AWS Microsoft AD yang Dikelola.

- [Menggunakan otentikasi Windows dengan instans Amazon RDS for SQL Server DB](#)
- [Menggunakan otentikasi Kerberos untuk MySQL](#)
- [Menggunakan otentikasi Kerberos dengan Amazon RDS for Oracle](#)
- [Menggunakan otentikasi Kerberos dengan Amazon RDS for PostgreSQL](#)

Amazon RDS juga mendukung Berbagi Direktori Microsoft AD yang AWS Dikelola. Untuk informasi lebih lanjut, lihat:

- [Bagikan iklan Microsoft yang AWS Dikelola](#)
- [Bergabung dengan instans Amazon RDS DB Anda di seluruh akun ke satu domain bersama](#)

Untuk informasi selengkapnya tentang menggabungkan Amazon RDS for SQL Server ke Active Directory, [lihat Bergabung dengan Amazon RDS for SQL Server](#) ke Active Directory yang dikelola sendiri.

Aplikasi .NET menggunakan Amazon RDS for SQL Server dengan Akun Layanan Terkelola grup

Anda dapat mengintegrasikan Amazon RDS for SQL Server dengan aplikasi.NET dasar dan grup Akun Layanan Terkelola (g). MSAs Untuk informasi selengkapnya, lihat [Cara Microsoft AD yang AWS Dikelola Membantu Menyederhanakan Penerapan dan Meningkatkan Keamanan Aplikasi .NET Terintegrasi Direktori Aktif](#)

Kasus Penggunaan 2: Mengelola instans Amazon EC2

Dengan menggunakan alat administrasi Direktori Aktif yang sudah dikenal, Anda dapat menerapkan objek kebijakan grup Active Directory (GPO) untuk mengelola instans Amazon EC2 untuk Windows

atau Linux secara terpusat [dengan menggabungkan instans ke domain Microsoft AD yang AWS Dikelola](#).

Selain itu, pengguna Anda dapat masuk ke instans Anda dengan kredensial Direktori Aktif mereka. Ini menghilangkan kebutuhan untuk menggunakan kredensial instans individu atau mendistribusikan file kunci pribadi (PEM). Ini memudahkan Anda untuk langsung memberikan atau mencabut akses ke pengguna dengan menggunakan alat administrasi pengguna Active Directory yang sudah Anda gunakan.

Kasus Penggunaan 3: Menyediakan layanan direktori ke beban kerja sadar Direktori Aktif Anda

AWS Microsoft AD yang dikelola adalah Microsoft Active Directory aktual yang memungkinkan Anda menjalankan beban kerja tradisional yang sadar Active Directory seperti [Remote Desktop Licensing Manager Microsoft](#) [SharePoint](#) dan [Microsoft SQL Server](#) Always On di Cloud. AWS AWS Microsoft AD yang dikelola juga membantu Anda menyederhanakan dan meningkatkan keamanan aplikasi.NET yang terintegrasi dengan Active Directory dengan menggunakan [grup Akun Layanan Terkelola \(gMSAs\)](#) dan [delegasi terbatas Kerberos \(KCD\)](#).

Kasus Penggunaan 4: AWS IAM Identity Center ke Office 365 dan aplikasi cloud lainnya

Anda dapat menggunakan Microsoft AD yang AWS Dikelola untuk menyediakan AWS IAM Identity Center layanan untuk aplikasi cloud. Anda dapat menggunakan Microsoft Entra Connect (sebelumnya dikenal sebagai Azure Active Directory Connect) untuk menyinkronkan pengguna Anda ke Microsoft Entra (sebelumnya dikenal sebagai Azure Active Directory (AzureAD)), dan kemudian menggunakan Active Directory Federation Services (AD FS) sehingga pengguna Anda dapat mengakses [Microsoft Office 365](#) dan aplikasi cloud SAMP 2.0 lainnya dengan menggunakan kredensial Active Directory mereka.

[Mengintegrasikan Microsoft AD AWS Terkelola dengan IAM Identity Center](#) menambahkan kemampuan SAMP ke AWS Microsoft AD dan/yang Dikelola atau domain tepercaya lokal Anda. Setelah terintegrasi, pengguna Anda dapat menggunakan IAM Identity Center dengan layanan yang mendukung SAMP, termasuk aplikasi cloud pihak ketiga Konsol Manajemen AWS dan pihak ketiga seperti Office 365, Concur, dan Salesforce tanpa harus mengonfigurasi infrastruktur SAMP. Untuk demonstrasi tentang proses mengizinkan pengguna lokal menggunakan Pusat Identitas IAM, lihat video berikut. YouTube

 Note

AWS Single Sign-On diubah namanya menjadi IAM Identity Center.

Kasus Penggunaan 5: Perluas Direktori Aktif lokal Anda ke AWS Cloud

Jika Anda sudah memiliki infrastruktur Direktori Aktif dan ingin menggunakannya saat memigrasikan beban kerja sadar Direktori Aktif ke, AWS Microsoft AD AWS Cloud Terkelola dapat membantu. Anda dapat menggunakan [trust Active Directory](#) untuk menghubungkan AD Microsoft AWS Terkelola ke Active Directory yang ada. Ini berarti pengguna Anda dapat mengakses Active Directory-aware dan AWS aplikasi dengan kredensial Active Directory lokal mereka, tanpa perlu Anda menyinkronkan pengguna, grup, atau kata sandi.

Misalnya, pengguna Anda dapat masuk ke Amazon Konsol Manajemen AWS dan Amazon WorkSpaces dengan menggunakan nama pengguna dan kata sandi Active Directory yang ada. Selain itu, saat Anda menggunakan aplikasi Active Directory-aware seperti dengan AWS Microsoft AD yang SharePoint Dikelola, Windows pengguna yang masuk dapat mengakses aplikasi ini tanpa perlu memasukkan kredensial lagi.

Anda juga dapat memigrasikan domain Active Directory lokal AWS agar bebas dari beban operasional infrastruktur Active Directory menggunakan Active [Directory Migration Toolkit \(ADMT\) bersama dengan Layanan Ekspor Kata Sandi \(PES\) untuk melakukan migrasi.](#)

Kasus Penggunaan 6: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 dengan mulus ke domain di seluruh akun AWS

Berbagi direktori Anda di beberapa AWS akun memungkinkan Anda mengelola AWS layanan seperti [Amazon EC2](#) dengan mudah tanpa perlu mengoperasikan direktori untuk setiap akun dan setiap VPC. Anda dapat menggunakan direktori Anda dari akun AWS mana pun dan dari [Amazon VPC](#) mana pun dalam Region AWS . Kemampuan ini membuatnya lebih mudah dan lebih hemat biaya untuk mengelola beban kerja sadar direktori dengan satu direktori di seluruh akun dan. VPCs Misalnya, Anda sekarang dapat mengelola [beban kerja Windows](#) yang diterapkan dalam instans EC2 di beberapa akun dan VPCs dengan mudah menggunakan satu direktori AWS Microsoft AD Terkelola.

Saat membagikan direktori Microsoft AD AWS Terkelola dengan AWS akun lain, Anda dapat menggunakan konsol Amazon EC2 atau [AWS Systems Manager](#) bergabung dengan instans Anda

dengan mulus dari VPC Amazon apa pun dalam akun dan Wilayah. AWS Anda dapat dengan cepat men-deploy beban kerja sadar direktori pada instans EC2 dengan menghilangkan kebutuhan untuk secara manual menggabungkan instans Anda ke domain atau untuk men-deploy direktori di setiap akun dan VPC. Untuk informasi selengkapnya, lihat [Bagikan iklan Microsoft yang AWS Dikelola](#).

Pertahankan Microsoft AD yang AWS Dikelola

Anda dapat menggunakan Konsol Manajemen AWS untuk mempertahankan iklan Microsoft yang AWS Dikelola dan menyelesaikan tugas day-to-day administratif. Cara Anda dapat mempertahankan direktori Anda meliputi:

- [Lihat detail direktori Microsoft AD AWS](#) untuk mempelajari jenis direktori Microsoft AD Terkelola, ID direktori, status direktori, dan detail jaringan seperti VPC Amazon, subnet, dan zona Ketersediaan.
- [Pulihkan iklan Microsoft AWS Terkelola Anda dengan snapshot](#). Anda juga dapat membuat snapshot dan menghapus snapshot.
- [Terapkan pengontrol domain tambahan](#) untuk meningkatkan kinerja dan ketersediaan AWS Microsoft AD Terkelola Anda.
- [Tingkatkan iklan Microsoft AWS Terkelola Anda](#) dari edisi Standar ke edisi Enterprise yang mendukung lebih banyak objek direktori.
- [Tambahkan nama utama pengguna alternatif \(UPN\)](#) untuk meningkatkan pengalaman login pengguna.
- [Ganti nama situs Microsoft AD AWS Terkelola](#) untuk meningkatkan kemampuan Microsoft AD AWS Terkelola untuk menemukan dan mengautentikasi pengguna Direktori Aktif yang ada di direktori lokal Anda.
- [Hapus iklan Microsoft yang AWS Dikelola](#) saat Anda tidak lagi membutuhkannya.

Melihat informasi direktori Microsoft AD yang AWS Dikelola

Anda dapat menggunakan Konsol Manajemen AWS untuk melihat detail direktori Microsoft AD AWS Terkelola seperti:

- Jenis direktori
- ID Direktori
- Status direktori

- Detail jaringan untuk iklan Microsoft AWS Terkelola Anda seperti:
 - Amazon VPC
 - Subnet
 - Zona ketersediaan
 - Alamat DNS

Anda dapat menemukan informasi berikut tentang Microsoft AD yang AWS Dikelola:

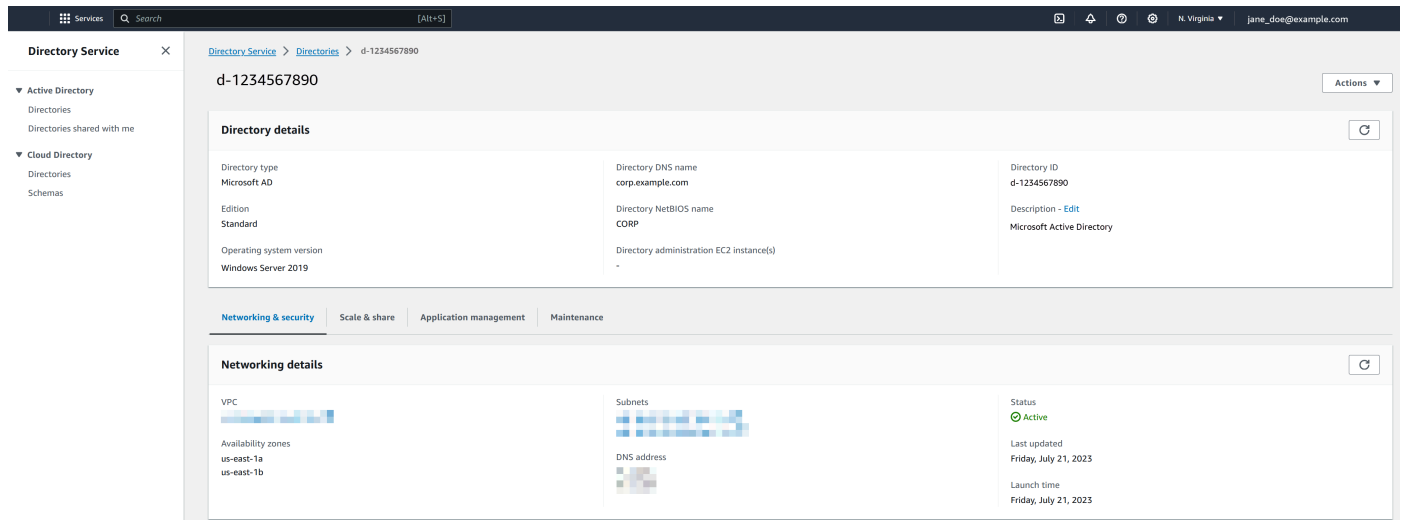
- Di bawah tab Bagikan & bagikan, Anda dapat membagikan iklan Microsoft AWS Terkelola dengan orang lain Akun AWS dan mempelajari detail jaringan untuk pengontrol domain Anda.
- Di bawah tab Manajemen aplikasi, Anda dapat mengaktifkan URL akses aplikasi untuk iklan Microsoft AWS Terkelola dan mengaktifkan AWS aplikasi dan layanan untuk iklan Microsoft yang AWS Dikelola.
- Di bawah tab Pemeliharaan, Anda dapat mengaktifkan Layanan Pemberitahuan Sederhana Amazon untuk menerima pemberitahuan status iklan Microsoft AWS Terkelola dan meninjau snapshot dari Microsoft AD yang AWS Dikelola.
- Untuk informasi selengkapnya tentang bidang Status, lihat [Memahami status direktori Microsoft AD yang AWS Dikelola](#).

Anda dapat melihat informasi direktori Microsoft AD yang AWS Dikelola menggunakan Konsol Manajemen AWS, AWS CLI, atau PowerShell:

Konsol Manajemen AWS

Untuk melihat informasi direktori terperinci.

1. Di panel navigasi [Konsol AWS Directory Service](#), di bawah Direktori Aktif, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda. Informasi tentang direktori ditampilkan dalam halaman Detail direktori.



AWS CLI

Untuk melihat informasi direktori terperinci dengan AWS CLI

- Buka AWS CLI. Untuk melihat informasi direktori Microsoft AD AWS Terkelola, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola:

```
aws ds describe-directories --directory-id d-1234567890 --output table
```

Untuk informasi selengkapnya, lihat [describe-directories](#).

PowerShell

Untuk melihat informasi direktori terperinci dengan PowerShell

- Buka PowerShell. Untuk melihat informasi direktori Microsoft AD AWS Terkelola, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola:

```
(Get-DSDirectory -DirectoryId d-1234567890 |  
  ForEach-Object {$_, $_.RegionsInfo, $_.VpcSettings}) |  
Format-List *
```

Lihat informasi yang lebih lengkap di [Get-DSDirectory](#).

Memulihkan iklan Microsoft AWS Terkelola Anda dengan snapshot

AWS Directory Service menyediakan snapshot harian otomatis dan kemampuan untuk mengambil snapshot manual data untuk Direktori Aktif AWS Microsoft AD Terkelola Anda. Snapshot ini dapat digunakan untuk melakukan point-in-time restore untuk Active Directory Anda. Anda dibatasi hingga lima snapshot manual untuk setiap Direktori Aktif Microsoft AD yang AWS Dikelola. Jika Anda telah mencapai batas ini, Anda harus menghapus salah satu snapshot manual yang ada sebelum Anda dapat membuat yang lain. Anda tidak dapat mengambil snapshot dari direktori AD Connector.

Note

Snapshot adalah fitur global dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [Konfigurasi replikasi Multi-Wilayah untuk AWS Microsoft AD yang Dikelola](#), prosedur berikut harus dilakukan di [Region primer](#). Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Topik

- [Membuat snapshot dari direktori Anda](#)
- [Memulihkan direktori Anda dari snapshot](#)
- [Menghapus snapshot](#)

Membuat snapshot dari direktori Anda

Snapshot dapat digunakan untuk memulihkan direktori Anda ke apa itu pada titik waktu yang snapshot diambil. Untuk membuat snapshot manual dari direktori Anda, lakukan langkah-langkah berikut.

Note

Anda dibatasi hingga 5 snapshot manual untuk setiap direktori. Jika Anda telah mencapai batas ini, Anda harus menghapus salah satu snapshot manual yang ada sebelum Anda dapat membuat yang lain.

Gunakan prosedur berikut untuk membuat snapshot manual dari Microsoft AD yang AWS Dikelola dengan Konsol Manajemen AWS, AWS CLI, atau PowerShell:

Konsol Manajemen AWS

Untuk membuat snapshot manual di Konsol Manajemen AWS

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih Tindakan, dan kemudian pilih Membuat snapshot.
5. Pada kotak dialog Membuat snapshot direktori, berikan nama untuk snapshot, jika diinginkan. Ketika siap, pilih Buat.

AWS CLI

Untuk membuat snapshot manual dengan AWS CLI

- Buka AWS CLI. Untuk membuat snapshot dari iklan Microsoft yang AWS Dikelola, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola:

```
aws ds create-snapshot --directory-id d-1234567890 --name ManualSnapshot
```

Untuk informasi selengkapnya, lihat [create-snapshot](#).

PowerShell

Untuk membuat snapshot manual dengan PowerShell

- Buka PowerShell. Untuk membuat snapshot dari iklan Microsoft yang AWS Dikelola, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola:

```
New-DSSnapshot -DirectoryId d-1234567890 -Name ManualSnapshot
```

Untuk informasi selengkapnya, lihat [New-DSSnapshot](#).

Tergantung pada ukuran direktori Anda, mungkin diperlukan beberapa menit untuk membuat snapshot. Ketika snapshot siap, nilai Status akan berubah menjadi Completed.

Memulihkan direktori Anda dari snapshot

Memulihkan direktori dari snapshot setara dengan memindahkan direktori kembali ke waktu dulu. Direktori snapshot unik untuk direktori tempat mereka dibuat. Snapshot hanya dapat dipulihkan ke direktori dari mana ia dibuat. Selain itu, usia maksimum yang didukung dari snapshot manual adalah 180 hari. Untuk informasi selengkapnya, lihat [Umur simpan yang berguna dari cadangan status sistem Active Directory di situs](#) web. Microsoft

Warning

Kami rekomendasikan Anda menghubungi [Pusat AWS Dukungan](#) sebelum pemulihan snapshot apa pun; kami mungkin dapat membantu Anda menghindari kebutuhan untuk melakukan pemulihan snapshot. Setiap pemulihan dari snapshot dapat mengakibatkan kehilangan data karena mereka adalah titik waktu. Penting Anda memahami bahwa semua server DNS DCs dan yang terkait dengan direktori akan offline sampai operasi pemulihan selesai.

Gunakan prosedur berikut untuk memulihkan direktori Anda dari snapshot menggunakan Konsol Manajemen AWS, AWS CLI, atau PowerShell:

Konsol Manajemen AWS

Untuk mengembalikan direktori dari snapshot di Konsol Manajemen AWS

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih snapshot dalam daftar, pilih Tindakan, dan kemudian pilih Memulihkan snapshot.
5. Tinjau informasi di kotak dialog Memulihkan snapshot direktori, dan pilih Pemulihan.

AWS CLI

Untuk mengembalikan direktori dari snapshot dengan AWS CLI

1. Buka AWS CLI. Untuk mencantumkan snapshot untuk iklan Microsoft AWS Terkelola, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola:

```
aws ds describe-snapshots --directory-id d-1234567890 \
  --query '(sort_by(Snapshots[*],
{ID:SnapshotId,Status:Status,Type:Type,StartTime:StartTime}, &StartTime))' \
  --output table
```

2. Untuk memulihkan iklan Microsoft AWS Terkelola dari snapshot, Anda dapat menggunakan [restore-from-snapshot](#) perintah. Pastikan Anda mengganti snapshot-id parameter dengan ID snapshot yang ingin Anda gunakan untuk memulihkan iklan Microsoft AWS Terkelola:

```
aws ds restore-from-snapshot --snapshot-id s-1234567890
```

PowerShell

Untuk mengembalikan direktori dari snapshot dengan PowerShell

1. Buka PowerShell. Untuk mencantumkan snapshot untuk iklan Microsoft AWS Terkelola, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola:

```
Get-DSSnapshot -DirectoryId d-1234567890 | Sort-Object StartTime | Format-Table
```

2. Untuk memulihkan iklan Microsoft AWS Terkelola dari snapshot, Anda dapat menggunakan [Restore-DSFromSnapshot](#) perintah. Pastikan Anda mengganti snapshot-id parameter dengan ID snapshot yang ingin Anda gunakan untuk memulihkan iklan Microsoft AWS Terkelola:

```
Restore-DSFromSnapshot -SnapshotId s-1234567890
```

Untuk direktori Microsoft AD yang AWS Dikelola, diperlukan waktu dua hingga tiga jam agar direktori dipulihkan. Ketika berhasil dipulihkan, nilai Status direktori berubah menjadi *Active*. Setiap perubahan yang dibuat ke direktori setelah tanggal snapshot akan ditimpa.

Menghapus snapshot

Gunakan prosedur berikut untuk menghapus snapshot iklan Microsoft AWS Terkelola Anda dengan Konsol Manajemen AWS, AWS CLI, atau PowerShell:

Konsol Manajemen AWS

Untuk menghapus snapshot di Konsol Manajemen AWS

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih Tindakan, dan kemudian pilih Hapus snapshot.
5. Verifikasi bahwa Anda ingin menghapus snapshot tersebut, lalu pilih Hapus.

AWS CLI

Untuk menghapus snapshot dengan AWS CLI

1. Buka AWS CLI. Untuk mencantumkan snapshot untuk iklan Microsoft AWS Terkelola, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola:

```
aws ds describe-snapshots --directory-id d-1234567890 \  
  --query '(sort_by(Snapshots[*].  
{ID:SnapshotId,Status:Status,Type:Type,StartTime:StartTime}, &StartTime))' \  
  --output table
```

2. Untuk menghapus snapshot dari iklan Microsoft yang AWS Dikelola, Anda dapat menggunakan [delete-snapshot](#) perintah tersebut. Pastikan Anda mengganti snapshot-id parameter dengan ID snapshot dari snapshot yang ingin Anda hapus:

```
aws ds delete-snapshot --snapshot-id s-1234567890
```

PowerShell

Untuk menghapus snapshot dengan PowerShell

1. Buka PowerShell. Untuk mencantumkan snapshot untuk iklan Microsoft AWS Terkelola, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola:

```
Get-DSSnapshot -DirectoryId d-1234567890 | Sort-Object StartTime | Format-Table
```

2. Untuk memulihkan iklan Microsoft AWS Terkelola dari snapshot, Anda dapat menggunakan [Remove-DSnapshot](#) perintah. Pastikan Anda mengganti `snapshot-id` parameter dengan ID snapshot dari snapshot yang ingin Anda hapus:

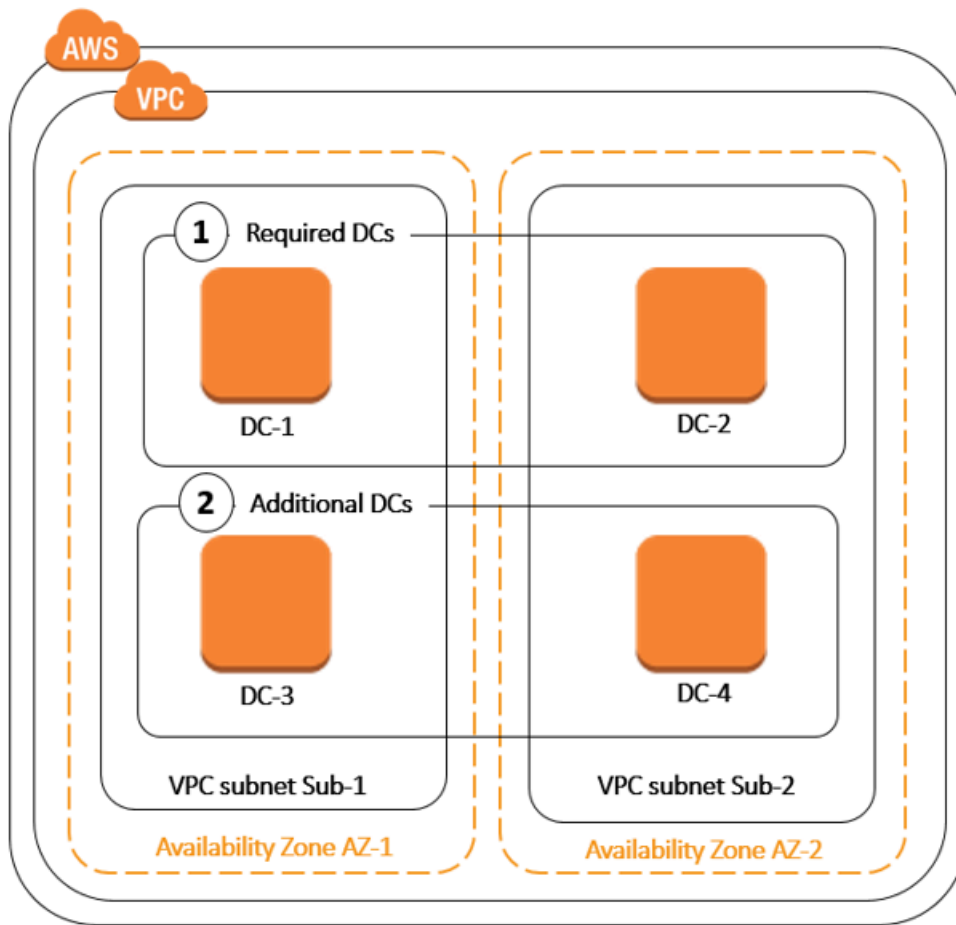
```
Remove-DSSnapshot -SnapshotId s-1234567890
```

Menerapkan pengontrol domain tambahan untuk AWS Microsoft AD yang Dikelola

Menerapkan pengontrol domain tambahan untuk AWS Microsoft AD Terkelola meningkatkan redundansi, yang menghasilkan ketahanan yang lebih besar dan ketersediaan yang lebih tinggi. Hal ini juga meningkatkan performa direktori Anda dengan mendukung lebih banyak permintaan Direktori Aktif. Misalnya, Anda sekarang dapat menggunakan Microsoft AD yang AWS Dikelola untuk mendukung beberapa aplikasi.NET yang digunakan pada armada besar Amazon EC2 dan Amazon RDS for SQL Server instans.

Saat pertama kali membuat direktori, Microsoft AD AWS Terkelola akan menerapkan dua pengontrol domain di beberapa Availability Zone, yang diperlukan untuk tujuan ketersediaan tinggi. Kemudian, Anda dapat dengan mudah menerapkan pengontrol domain tambahan melalui Directory Service konsol hanya dengan menentukan jumlah total pengontrol domain yang Anda inginkan. AWS Microsoft AD yang dikelola mendistribusikan pengontrol domain tambahan ke Availability Zones dan subnet Amazon VPC tempat direktori Anda berjalan.

Misalnya, dalam ilustrasi di bawah ini, DC-1 dan DC-2 mewakili dua pengendali domain yang awalnya dibuat dengan direktori Anda. Directory Service Konsol mengacu pada pengontrol domain default ini sebagai Diperlukan. AWS Microsoft AD yang dikelola dengan sengaja menempatkan masing-masing pengontrol domain ini di Availability Zone terpisah selama proses pembuatan direktori. Kemudian, Anda mungkin memutuskan untuk menambahkan dua pengontrol domain lagi untuk membantu mendistribusikan beban autentikasi selama waktu masuk puncak. DC-3 dan DC-4 mewakili pengendali domain baru, yang di mana konsol tersebut sekarang mengacu sebagai Tambahan. Seperti sebelumnya, Microsoft AD yang AWS Dikelola kembali secara otomatis menempatkan pengontrol domain baru di Availability Zone yang berbeda untuk memastikan ketersediaan domain Anda yang tinggi.



Proses ini menghilangkan kebutuhan Anda untuk secara manual mengkonfigurasi direktori data replikasi, snapshot harian otomatis, atau pemantauan untuk pengendali domain tambahan. Ini juga lebih mudah bagi Anda untuk bermigrasi dan menjalankan Direktori Aktif penting misi — beban kerja terintegrasi di dalam AWS Cloud tanpa harus menerapkan dan memelihara infrastruktur Direktori Aktif Anda sendiri.

Anda dapat menggunakan salah satu alat berikut untuk menyebarkan atau menghapus pengontrol domain tambahan ke AWS Microsoft AD yang Dikelola:

- [update-number-of-domain-controllers](#) AWS CLI perintah
- API [UpdateNumberOfDomainControllers](#)
- [Menambahkan atau menghapus pengontrol domain tambahan dengan Konsol Manajemen AWS](#)

 Note

Pengontrol domain tambahan adalah fitur Regional dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [replikasi Multi-Region](#), prosedur berikut harus diterapkan secara terpisah di setiap Wilayah. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Menambahkan atau menghapus pengontrol domain tambahan dengan Konsol Manajemen AWS

Anda dapat menggunakan Konsol Manajemen AWS untuk menambah atau menghapus pengontrol domain tambahan ke Microsoft AD yang AWS Dikelola.

Prasyarat

Sebelum menambahkan atau menghapus pengontrol domain tambahan ke Microsoft AD yang AWS Dikelola, berikut informasi selengkapnya tentang persyaratan pengontrol domain:

- Setelah men-deploy pengendali domain tambahan, Anda dapat mengurangi jumlah pengendali domain hingga dua, yang merupakan minimum yang diperlukan untuk toleransi kesalahan dan tujuan ketersediaan tinggi.
- Pengontrol domain yang dihapus akan dihapus dari daftar pengontrol domain tambahan. Pengontrol domain primer dan sekunder diperlukan dan tidak dapat dihapus.
- Jika Anda telah mengonfigurasi iklan Microsoft AWS Terkelola untuk mengaktifkan LDAPS, pengontrol domain tambahan apa pun yang Anda tambahkan juga akan mengaktifkan LDAPS secara otomatis. Untuk informasi selengkapnya, lihat [Aktifkan LDAP Aman atau LDAPS](#).

Prosedur

Gunakan prosedur berikut untuk menerapkan atau menghapus pengontrol domain tambahan di AWS Microsoft AD Terkelola Anda dengan Konsol Manajemen AWS, AWS CLI, atau PowerShell

Konsol Manajemen AWS

Untuk menambah atau menghapus pengontrol domain tambahan dengan Konsol Manajemen AWS

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.

2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menambahkan menghapus pengendali domain, lalu pilih tab Menskalakan & bagikan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Menskalakan & bagikan.
4. Di bagian Pengendali Domain, pilih Edit.
5. Tentukan jumlah pengendali domain untuk menambah atau menghapus dari direktori Anda, dan kemudian pilih Modifikasi.
6. Saat Microsoft AD yang AWS Dikelola menyelesaikan proses penerapan, semua pengontrol domain menampilkan status Aktif, dan subnet Availability Zone dan Amazon VPC yang ditetapkan akan muncul. Pengendali domain baru sama-sama didistribusikan di Availability Zone dan subnet di mana direktori Anda sudah di-deploy.

AWS CLI

Untuk menambah atau menghapus pengontrol domain tambahan dengan AWS CLI

1. Buka AWS CLI. Untuk memeriksa jumlah pengontrol domain saat ini, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola Anda:

```
aws ds describe-directories --directory-id d-1234567890 | grep  
DesiredNumberOfDomainControllers
```

2. Untuk menambah atau menghapus pengontrol domain, Anda dapat menggunakan [update-number-of-domain-controllers](#) perintah. Misalnya, Anda dapat menggunakan perintah berikut untuk mengatur jumlah total pengontrol domain menjadi 4. Pastikan Anda mengganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola dan `desired-number` parameternya dengan jumlah pengontrol domain yang ingin Anda gunakan.

```
aws ds update-number-of-domain-controllers --directory-id d-1234567890 --  
desired-number 4
```


PowerShell

Untuk menambah atau menghapus pengontrol domain tambahan dengan PowerShell

1. Buka PowerShell. Untuk memeriksa jumlah pengontrol domain saat ini, jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola Anda:

```
Get-DSDirectory -DirectoryId d-1234567890 | Select-Object  
DesiredNumberOfDomainControllers
```

2. Untuk menambah atau menghapus pengontrol domain, Anda dapat menggunakan [Set-DSDomainControllerCount](#) perintah. Misalnya, Anda dapat menggunakan perintah berikut untuk mengatur jumlah total pengontrol domain menjadi 4. Pastikan Anda mengganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola dan DesiredNumber parameternya dengan jumlah pengontrol domain yang ingin Anda gunakan.

```
Set-DSDomainControllerCount -DirectoryId d-1234567890 -DesiredNumber 4
```

Artikel Blog AWS Keamanan Terkait

- [Cara meningkatkan redundansi dan kinerja Anda Directory Service untuk AWS Microsoft AD yang Dikelola dengan menambahkan pengontrol domain](#)

Memutakhirkan Microsoft AD yang AWS Dikelola

Anda dapat memutakhirkan edisi Standar Microsoft AD AWS Terkelola ke edisi Enterprise. Berikut ini menguraikan perbedaan antara edisi Standar dan Perusahaan:

- Edisi Standar: Microsoft AD yang Dikelola AWS (Edisi Standar) dioptimalkan untuk menjadi direktori primer untuk bisnis kecil dan menengah sampai dengan 5.000 karyawan. Ini menyediakan kapasitas penyimpanan yang cukup untuk mendukung hingga 30.000* objek direktori, seperti pengguna, grup, dan komputer.
- Edisi Enterprise: Microsoft AD yang Dikelola AWS (Edisi Enterprise) dirancang untuk mendukung organisasi korporasi dengan hingga 500.000* direktori objek.

* batas atas adalah perkiraan. Direktori Anda mungkin mendukung lebih atau kurang objek direktori tergantung pada ukuran objek Anda dan perilaku dan kebutuhan performa aplikasi Anda.

Untuk memutakhirkan edisi Standar Microsoft AD AWS Terkelola ke edisi Enterprise, gunakan [UpdateDirectorySetup](#) dari API, [update-directory-setup](#) dari AWS CLI, atau [Perbarui- DSDirectory Pengaturan](#) dari AWS Tools for PowerShell.

API

Untuk memutakhirkan edisi Standar Microsoft AD AWS Terkelola ke edisi Enterprise:

```
{
  "DirectoryId": "d-1234567890",
  "UpdateType": "SIZE",
  "DirectorySizeUpdateSettings": {
    "DirectorySize": "Large"
  }
}
```

AWS CLI

Untuk memutakhirkan edisi Standar Microsoft AD AWS Terkelola ke edisi Enterprise:

```
aws ds update-directory-setup \
  --directory-id d-1234567890 \
  --update-type SIZE \
  --directory-size-update-settings DirectorySize=Large
```

PowerShell

Untuk memutakhirkan edisi Standar Microsoft AD AWS Terkelola ke edisi Enterprise:

```
Update-DSDirectorySetup `
  -DirectoryId d-9a676e4148 `
  -UpdateType SIZE `
  -DirectorySizeUpdateSettings_DirectorySize Large
```

Ada beberapa batasan yang harus diperhatikan saat memutakhirkan iklan Microsoft AWS Terkelola Anda. File tersebut adalah:

- Upgrade akan dikenakan biaya tambahan. Lihat [Directory Service Harga](#) untuk informasi lebih lanjut.
- Setelah Active Directory Anda ditingkatkan, itu tidak dapat dikembalikan ke edisi sebelumnya.

- Snapshot sebelumnya tidak dapat digunakan untuk memulihkan Direktori Aktif setelah ditingkatkan.
- Proses upgrade membutuhkan empat hingga lima jam.
- Selama proses pemutakhiran, pengontrol domain iklan Microsoft AWS Terkelola Anda ditingkatkan satu per satu. Hal ini dapat berdampak negatif pada kinerja Anda dan dapat menyebabkan downtime selama jendela pemeliharaan Anda.
- Proses upgrade akan mengubah nama host dari setiap instance pengontrol domain, tetapi alamat IP mereka akan tetap sama.
- Jika Anda menggunakan LDAPS (Lightweight Directory Access Protocol over SSL), pengontrol domain akan memerlukan sertifikat baru.

Memperbarui jenis jaringan direktori

Anda dapat memperbarui jenis jaringan Directory Service direktori Anda dari IPv4 ke Dual-stack (IPv4 dan IPv6). Memperbarui jenis jaringan untuk menyertakan alamat IPv6 IP menyediakan ruang alamat yang lebih besar daripada IPv4. IPv4 dan IPv6 komunikasi independen satu sama lain.

Untuk detailnya, lihat [Bandingkan IPv4 dan IPv6](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Important

Ini adalah operasi satu arah yang tidak dapat dibalik. Uji di lingkungan non-produksi terlebih dahulu.

Prasyarat

Sebelum memperbarui jenis jaringan direktori Anda, pastikan persyaratan berikut terpenuhi:

- VPC Anda dan subnet terkait di mana direktori Anda saat ini ada harus dikonfigurasi dengan IPv6 rentang CIDR. Untuk detailnya, lihat [IPv6 dukungan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.
- Anda memiliki akses administratif ke Konsol Manajemen AWS.
- Direktori Anda harus dalam status Aktif.
- Anda memiliki izin IAM yang sesuai untuk mengubah Directory Service pengaturan.

Untuk memperbarui jenis jaringan direktori

Untuk memperbarui direktori Anda ke jaringan dual-stack

Note

Jika direktori Anda direplikasi di beberapa wilayah, lakukan pembaruan ini di setiap wilayah.

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih direktori target.
3. Buka tab Jaringan & Keamanan.
4. Pilih Tambahkan IPv6 dukungan. Opsi ini hanya tersedia untuk direktori IPv4 -only.
5. Tinjau informasi pembaruan dan detail harga.
6. Pilih Tambah untuk mengonfirmasi pembaruan.

Setelah memulai pembaruan, status direktori berubah menjadi Memperbarui selama proses pembaruan. Pembaruan biasanya membutuhkan waktu 15-30 menit untuk diselesaikan. Setelah selesai, status direktori kembali ke Aktif.

Menambahkan sufiks UPN alternatif ke Microsoft AD yang Dikelola AWS

Anda dapat menyederhanakan pengelolaan nama login Active Directory (AD) dan meningkatkan pengalaman login pengguna dengan menambahkan akhiran nama utama pengguna (UPN) alternatif ke direktori AWS Microsoft AD Terkelola Anda. Untuk melakukan itu, Anda harus masuk dengan akun Admin atau dengan akun yang merupakan anggota dari grup Administrator Akhiran Nama Dasar Pengguna yang Didelegasikan AWS. Untuk informasi selengkapnya tentang grup ini, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).

Untuk menambahkan akhiran UPN alternatif

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Temukan EC2 instans Amazon yang digabungkan ke direktori AD Microsoft AWS Terkelola Anda. Pilih instans, lalu pilih Hubungkan.
3. Di jendela Pengelola Server, pilih Alat. Lalu pilih Domain Direktori Aktif dan Kepercayaan.
4. Di panel sebelah kiri, klik kanan Domain Direktori Aktif dan Kepercayaan lalu pilih Properti.

5. Di tab Akhiran UPN, ketik alternatif akhiran UPN (seperti **sales.example.com**). Pilih Tambahkan , lalu pilih Terapkan .
6. Jika Anda perlu menambahkan akhiran UPN alternatif tambahan, ulangi langkah 5 sampai Anda memiliki akhiran UPN yang Anda butuhkan.

Mengganti nama situs direktori Microsoft AD yang AWS Dikelola

Anda dapat mengganti nama situs default direktori Microsoft AD yang AWS Dikelola sehingga cocok dengan nama situs Microsoft Active Directory (AD) yang ada. Hal ini mempercepat Microsoft AD yang AWS Dikelola untuk menemukan dan mengautentikasi pengguna AD yang ada di direktori lokal. Hasilnya adalah pengalaman yang lebih baik ketika pengguna masuk ke AWS sumber daya seperti [Amazon EC2 dan Amazon RDS for SQL](#) Server instance yang telah Anda gabungkan ke direktori Microsoft AD AWS Terkelola.

Untuk melakukan itu, Anda harus masuk dengan akun Admin atau dengan akun yang merupakan anggota dari grup Administrator Situs dan Layanan yang Didelegasikan AWS . Untuk informasi selengkapnya tentang grup ini, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).

Untuk manfaat tambahan dari mengubah nama situs Anda dalam kaitannya dengan kepercayaan, lihat [Domain Locator di Kepercayaan Forest](#) di situs web Microsoft.

Untuk mengganti nama situs Microsoft AD yang AWS Dikelola

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Temukan EC2 instans Amazon yang digabungkan ke direktori AD Microsoft AWS Terkelola Anda. Pilih instans, lalu pilih Hubungkan.
3. Di jendela Pengelola Server, pilih Alat. Lalu pilih Situs dan Layanan Direktori Aktif.
4. Di panel sebelah kiri, perluas folder Situs, klik kanan nama situs (default adalah Default-Situs-Nama), lalu pilih Mengubah nama.
5. Ketik nama situs baru, dan kemudian pilih Masukkan.

Menghapus iklan Microsoft yang AWS Dikelola

Ketika direktori Microsoft AD, Simple AD, atau hybrid AWS terkelola dihapus, semua data direktori dan snapshot dihapus dan tidak dapat dipulihkan. Setelah direktori dihapus, semua instans yang bergabung ke direktori tetap utuh. Anda tidak dapat, bagaimanapun, menggunakan kredensial

direktori Anda untuk masuk ke instans ini. Anda harus log in ke instans ini dengan akun pengguna yang lokal untuk instans.

Saat Konektor AD dihapus, direktori lokal Anda tetap utuh. Semua instans yang bergabung ke direktori juga tetap utuh dan tetap bergabung ke direktori on-premise Anda. Anda masih bisa menggunakan kredensial direktori Anda untuk masuk ke instans ini.

Untuk menghapus direktori

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori. Pastikan Anda berada di AWS Region tempat Active Directory Anda digunakan. Untuk informasi selengkapnya, lihat [Memilih Wilayah](#).
2. Pastikan tidak ada AWS aplikasi yang diaktifkan untuk direktori yang ingin Anda hapus. AWS Aplikasi yang diaktifkan akan mencegah Anda menghapus iklan Microsoft AWS Terkelola atau Simple AD Anda.
 - a. Pada halaman Direktori, pilih ID direktori Anda.
 - b. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi. Di bagian AWS aplikasi & layanan, Anda melihat AWS aplikasi mana yang diaktifkan untuk direktori Anda.
 - Nonaktifkan Konsol Manajemen AWS akses. Untuk informasi selengkapnya, lihat [Menonaktifkan akses Konsol Manajemen AWS](#).
 - Untuk menonaktifkan Amazon WorkSpaces, Anda harus membatalkan pendaftaran layanan dari direktori di konsol. WorkSpaces Untuk informasi selengkapnya, lihat [Menghapus direktori](#) di Panduan WorkSpaces Administrasi Amazon.
 - Untuk menonaktifkan WorkDocs, Anda harus menghapus WorkDocs situs di WorkDocs konsol. Untuk informasi selengkapnya, lihat [Menghapus situs](#) di Panduan WorkDocs Administrasi Amazon.
 - Untuk menonaktifkan Amazon WorkMail, Anda harus menghapus WorkMail organisasi Amazon di WorkMail konsol Amazon. Untuk informasi selengkapnya, lihat [Menghapus organisasi](#) di Panduan WorkMail Administrator Amazon.
 - Untuk menonaktifkan Amazon FSx untuk Windows File Server, Anda harus menghapus sistem FSx file Amazon dari domain. Untuk informasi selengkapnya, lihat [Bekerja dengan Active Directory FSx untuk Windows File Server](#) di Amazon FSx untuk Windows File Server User Guide.

- Untuk menonaktifkan Amazon Relational Database Service, Anda harus menghapus instans Amazon RDS dari domain. Untuk informasi selengkapnya, lihat [Mengelola instans DB dalam domain](#) dalam Panduan Pengguna Amazon RDS.
- Untuk menonaktifkan AWS Client VPN Layanan, Anda harus menghapus layanan direktori dari Endpoint Client VPN. Untuk informasi selengkapnya, lihat [Bekerja dengan Client VPN](#) di Panduan AWS Client VPN Administrator.
- Untuk menonaktifkan Amazon Connect, Anda harus menghapus Instans Amazon Connect. Untuk informasi selengkapnya, lihat [Menghapus instans Amazon Connect](#) di Panduan Administrasi Amazon Connect.
- Untuk menonaktifkan Amazon Quick, Anda harus berhenti berlangganan Amazon Quick. Untuk informasi selengkapnya, lihat [Menutup Amazon Quick akun Anda](#) di Panduan Pengguna Cepat Amazon.

 Note

Jika Anda menggunakan AWS IAM Identity Center dan sebelumnya telah menghubungkannya ke direktori Microsoft AD AWS Terkelola yang ingin Anda hapus, Anda harus terlebih dahulu mengubah sumber identitas sebelum dapat menghapusnya. Untuk informasi selengkapnya, lihat [Mengubah sumber identitas Anda](#) di Panduan Pengguna Pusat Identitas IAM.

3. Di panel navigasi, pilih Direktori.
4. Pilih hanya direktori yang akan dihapus dan klik Hapus. Ini akan memerlukan beberapa menit agar direktori dihapus. Ketika direktori telah dihapus, itu akan dihapus dari daftar direktori Anda.

Amankan Microsoft AD yang AWS Dikelola

Anda dapat menggunakan kebijakan kata sandi, fitur seperti otentikasi multi-faktor (MFA), dan pengaturan untuk mengamankan iklan Microsoft yang Dikelola AWS . Cara Anda dapat mengamankan direktori Anda meliputi:

- [Pahami cara kerja kebijakan kata sandi di Active Directory](#) sehingga dapat diterapkan ke pengguna Microsoft AD yang AWS Dikelola. Anda juga dapat mendelegasikan pengguna mana yang dapat mengelola kebijakan kata sandi Microsoft AD AWS Terkelola Anda.
- [Aktifkan MFA](#) yang meningkatkan keamanan AWS Microsoft AD Terkelola Anda.

- [> Aktifkan Protokol Akses Direktori Ringan melalui Secure Socket Layer \(SSL\) /Transport Layer Security \(TLS\) \(LDAPS\)](#) sehingga komunikasi melalui LDAP dienkripsi dan meningkatkan keamanan.
- [Kelola kepatuhan Microsoft AD AWS Terkelola Anda](#) dengan standar seperti Federal Risk and Authorization Management Program (FedRAMP) dan Payment Card Industry (PCI) Data Security Standard (DSS).
- [Tingkatkan konfigurasi keamanan jaringan Microsoft AD AWS Terkelola Anda](#) dengan memodifikasi Grup AWS Keamanan untuk memenuhi kebutuhan lingkungan Anda.
- [Edit pengaturan keamanan direktori Microsoft AD AWS Terkelola Anda](#) seperti Otentikasi Basis Sertifikat, Cipher Saluran Aman, dan Protokol untuk memenuhi kebutuhan Anda.
- [Siapkan AWS Private Certificate Authority Konektor untuk AD](#) sehingga Anda dapat menerbitkan dan mengelola sertifikat untuk Microsoft AD yang AWS Dikelola AWS Private CA.

Memahami kebijakan kata sandi Microsoft AD yang AWS Dikelola

AWS Microsoft AD yang dikelola memungkinkan Anda menentukan dan menetapkan kebijakan penguncian kata sandi dan akun yang berbeda (juga disebut sebagai [kebijakan kata sandi berbutir halus](#)) untuk grup pengguna yang Anda kelola di domain Microsoft AD Terkelola AWS . Saat Anda membuat direktori Microsoft AD AWS Terkelola, kebijakan domain default dibuat dan diterapkan ke Direktori Aktif. Kebijakan ini mencakup pengaturan berikut:

Kebijakan	Pengaturan
Memberlakukan riwayat kata sandi	24 kata sandi diingat
Usia kata sandi maksimal	42 hari *
Usia kata sandi minimum	1 hari
Panjang kata sandi minimum	7 karakter
Kata sandi harus memenuhi persyaratan kompleksitas	Diaktifkan
Menyimpan kata sandi menggunakan enkripsi reversibel	Nonaktif

Note

* Usia kata sandi maksimum 42 hari termasuk kata sandi admin.

Misalnya, Anda dapat menetapkan pengaturan kebijakan yang kurang ketat untuk karyawan yang memiliki akses ke informasi sensitivitas rendah saja. Untuk manajer senior yang secara teratur mengakses informasi rahasia Anda dapat menerapkan pengaturan yang lebih ketat.

Sumber daya berikut memberikan informasi lebih lanjut tentang kebijakan kata sandi dan kebijakan keamanan berbutir halus Microsoft Active Directory:

- [Konfigurasi setelan kebijakan keamanan](#)
- [Persyaratan kompleksitas kata sandi](#)
- [Pertimbangan keamanan kompleksitas kata sandi](#)

AWS menyediakan serangkaian kebijakan kata sandi berbutir halus di AWS Microsoft AD Terkelola yang dapat Anda konfigurasi dan tetapkan ke grup Anda. Untuk mengonfigurasi kebijakan, Anda dapat menggunakan alat Microsoft kebijakan standar seperti [Pusat Administrasi Direktori Aktif](#). Untuk memulai dengan alat Microsoft kebijakan, lihat [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#).

Bagaimana kebijakan kata sandi diterapkan

Ada perbedaan dalam bagaimana kebijakan kata sandi berbutir halus diterapkan tergantung pada apakah kata sandi disetel ulang atau diubah. Pengguna domain dapat mengubah kata sandi mereka sendiri. Administrator Active Directory atau pengguna dengan izin yang diperlukan dapat [mengatur ulang kata sandi pengguna](#). Lihat bagan berikut untuk informasi lebih lanjut.

Kebijakan	Reset Kata Sandi	Perubahan Kata Sandi
Memberlakukan riwayat kata sandi	 Tida	 Ya

Kebijakan	Reset Kata Sandi	Perubahan Kata Sandi
Usia kata sandi maksimal	 Ya	 Ya
Usia kata sandi minimum	 Tida	 Ya
Panjang kata sandi minimum	 Ya	 Ya
Kata sandi harus memenuhi persyaratan kompleksitas	 Ya	 Ya

Perbedaan-perbedaan ini memiliki implikasi keamanan. Misalnya, setiap kali kata sandi pengguna disetel ulang, riwayat penegakan kata sandi dan kebijakan usia kata sandi minimum tidak diberlakukan. Untuk informasi selengkapnya, lihat dokumentasi Microsoft tentang pertimbangan keamanan yang terkait dengan [menerapkan riwayat kata sandi dan kebijakan usia kata sandi minimum](#).

Pengaturan kebijakan yang didukung

AWS Microsoft AD yang dikelola mencakup lima kebijakan berbutir halus dengan nilai prioritas yang tidak dapat diedit. Kebijakan memiliki sejumlah properti yang dapat Anda konfigurasi untuk memberlakukan kekuatan kata sandi, dan tindakan penguncian akun jika terjadi peristiwa kegagalan login. Anda dapat menetapkan kebijakan ke nol atau lebih grup Direktori Aktif. Jika pengguna akhir adalah anggota dari beberapa grup dan menerima lebih dari satu kebijakan kata sandi, Direktori Aktif memberlakukan kebijakan dengan nilai prioritas terendah.

AWS kebijakan kata sandi yang telah ditentukan sebelumnya

Tabel berikut mencantumkan lima kebijakan yang disertakan dalam direktori AD Microsoft AWS Terkelola dan nilai prioritas yang ditetapkan. Untuk informasi selengkapnya, lihat [Precedence](#).

Nama kebijakan	Precedence
PelangganPSO-01	10
PelangganPSO-02	20
PelangganPSO-03	30
PelangganPSO-04	40
PelangganPSO-05	50

Properti kebijakan kata sandi

Anda dapat mengedit properti berikut dalam kebijakan kata sandi agar sesuai dengan standar kepatuhan yang memenuhi kebutuhan bisnis Anda.

- Nama kebijakan
- [Menegakkan riwayat kata sandi](#)
- [Panjang kata sandi minimum](#)
- [Usia kata sandi minimum](#)
- [Usia kata sandi maksimum](#)
- [Simpan kata sandi menggunakan enkripsi yang dapat dibalik](#)
- [Kata sandi harus memenuhi persyaratan kompleksitas](#)

Anda tidak dapat mengubah nilai prioritas untuk kebijakan ini. Untuk detail selengkapnya tentang bagaimana pengaturan ini memengaruhi penegakan kata sandi, lihat [AD DS: Kebijakan kata sandi butir halus di situs](#) web Microsoft. TechNet Untuk informasi umum tentang kebijakan ini, lihat [Kebijakan kata sandi](#) di TechNet situs web Microsoft.

Kebijakan penguncian akun

Anda juga dapat mengubah properti berikut dari kebijakan kata sandi Anda untuk menentukan apakah dan bagaimana Direktori Aktif harus mengunci akun setelah kegagalan login:

- Jumlah upaya masuk yang gagal diizinkan

- Durasi penguncian akun
- Mengatur ulang upaya masuk yang gagal setelah beberapa durasi

Untuk informasi umum tentang kebijakan ini, lihat [Kebijakan penguncian akun](#) di TechNet situs web Microsoft.

Precedence

Kebijakan dengan nilai prioritas yang lebih rendah memiliki prioritas yang lebih tinggi. Anda menetapkan kebijakan kata sandi untuk grup keamanan Direktori Aktif. Meskipun Anda harus menerapkan kebijakan tunggal untuk grup keamanan, satu pengguna tunggal mungkin menerima lebih dari satu kebijakan kata sandi. Sebagai contoh, misalkan `jsmith` adalah anggota dari grup HR dan juga anggota dari grup MANAJER. Jika Anda menetapkan CustomerPSO-05 (yang memiliki prioritas 50) untuk grup HR, dan CustomerPSO-04 (yang memiliki prioritas 40) untuk MANAJER, CustomerPSO-04 memiliki prioritas yang lebih tinggi dan Direktori Aktif menerapkan kebijakan tersebut untuk `jsmith`.

Jika Anda menetapkan beberapa kebijakan untuk pengguna atau grup, Direktori Aktif menentukan kebijakan yang dihasilkan sebagai berikut:

1. Kebijakan yang Anda tetapkan langsung ke objek pengguna berlaku.
2. Jika tidak ada kebijakan yang diberikan langsung ke objek pengguna, kebijakan dengan nilai prioritas terendah dari semua kebijakan yang diterima oleh pengguna sebagai hasil dari keanggotaan grup berlaku.

Untuk detail tambahan, lihat [AD DS: Kebijakan kata sandi berbutir halus](#) di situs web Microsoft TechNet

Topik

- [Menetapkan kebijakan kata sandi ke pengguna Microsoft AD yang AWS Dikelola](#)
- [Mendelegasikan siapa yang dapat mengelola kebijakan kata sandi Microsoft AD AWS Terkelola](#)

Artikel blog AWS Keamanan Terkait

- [Cara mengonfigurasi kebijakan kata sandi yang lebih kuat untuk membantu memenuhi standar keamanan Anda dengan menggunakan Directory Service untuk Microsoft AD yang AWS Dikelola](#)

Menetapkan kebijakan kata sandi ke pengguna Microsoft AD yang AWS Dikelola

Akun pengguna yang merupakan anggota grup keamanan Administrator Kebijakan Kata Sandi Terperinci yang Didelegasikan AWS dapat menggunakan prosedur berikut untuk menetapkan kebijakan untuk pengguna dan grup keamanan.

Untuk menetapkan kebijakan kata sandi ke pengguna Anda

1. Luncurkan [Pusat Administratif Direktori Aktif \(ADAC\)](#) dari instans EC2 terkelola yang Anda gabungkan ke domain AWS Microsoft AD Terkelola.
2. Beralih ke Tampilan pohon dan arahkan ke Kontainer pengaturan Sistem\Kata sandi.
3. Klik dua kali pada kebijakan terperinci yang ingin Anda edit. Klik Tambahkan untuk mengedit properti kebijakan, dan menambahkan pengguna atau grup keamanan ke kebijakan tersebut. Untuk informasi selengkapnya tentang kebijakan terperinci default yang disediakan dengan Microsoft AD yang Dikelola AWS, lihat [AWS kebijakan kata sandi yang telah ditentukan sebelumnya](#).
4. Untuk memverifikasi kebijakan kata sandi telah diterapkan, jalankan PowerShell perintah berikut:

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

Note

Hindari menggunakan `net user` perintah karena hasilnya bisa tidak akurat.

Jika Anda tidak mengonfigurasi salah satu dari lima kebijakan kata sandi di direktori Microsoft AD AWS Terkelola, Active Directory menggunakan kebijakan grup domain default. Untuk detail tambahan tentang penggunaan Kontainer pengaturan kata sandi, lihat [Postingan blog Microsoft](#).

Mendelegasikan siapa yang dapat mengelola kebijakan kata sandi Microsoft AD AWS Terkelola

Anda dapat mendelegasikan izin untuk mengelola kebijakan kata sandi ke akun pengguna tertentu yang Anda buat di AWS Microsoft AD Terkelola dengan menambahkan akun ke grup keamanan Administrator Kebijakan Kata Sandi Berbutir Halus yang AWS Delegasi. Ketika sebuah akun menjadi anggota grup ini, akun tersebut memiliki izin untuk mengedit dan mengkonfigurasi salah satu kebijakan kata sandi yang tercantum [sebelumnya](#).

Untuk mendelegasikan siapa yang dapat mengelola kebijakan kata sandi

1. Luncurkan [Pusat Administratif Direktori Aktif \(ADAC\)](#) dari instans EC2 terkelola yang Anda gabungkan ke domain AWS Microsoft AD Terkelola.
2. Beralih ke Tampilan pohon dan arahkan ke OU AWS Grup yang didelegasikan. Untuk informasi selengkapnya tentang OU ini, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).
3. Temukan pengguna grup Administrator Kebijakan Kata Sandi Terperinci yang Didelegasikan AWS . Menambahkan setiap pengguna atau grup dari domain Anda ke grup ini.

Mengaktifkan otentikasi multi-faktor untuk Microsoft AD yang Dikelola AWS

Anda dapat mengaktifkan autentikasi multi-faktor (MFA) untuk direktori AWS Microsoft AD Terkelola untuk meningkatkan keamanan saat pengguna menentukan kredensi AD mereka untuk mengakses aplikasi Amazon Enterprise yang Didukung. Saat Anda mengaktifkan MFA, pengguna Anda memasukkan nama pengguna dan kata sandi mereka (faktor pertama) seperti biasa, dan mereka juga harus memasukkan kode autentikasi (faktor kedua) yang mereka dapatkan dari solusi MFA virtual atau perangkat keras Anda. Faktor-faktor ini bersama-sama memberikan keamanan tambahan dengan mencegah akses ke aplikasi Amazon Enterprise Anda, kecuali pengguna menyediakan kredensial pengguna yang valid dan kode MFA yang valid.

Untuk mengaktifkan MFA, Anda harus memiliki solusi MFA yang adalah server [Layanan autentikasi jarak jauh panggilan masuk pengguna](#) (RADIUS), atau Anda harus memiliki plugin MFA ke server RADIUS yang sudah diterapkan di infrastruktur on-premise Anda. Solusi MFA Anda harus menerapkan Kode Sandi Sekali Pakai (OTP) yang diperoleh pengguna dari perangkat keras atau dari perangkat lunak yang berjalan pada perangkat seperti ponsel.

RADIUS adalah client/server protokol standar industri yang menyediakan otentikasi, otorisasi, dan manajemen akuntansi untuk memungkinkan pengguna terhubung ke layanan jaringan. AWS Microsoft AD yang dikelola mencakup klien RADIUS yang terhubung ke server RADIUS tempat Anda menerapkan solusi MFA Anda. Server RADIUS Anda memvalidasi nama pengguna dan kode OTP. Jika server RADIUS Anda berhasil memvalidasi pengguna, Microsoft AD yang AWS dikelola kemudian mengautentikasi pengguna terhadap Active Directory. Setelah otentikasi Active Directory berhasil, pengguna kemudian dapat mengakses AWS aplikasi. Komunikasi antara klien Microsoft AD RADIUS AWS Terkelola dan server RADIUS Anda mengharuskan Anda mengonfigurasi grup AWS keamanan yang mengaktifkan komunikasi melalui port 1812.

Anda dapat mengaktifkan autentikasi multi-faktor untuk direktori AWS Microsoft AD Terkelola dengan melakukan prosedur berikut. Untuk informasi selengkapnya tentang cara mengkonfigurasi server

RADIUS Anda untuk bekerja dengan Directory Service dan MFA, lihat [Prasyarat autentikasi multi-faktor](#).

Pertimbangan-pertimbangan

Berikut ini adalah beberapa pertimbangan untuk otentikasi multi-faktor untuk AWS Microsoft AD Terkelola Anda:

- Autentikasi multi-faktor tidak tersedia untuk Simple AD. Namun, MFA dapat diaktifkan untuk direktori AD Connector Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan otentikasi multi-faktor untuk AD Connector](#).
- MFA adalah fitur Regional dari AWS Microsoft AD yang Dikelola. Jika Anda menggunakan [replikasi Multi-Region](#), Anda hanya dapat menggunakan MFA di Wilayah Utama Microsoft AD yang Dikelola AWS.
- Jika Anda bermaksud menggunakan Microsoft AD yang AWS Dikelola untuk komunikasi eksternal, kami sarankan Anda mengonfigurasi Gateway Internet Gateway atau Internet Gateway Terjemahan Alamat Jaringan (NAT) di luar AWS jaringan untuk komunikasi ini.
 - Jika Anda ingin mendukung komunikasi eksternal antara Microsoft AD yang AWS Dikelola dan server RADIUS yang dihosting di AWS jaringan, silakan hubungi [Dukungan](#).
- Semua aplikasi TI Amazon Enterprise termasuk WorkSpaces, WorkDocs, Amazon WorkMail, Amazon Quick, dan akses ke AWS IAM Identity Center dan Konsol Manajemen AWS didukung saat menggunakan Konektor AD dan AD Microsoft AWS Terkelola dengan MFA. AWS Aplikasi ini menggunakan MFA tidak didukung di multi-wilayah.

Untuk informasi selengkapnya, lihat [Cara mengaktifkan autentikasi multi-faktor untuk AWS layanan menggunakan AWS Microsoft AD Terkelola dan kredensial lokal](#).

- Untuk informasi tentang cara mengonfigurasi akses pengguna dasar ke aplikasi Amazon Enterprise, AWS Single Sign-On dan Konsol Manajemen AWS penggunaan Directory Service, lihat [Akses ke AWS aplikasi dan layanan dari Microsoft AD yang AWS Dikelola](#) dan [Mengaktifkan Konsol Manajemen AWS akses dengan kredensial Microsoft AD yang AWS Dikelola](#).
- Lihat postingan Blog AWS Keamanan berikut ini untuk mempelajari cara mengaktifkan MFA untuk WorkSpaces pengguna Amazon di AWS Microsoft AD yang Dikelola, [Cara mengaktifkan autentikasi multi-faktor untuk AWS layanan menggunakan iklan AWS Microsoft Terkelola](#) dan kredensial lokal

Aktifkan otentikasi multi-faktor untuk AWS Microsoft AD yang Dikelola

Prosedur berikut menunjukkan cara mengaktifkan otentikasi multi-faktor untuk AWS Microsoft AD yang Dikelola.

1. Identifikasi alamat IP server MFA RADIUS Anda dan direktori AWS Microsoft AD Terkelola Anda.
2. Edit grup keamanan Virtual Private Cloud (VPC) Anda untuk mengaktifkan komunikasi melalui port 1812 antara titik akhir IP AWS Microsoft AD Terkelola dan server MFA RADIUS Anda.
3. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
4. Pilih tautan ID direktori untuk direktori Microsoft AD AWS Terkelola Anda.
5. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengaktifkan autentikasi multi-faktor (MFA), lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
6. Di bagian Autentikasi multi-faktor, pilih Tindakan, lalu pilih Aktifkan.
7. Pada halaman Aktifkan multi-factor authentication (MFA), berikan nilai berikut:

Label tampilan

Berikan nama label.

Nama DNS server RADIUS atau alamat IP

Alamat IP titik akhir server RADIUS, atau alamat IP penyeimbang beban server RADIUS. Anda dapat memasukkan beberapa alamat IP dengan memisahkannya dengan koma (misalnya, 192.0.0.0,192.0.0.12).

Note

RADIUS MFA hanya berlaku untuk mengautentikasi akses ke Konsol Manajemen AWS, atau ke aplikasi dan layanan Amazon Enterprise seperti, WorkSpaces Amazon Quick, atau Amazon Chime. Aplikasi dan layanan Amazon Enterprise hanya didukung di Wilayah Utama jika replikasi Multi-Wilayah dikonfigurasi untuk AWS Microsoft AD yang Dikelola. Itu tidak menyediakan beban kerja MFA ke Windows yang

berjalan pada instans EC2, atau untuk masuk ke instans EC2. Directory Service tidak mendukung otentikasi RADIUS Challenge/Response.

Pengguna harus memiliki kode autentikasi multi-faktor (MFA) mereka pada saat mereka memasukkan nama pengguna dan kata sandi. Atau, Anda harus menggunakan solusi yang melakukan MFA out-of-band seperti pemberitahuan push atau authenticator one-time password (OTP) untuk pengguna. Dalam solusi out-of-band MFA, Anda harus memastikan bahwa Anda menetapkan nilai batas waktu RADIUS dengan tepat untuk solusi Anda. Saat menggunakan solusi out-of-band MFA, halaman masuk akan meminta pengguna untuk kode MFA. Dalam hal ini, pengguna harus memasukkan kata sandi mereka di bidang kata sandi dan bidang MFA.

Port

Port yang digunakan oleh server RADIUS Anda untuk komunikasi. Jaringan lokal Anda harus mengizinkan lalu lintas masuk melalui port server RADIUS default (UDP:1812) dari server.

Directory Service

Kode rahasia bersama

Kode rahasia bersama yang ditentukan ketika titik akhir RADIUS Anda dibuat.

Konfirmasikan kode rahasia bersama

Konfirmasi kode rahasia bersama untuk titik akhir RADIUS Anda.

Protokol

Pilih protokol yang ditentukan saat titik akhir RADIUS Anda dibuat.

Batas waktu server (dalam hitungan detik)

Jumlah waktu, dalam detik, untuk menunggu server RADIUS menanggapi. Ini harus berupa nilai antara 1 dan 50.

Note

Sebaiknya konfigurasi batas waktu server RADIUS Anda menjadi 20 detik atau kurang. Jika batas waktu melebihi 20 detik, sistem tidak dapat mencoba lagi dengan server RADIUS lain dan dapat mengakibatkan kegagalan batas waktu.

Permintaan Max RADIUS mencoba ulang

Berapa kali komunikasi dengan server RADIUS dicoba. Ini harus berupa nilai antara 0 dan 10.

Autentikasi multi-faktor tersedia ketika Status RADIUS berubah ke Diaktifkan.

8. Pilih Aktifkan.

Aktifkan LDAP Aman atau LDAPS

Lightweight Directory Access Protocol (LDAP) adalah protokol komunikasi standar yang digunakan untuk membaca dan menulis data ke dan dari Direktori Aktif. Beberapa aplikasi menggunakan LDAP untuk menambah, menghapus, atau mencari pengguna dan grup di Direktori Aktif atau untuk mengangkut kredensial untuk autentikasi pengguna di Direktori Aktif. Setiap komunikasi LDAP termasuk klien (seperti aplikasi) dan server (seperti Direktori Aktif).

Secara default, komunikasi melalui LDAP tidak dienkripsi. Hal ini memungkinkan bagi pengguna berbahaya untuk menggunakan perangkat lunak pemantauan jaringan untuk melihat paket data melalui kabel. Inilah sebabnya mengapa banyak kebijakan keamanan perusahaan biasanya mengharuskan organisasi mengenkripsi semua komunikasi LDAP.

Untuk mengurangi bentuk paparan data ini, AWS Microsoft AD yang dikelola menyediakan opsi: Anda dapat mengaktifkan LDAP melalui Secure Sockets Layer (SSL) /Transport Layer Security (TLS), juga dikenal sebagai LDAPS. Dengan LDAPS, Anda dapat meningkatkan keamanan di seluruh kabel. Anda juga dapat memenuhi persyaratan kepatuhan dengan mengenkripsi semua komunikasi antara aplikasi berkemampuan LDAP dan Microsoft AD yang Dikelola. AWS

AWS Microsoft AD yang dikelola menyediakan dukungan untuk LDAPS dalam skenario penerapan berikut:

- LDAPS sisi Server mengenkripsi komunikasi LDAP antara aplikasi sadar LDAP komersial atau buatan sendiri Anda (bertindak sebagai klien LDAP) dan Microsoft AD yang Dikelola AWS (bertindak sebagai server LDAP). Untuk informasi selengkapnya, lihat [Mengaktifkan LDAPS sisi server menggunakan Microsoft AD yang Dikelola AWS](#).
- LDAPS sisi klien mengenkripsi komunikasi LDAP antara AWS aplikasi seperti WorkSpaces (bertindak sebagai klien LDAP) dan Direktori Aktif yang dikelola sendiri (lokal) Anda (bertindak

sebagai server LDAP). Untuk informasi selengkapnya, lihat [Mengaktifkan LDAPS sisi klien menggunakan Microsoft AD yang Dikelola AWS](#).

Untuk informasi selengkapnya tentang praktik terbaik terkait mengamankan implementasi Microsoft Active Directory Certificate Services, lihat [Microsoft dokumentasi](#).

Topik

- [Mengaktifkan LDAPS sisi server menggunakan Microsoft AD yang Dikelola AWS](#)
- [Mengaktifkan LDAPS sisi klien menggunakan Microsoft AD yang Dikelola AWS](#)

Mengaktifkan LDAPS sisi server menggunakan Microsoft AD yang Dikelola AWS

Lightweight Directory Access Protocol Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) Dukungan sisi server mengenkripsi LDAP komunikasi antara aplikasi LDAP sadar komersial atau lokal Anda dan direktori Microsoft AD Terkelola Anda. AWS Ini membantu meningkatkan keamanan di seluruh kabel dan memenuhi persyaratan kepatuhan menggunakan protokol Secure Sockets Layer (SSL) kriptografi.

Aktifkan LDAPS sisi server menggunakan AWS Private Certificate Authority

Untuk petunjuk terperinci tentang cara mengatur dan mengonfigurasi LDAPS sisi server dan server otoritas sertifikat (CA) yang Anda gunakan, lihat. AWS Private CA [Mengatur AWS Private CA Konektor untuk AD untuk Microsoft AD yang AWS Dikelola](#)

Aktifkan LDAPS sisi server menggunakan CA Microsoft

Untuk petunjuk terperinci tentang cara mengatur dan mengonfigurasi LDAPS sisi server dan server otoritas sertifikat (CA) Anda, lihat [Cara Mengaktifkan LDAPS Sisi Server untuk Direktori Microsoft AD Terkelola Anda AWS di Blog Keamanan](#). AWS

Anda harus melakukan sebagian besar pengaturan dari instans Amazon EC2 yang Anda gunakan untuk mengelola pengendali domain Microsoft AD yang Dikelola AWS Anda. Langkah-langkah berikut memandu Anda untuk mengaktifkan LDAPS untuk domain Anda di. AWS Cloud

Jika Anda ingin menggunakan otomatisasi untuk mengatur PKI Infrastruktur Anda, Anda dapat menggunakan [Infrastruktur Kunci Microsoft Publik pada AWS QuickStart Panduan](#). Secara khusus Anda akan ingin mengikuti petunjuk dalam panduan untuk memuat template untuk [Deploy Microsoft PKI ke dalam yang sudah ada VPC](#). AWS Setelah Anda memuat templat, pastikan untuk memilih **AWSManaged** saat Anda sampai ke opsi Jenis Layanan Domain Direktori Aktif. Jika Anda

menggunakan QuickStart panduan ini, Anda dapat melompat langsung ke [Langkah 3: Membuat templat sertifikat](#).

Topik

- [Langkah 1: Delegasikan yang dapat mengaktifkan LDAPS](#)
- [Langkah 2: Mengatur otoritas sertifikat Anda](#)
- [Langkah 3: Membuat templat sertifikat](#)
- [Langkah 4: Menambahkan aturan grup keamanan](#)

Langkah 1: Delegasikan yang dapat mengaktifkan LDAPS

Untuk mengaktifkan LDAPS sisi server, Anda harus menjadi anggota grup Admin atau Administrator Otoritas Sertifikat Perusahaan yang AWS Delegasi di direktori Microsoft AD yang Dikelola. AWS Atau, Anda dapat menjadi pengguna administratif default (akun Admin). Jika mau, Anda dapat memiliki pengguna selain LDAPS pengaturan akun Admin. Jika demikian, tambahkan pengguna tersebut ke grup Admin atau Administrator Otoritas Sertifikat Perusahaan AWS yang Delegasi di direktori AD AWS Microsoft Terkelola Anda.

Langkah 2: Mengatur otoritas sertifikat Anda

Sebelum Anda dapat mengaktifkan LDAPS sisi server, Anda harus membuat sertifikat. Sertifikat ini harus dikeluarkan oleh Microsoft Enterprise CA server yang bergabung dengan domain Microsoft AD AWS Terkelola Anda. Setelah dibuat, sertifikat harus diinstal pada masing-masing pengendali domain Anda di domain tersebut. Sertifikat ini memungkinkan LDAP layanan pada pengontrol domain mendengarkan dan secara otomatis menerima SSL koneksi dari LDAP klien.

Note

LDAPS sisi server dengan Microsoft AD yang AWS Dikelola tidak mendukung sertifikat yang dikeluarkan oleh CA mandiri. Itu juga tidak mendukung sertifikat yang dikeluarkan oleh otoritas sertifikasi pihak ketiga.

Tergantung pada kebutuhan bisnis Anda, Anda memiliki pilihan berikut untuk mengatur atau menghubungkan ke CA di domain Anda:

- Buat bawahan Microsoft Enterprise CA — (Disarankan) Dengan opsi ini, Anda dapat menggunakan Microsoft Enterprise CA server bawahan di Cloud. AWS Server dapat menggunakan Amazon EC2

sehingga berfungsi dengan root Microsoft CA yang ada. Untuk informasi selengkapnya tentang cara menyiapkan bawahan Microsoft Enterprise CA, lihat Langkah 4: Menambahkan Microsoft Enterprise CA ke AWS Microsoft AD direktori Anda di [Cara Mengaktifkan LDAPS Sisi Server untuk Direktori Microsoft AD yang Dikelola](#). AWS

- Buat root Microsoft Enterprise CA — Dengan opsi ini, Anda dapat membuat root Microsoft Enterprise CA di AWS Cloud menggunakan Amazon EC2 dan menggabungkannya ke domain AWS Microsoft AD yang Dikelola. Root CA ini dapat mengeluarkan sertifikat untuk pengendali domain Anda. Untuk informasi selengkapnya tentang menyiapkan CA root baru, lihat Langkah 3: Menginstal dan mengonfigurasi CA offline di [Cara Mengaktifkan LDAPS Sisi Server untuk Direktori Microsoft AD yang Dikelola AWS Anda](#).

Untuk informasi selengkapnya tentang cara menggabungkan instans EC2 Anda ke domain, lihat [Cara untuk bergabung dengan instans Amazon EC2 ke AWS Microsoft AD yang Dikelola](#).

Langkah 3: Membuat templat sertifikat

Setelah Anda Enterprise CA telah diatur, Anda dapat mengkonfigurasi template sertifikat Kerberos otentikasi.

Membuat templat sertifikat

1. Luncurkan Pengelola Server Microsoft Windows Pilih Alat > Otoritas Sertifikasi.
2. Di jendela Otoritas Sertifikat, perluas pohon Otoritas Sertifikat di panel kiri. Klik kanan Templat Sertifikat, dan pilih Kelola.
3. Di jendela Konsol Templat Sertifikat, klik kanan Autentikasi Kerberos dan pilih Templat Duplikasi.
4. Jendela Properti Templat Baru akan muncul.
5. Di jendela Properti Templat Baru, pergi ke tab Kompatibilitas, dan kemudian lakukan hal berikut:
 - a. Ubah Otoritas Sertifikasi ke OS yang cocok dengan CA Anda.
 - b. Jika jendela Perubahan yang dihasilkan muncul, pilih OK.
 - c. Ubah penerima Sertifikasi ke Windows 10/Windows Server 2016.

Note

AWS Microsoft AD yang dikelola didukung oleh Windows Server 2019.

- d. Jika jendela Perubahan yang dihasilkan muncul, pilih OK.

6. Klik tab Umum dan ubah nama tampilan Template menjadi LDAPOverSSL atau nama lain yang Anda inginkan.
7. Klik tab Keamanan, dan pilih Pengontrol domain di bagian Nama grup atau pengguna. Di bagian Izin untuk Pengendali Domain, verifikasi bahwa kotak centang Izinkan untuk Baca, Mendaftar, dan Autoenroll dicentang.
8. Pilih OK untuk membuat template sertifikat LDAPOverSSL (atau nama yang Anda tentukan di atas). Tutup jendela Konsol Templat Sertifikat.
9. Di jendela Otoritas Sertifikat, klik kanan Templat Sertifikat, dan pilih Baru > Templat Sertifikat untuk Diterbitkan.
10. Di jendela Aktifkan Templat Sertifikat, pilih LDAPOverSSL (atau nama yang Anda tentukan di atas), lalu pilih OK.

Langkah 4: Menambahkan aturan grup keamanan

Pada langkah terakhir, Anda harus membuka konsol Amazon EC2 dan menambahkan aturan grup keamanan. Aturan ini memungkinkan pengontrol domain Anda terhubung ke Anda Enterprise CA untuk meminta sertifikat. Untuk melakukan ini, Anda menambahkan aturan masuk sehingga Anda Enterprise CA dapat menerima lalu lintas masuk dari pengontrol domain Anda. Kemudian Anda menambahkan aturan keluar untuk mengizinkan lalu lintas dari pengontrol domain Anda ke Enterprise CA.

Setelah kedua aturan telah dikonfigurasi, pengontrol domain Anda meminta sertifikat dari Anda Enterprise CA secara otomatis dan mengaktifkan LDAPS untuk direktori Anda. LDAP Layanan pada pengontrol domain Anda sekarang siap menerima koneksi LDAPS.

Mengonfigurasi aturan grup keamanan

1. Arahkan ke konsol Amazon EC2 Anda di <https://console.aws.amazon.com/ec2> dan masuk dengan kredensial administrator.
2. Di panel kiri, pilih Kelompok Keamanan di bawah Jaringan & Keamanan.
3. Di panel utama, pilih grup AWS keamanan untuk CA Anda.
4. Pilih tab Masuk, lalu pilih Edit .
5. Di kotak dialog Edit aturan masuk, lakukan hal berikut:
 - Pilih Tambahkan aturan.
 - Pilih Semua Lalu lintas untuk Jenis dan Khusus untuk Sumber.

- Masukkan grup AWS keamanan (misalnya, sg-123456789) untuk direktori Anda di kotak di sebelah Sumber.
 - Pilih Simpan.
6. Sekarang pilih grup AWS keamanan direktori Microsoft AD AWS Terkelola Anda. Pilih tab Keluar, lalu pilih Edit.
7. Di kotak dialog Edit aturan keluar, lakukan hal berikut:
- Pilih Tambahkan aturan.
 - Pilih Semua Lalu lintas untuk Jenis dan Khusus untuk Tujuan.
 - Masukkan grup AWS keamanan untuk CA Anda di kotak di sebelah Tujuan.
 - Pilih Simpan.

Anda dapat menguji koneksi LDAPS ke direktori AWS Microsoft AD yang Dikelola menggunakan alat ini. LDP Alat ini dilengkapi dengan Active Directory Administrative Tools. Untuk informasi selengkapnya, lihat [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#).

 Note

Sebelum Anda menguji koneksi LDAPS, Anda harus menunggu hingga 30 menit untuk CA bawahan mengeluarkan sertifikat untuk pengendali domain Anda.

Untuk detail tambahan tentang LDAPS sisi server dan untuk melihat contoh kasus penggunaan tentang cara mengaturnya, lihat [Cara Mengaktifkan LDAPS Sisi Server untuk Direktori Microsoft AD Terkelola Anda AWS di Blog Keamanan](#). AWS

Mengaktifkan LDAPS sisi klien menggunakan Microsoft AD yang Dikelola AWS

Dukungan Lightweight Directory Access Protocol Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) di Microsoft AD AWS Terkelola mengenkripsi komunikasi antara Microsoft Active Directory (AD) yang dikelola sendiri (lokal) dan aplikasi. AWS Contoh aplikasi tersebut termasuk WorkSpaces,, Quick AWS IAM Identity Center, dan Amazon Chime. Enkripsi ini membantu Anda melindungi data identitas organisasi dengan lebih baik dan memenuhi persyaratan keamanan Anda.

Prasyarat

Sebelum Anda mengaktifkan LDAPS sisi klien, Anda harus memenuhi persyaratan berikut.

Topik

- [Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan Direktori Microsoft Aktif yang dikelola sendiri](#)
- [Men-deploy sertifikat server di Direktori Aktif](#)
- [Persyaratan sertifikat Otoritas Sertifikat](#)
- [Persyaratan jaringan](#)

Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan Direktori Microsoft Aktif yang dikelola sendiri

Pertama, Anda perlu membangun hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan Direktori Microsoft Aktif yang dikelola sendiri untuk mengaktifkan LDAPS sisi klien. Untuk informasi selengkapnya, lihat [the section called “Menciptakan hubungan kepercayaan”](#).

Men-deploy sertifikat server di Direktori Aktif

Untuk mengaktifkan LDAPS sisi klien, Anda perlu untuk mendapatkan dan menginstal sertifikat server untuk setiap pengendali domain di Direktori Aktif. Sertifikat ini akan digunakan oleh layanan LDAP untuk mendengarkan dan secara otomatis menerima koneksi SSL dari klien LDAP. Anda dapat menggunakan sertifikat SSL yang dikeluarkan oleh deployment Active Directory Certificate Services (ADCS) atau dibeli dari penerbit komersial. Untuk informasi lebih lanjut tentang persyaratan sertifikat server Direktori Aktif, lihat [LDAP melalui Sertifikat SSL \(LDAPS\)](#) di situs web Microsoft.

Persyaratan sertifikat Otoritas Sertifikat

Sertifikat otoritas sertifikat (CA), yang mewakili penerbit sertifikat server Anda, diperlukan untuk operasi LDAPS sisi klien. Sertifikat CA cocok dengan sertifikat server yang disajikan oleh pengendali domain Direktori Aktif Anda untuk mengenkripsi komunikasi LDAP. Perhatikan persyaratan sertifikat CA berikut:

- Otoritas Sertifikasi Perusahaan (CA) diperlukan untuk mengaktifkan LDAPS sisi klien. Anda dapat menggunakan Layanan Sertifikat Direktori Aktif, otoritas sertifikat komersial pihak ketiga, atau [AWS Certificate Manager](#). Untuk informasi selengkapnya tentang Otoritas Sertifikat Microsoft Perusahaan, lihat [Microsoft dokumentasi](#).
- Untuk mendaftarkan sertifikat, harus lebih dari 90 hari dari kedaluwarsa.

- Sertifikat harus dalam format Privacy Enhanced Mail (PEM). Jika mengekspor sertifikat CA dari dalam Direktori Aktif, pilih base64 encoded X.509 (.CER) sebagai format file ekspor.
- Maksimal lima (5) sertifikat CA dapat disimpan per direktori Microsoft AD yang AWS Dikelola.
- Sertifikat yang menggunakan algoritma tanda tangan RSASSA-PSS tidak didukung.
- Sertifikat CA yang berantai untuk setiap sertifikat server di setiap domain terpercaya harus terdaftar.

Persyaratan jaringan

AWS lalu lintas aplikasi LDAP akan berjalan secara eksklusif pada port TCP 636, tanpa fallback ke port LDAP 389. Namun, komunikasi Windows LDAP yang mendukung replikasi, kepercayaan, dan banyak lagi akan terus menggunakan LDAP port 389 dengan keamanan native Windows. Konfigurasi grup AWS keamanan dan firewall jaringan untuk mengizinkan komunikasi TCP pada port 636 di AWS Microsoft AD Terkelola (keluar) dan Direktori Aktif yang dikelola sendiri (masuk). Biarkan port 389 LDAP terbuka antara Microsoft AD yang Dikelola AWS dan Direktori Aktif yang dikelola sendiri.

Aktifkan LDAPS sisi klien

Untuk mengaktifkan LDAPS sisi klien, Anda mengimpor sertifikat otoritas (CA) sertifikat ke Microsoft AD yang Dikelola AWS, dan kemudian mengaktifkan LDAPS pada direktori Anda. Setelah mengaktifkan, semua lalu lintas LDAP antara aplikasi AWS dan Direktori Aktif Anda akan mengalir dengan enkripsi saluran Lapisan Socket Aman (SSL).

Anda dapat menggunakan dua metode yang berbeda untuk mengaktifkan LDAPS sisi klien untuk direktori Anda. Anda dapat menggunakan Konsol Manajemen AWS metode atau AWS CLI metode.

Note

LDAPS Sisi Klien adalah fitur Regional dari Microsoft AD yang Dikelola AWS. Jika Anda menggunakan [replikasi Multi-Region](#), prosedur berikut harus diterapkan secara terpisah di setiap Wilayah. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Topik

- [Langkah 1: Daftarkan sertifikat di Directory Service](#)
- [Langkah 2: Periksa status pendaftaran](#)

- [Langkah 3: Aktifkan LDAPS sisi klien](#)
- [Langkah 4: Periksa status LDAPS](#)

Langkah 1: Daftarkan sertifikat di Directory Service

Gunakan salah satu metode berikut untuk mendaftarkan sertifikat Directory Service.

Metode 1: Untuk mendaftarkan sertifikat Anda di Directory Service (Konsol Manajemen AWS)

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mendaftarkan sertifikat Anda, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih menu Tindakan, lalu pilih Mendaftarkan sertifikat.
5. Di kotak dialog Daftarkan sertifikat CA, pilih Telusuri, lalu pilih sertifikat dan pilih Buka.
6. Pilih Daftarkan sertifikat.

Metode 2: Untuk mendaftarkan sertifikat Anda di Directory Service (AWS CLI)

- Jalankan perintah berikut. Untuk data sertifikat, arahkan ke lokasi file sertifikat CA Anda. ID sertifikat akan diberikan dalam tanggapan.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data  
file://your_file_path
```

Langkah 2: Periksa status pendaftaran

Untuk melihat status pendaftaran sertifikat atau daftar sertifikat terdaftar, gunakan salah satu metode berikut:

Metode 1: Untuk memeriksa status pendaftaran sertifikat di Directory Service (Konsol Manajemen AWS)

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Meninjau status pendaftaran sertifikat saat ini yang ditampilkan di bawah kolom Status pendaftaran. Ketika nilai status pendaftaran berubah menjadi Registered, sertifikat Anda telah berhasil didaftarkan.

Metode 2: Untuk memeriksa status pendaftaran sertifikat di Directory Service (AWS CLI)

- Jalankan perintah berikut. Jika nilai status mengembalikan Registered, sertifikat Anda telah berhasil didaftarkan.

```
aws ds list-certificates --directory-id your_directory_id
```

Langkah 3: Aktifkan LDAPS sisi klien

Gunakan salah satu metode berikut untuk mengaktifkan LDAPS sisi klien. Directory Service

 Note

Anda harus berhasil mendaftarkan setidaknya satu sertifikat sebelum Anda dapat mengaktifkan LDAPS sisi klien.

Metode 1: Untuk mengaktifkan LDAPS sisi klien di () Directory Service Konsol Manajemen AWS

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Pilih Aktifkan. Jika opsi ini tidak tersedia, verifikasi bahwa sertifikat yang valid telah berhasil terdaftar, dan kemudian coba lagi.
3. Di kotak dialog Aktifkan LDAPS sisi klien, pilih Aktifkan.

Metode 2: Untuk mengaktifkan LDAPS sisi klien di () Directory Service AWS CLI

- Jalankan perintah berikut.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Langkah 4: Periksa status LDAPS

Gunakan salah satu metode berikut untuk memeriksa status LDAPS di Directory Service

Metode 1: Untuk memeriksa status LDAPS di Directory Service (Konsol Manajemen AWS)

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Jika nilai status ditampilkan sebagai Diaktifkan, LDAPS telah berhasil dikonfigurasi.

Metode 2: Untuk memeriksa status LDAPS di Directory Service (AWS CLI)

- Jalankan perintah berikut. Jika nilai status mengembalikan Enabled, LDAPS telah berhasil dikonfigurasi.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

Mengelola LDAPS sisi klien

Gunakan perintah ini untuk mengelola konfigurasi LDAPS Anda.

Anda dapat menggunakan dua metode yang berbeda untuk mengelola pengaturan LDAPS sisi klien. Anda dapat menggunakan Konsol Manajemen AWS metode atau AWS CLI metode.

Melihat detail sertifikat

Gunakan salah satu metode berikut untuk melihat ketika sertifikat diatur untuk kedaluwarsa.

Metode 1: Untuk melihat detail sertifikat di Directory Service (Konsol Manajemen AWS)

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region di mana Anda ingin melihat sertifikat, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, di bawah Sertifikat CA, informasi tentang sertifikat akan ditampilkan.

Metode 2: Untuk melihat detail sertifikat di Directory Service (AWS CLI)

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Membatalkan pendaftaran sertifikat

Gunakan salah satu metode berikut untuk membatalkan pendaftaran sertifikat.

Note

Jika hanya satu sertifikat yang terdaftar, Anda harus terlebih dahulu menonaktifkan LDAPS sebelum Anda dapat membatalkan pendaftaran sertifikat.

Metode 1: Untuk membatalkan pendaftaran sertifikat di () Directory Service Konsol Manajemen AWS

- Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
- Pilih tautan ID direktori untuk direktori Anda.
- Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin membatalkan pendaftaran sertifikat Anda, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
- Di bagian LDAPS sisi klien, pilih Tindakan, lalu pilih Membatalkan pendaftaran sertifikat.
- Di kotak dialog Membatalkan pendaftaran sertifikat CA, pilih Batalkan pendaftaran.

Metode 2: Untuk membatalkan pendaftaran sertifikat di () Directory Service AWS CLI

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Menonaktifkan LDAPS sisi klien

Gunakan salah satu metode berikut untuk menonaktifkan LDAPS sisi klien.

Metode 1: Untuk menonaktifkan LDAPS sisi klien di () Directory Service Konsol Manajemen AWS

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menonaktifkan LDAPS sisi klien, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih Nonaktifkan.
5. Di kotak dialog Nonaktifkan LDAPS sisi klien, pilih Nonaktifkan.

Metode 2: Untuk menonaktifkan LDAPS sisi klien di () Directory Service AWS CLI

- Jalankan perintah berikut.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Masalah pendaftaran sertifikat

Proses untuk mendaftarkan pengontrol domain Microsoft AD AWS Terkelola dengan sertifikat CA dapat memakan waktu hingga 30 menit. Jika Anda mengalami masalah dengan pendaftaran sertifikat dan ingin memulai ulang pengontrol domain AWS Microsoft AD Terkelola, Anda dapat menghubungi Dukungan Untuk membuat kasus dukungan, lihat [Membuat kasus dukungan dan manajemen kasus](#).

Mengelola kepatuhan untuk Microsoft AD yang AWS Dikelola

Anda dapat menggunakan Microsoft AD AWS Terkelola untuk mendukung aplikasi sadar Direktori Aktif Anda, di AWS Cloud, yang tunduk pada persyaratan kepatuhan berikut. Namun, aplikasi Anda tidak akan mematuhi persyaratan kepatuhan jika Anda menggunakan Simple AD.

Standar kepatuhan yang didukung

AWS Microsoft AD yang dikelola telah menjalani audit untuk standar berikut dan memenuhi syarat untuk digunakan sebagai bagian dari solusi yang Anda perlukan untuk mendapatkan sertifikasi kepatuhan.



AWS Microsoft AD yang dikelola memenuhi persyaratan keamanan Program Manajemen Risiko dan Otorisasi Federal (FedRAMP) dan telah menerima Otorisasi Sementara FedRAMP Joint Authorization Board (JAB) untuk Beroperasi (P-ATO) di FedRAMP Moderate and High Baseline. Untuk informasi selengkapnya tentang FedRAMP, lihat [Kepatuhan FedRAMP](#).



AWS Microsoft AD yang dikelola memiliki Pengesahan Kepatuhan untuk Standar Keamanan Data (DSS) Industri Kartu Pembayaran (PCI) versi 3.2 di Penyedia Layanan Level 1. Pelanggan yang menggunakan AWS produk dan layanan untuk menyimpan, memproses, atau mengirimkan data pemegang kartu dapat menggunakan Microsoft AD yang AWS Dikelola saat mengelola sertifikasi kepatuhan PCI DSS mereka sendiri.

Untuk informasi selengkapnya tentang PCI DSS, termasuk cara meminta salinan PCI AWS Compliance Package, lihat [PCI DSS level 1](#). Yang penting, Anda harus mengonfigurasi kebijakan kata sandi berbutir halus di AWS Microsoft

AD yang Dikelola agar konsisten dengan standar PCI DSS versi 3.2. Untuk detail tentang kebijakan mana yang harus diberlakukan, lihat bagian di bawah ini berjudul Aktifkan Kepatuhan PCI untuk Direktori AWS Microsoft AD yang Dikelola Anda.



AWS [telah memperluas program kepatuhan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan \(HIPAA\) untuk memasukkan AWS Microsoft AD yang Dikelola sebagai layanan yang memenuhi syarat HIPAA.](#)

Jika Anda memiliki Perjanjian Rekanan Bisnis (BAA) yang dieksekusi AWS, Anda dapat menggunakan Microsoft AD AWS Terkelola untuk membantu membangun aplikasi yang sesuai dengan HIPAA.

AWS menawarkan [whitepaper yang berfokus pada HIPAA](#) untuk pelanggan yang tertarik untuk mempelajari lebih lanjut tentang bagaimana mereka dapat memanfaatkan pemrosesan dan AWS penyimpanan informasi kesehatan. Untuk informasi selengkapnya, lihat [Kepatuhan HIPAA](#).

Tanggung Jawab Bersama

Keamanan, termasuk kepatuhan FedRAMP, HIPAA, dan PCI, adalah [tanggung jawab bersama](#). Penting untuk dipahami bahwa status kepatuhan Microsoft AD yang AWS dikelola tidak berlaku secara otomatis untuk aplikasi yang Anda jalankan di AWS Cloud. Anda perlu memastikan bahwa penggunaan AWS layanan Anda sesuai dengan standar.

Untuk daftar lengkap berbagai program AWS kepatuhan yang didukung Microsoft AD AWS Terkelola, lihat [AWS layanan dalam cakupan berdasarkan program kepatuhan](#).

Aktifkan kepatuhan PCI untuk direktori Microsoft AD AWS Terkelola

Untuk mengaktifkan kepatuhan PCI untuk direktori Microsoft AD AWS Terkelola, Anda harus mengonfigurasi kebijakan kata sandi berbutir halus seperti yang ditentukan dalam dokumen Pengesahan Kepatuhan (AOC) dan Ringkasan Tanggung Jawab PCI DSS yang disediakan oleh AWS Artifact

Untuk informasi selengkapnya tentang menggunakan kebijakan kata sandi terperinci, lihat [Memahami kebijakan kata sandi Microsoft AD yang AWS Dikelola](#).

Meningkatkan konfigurasi keamanan jaringan Microsoft AD AWS Terkelola

Grup AWS Keamanan yang disediakan untuk direktori AWS Microsoft AD Terkelola dikonfigurasi dengan port jaringan masuk minimum yang diperlukan untuk mendukung semua kasus penggunaan yang diketahui untuk direktori AWS Microsoft AD Terkelola Anda. Untuk informasi selengkapnya tentang Grup AWS Keamanan yang disediakan, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#)

Untuk lebih meningkatkan keamanan jaringan direktori Microsoft AD AWS Terkelola, Anda dapat memodifikasi Grup AWS Keamanan berdasarkan skenario umum berikut.

Pengontrol domain pelanggan CIDR - Blok CIDR ini adalah tempat pengontrol domain lokal Anda berada.

Klien pelanggan CIDR - Blok CIDR ini adalah tempat klien Anda seperti komputer atau pengguna mengautentikasi ke AWS Microsoft AD Terkelola Anda. Pengontrol domain Microsoft AD AWS Terkelola Anda juga berada di blok CIDR ini.

Skenario

- [AWS aplikasi hanya mendukung](#)
- [AWS aplikasi hanya dengan dukungan kepercayaan](#)
- [AWS aplikasi dan dukungan beban kerja Active Directory asli](#)
- [AWS aplikasi dan dukungan beban kerja Active Directory asli dengan dukungan kepercayaan](#)

AWS aplikasi hanya mendukung

Semua akun pengguna hanya disediakan di AWS Microsoft AD Terkelola untuk digunakan dengan AWS aplikasi yang didukung, seperti berikut ini:

- Amazon Chime
- Amazon Connect
- Cepat
- AWS IAM Identity Center

- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- Konsol Manajemen AWS

Anda dapat menggunakan konfigurasi Grup AWS Keamanan berikut untuk memblokir semua lalu lintas yang tidak penting ke pengontrol domain Microsoft AD yang AWS Dikelola.

 Note

- Berikut ini tidak kompatibel dengan konfigurasi Grup AWS Keamanan ini:
 - Instans Amazon EC2
 - Amazon FSx
 - Amazon RDS for MySQL
 - Amazon RDS for Oracle
 - Amazon RDS for PostgreSQL
 - Amazon RDS for SQL Server
 - WorkSpaces
 - Kepercayaan Direktori Aktif
 - Domain bergabung klien atau server

Aturan Masuk

Tidak ada.

Aturan Keluar

Tidak ada.

AWS aplikasi hanya dengan dukungan kepercayaan

Semua akun pengguna disediakan di AWS Microsoft AD yang Dikelola atau Direktori Aktif tepercaya untuk digunakan dengan AWS aplikasi yang didukung, seperti berikut ini:

- Amazon Chime

- Amazon Connect
- Cepat
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- Konsol Manajemen AWS

Anda dapat mengubah konfigurasi Grup AWS Keamanan yang disediakan untuk memblokir semua lalu lintas yang tidak penting ke pengontrol domain AWS Microsoft AD Terkelola.

 Note

- Berikut ini tidak kompatibel dengan konfigurasi Grup AWS Keamanan ini:
 - Instans Amazon EC2
 - Amazon FSx
 - Amazon RDS for MySQL
 - Amazon RDS for Oracle
 - Amazon RDS for PostgreSQL
 - Amazon RDS for SQL Server
 - WorkSpaces
 - Kepercayaan Direktori Aktif
 - Domain bergabung klien atau server
- Konfigurasi ini mengharuskan Anda untuk memastikan jaringan “pengontrol domain pelanggan CIDR” aman.
- TCP 445 digunakan untuk pembuatan kepercayaan saja dan dapat dihapus setelah kepercayaan telah ditetapkan.
- TCP 636 hanya diperlukan ketika LDAP atas SSL sedang digunakan.

Aturan Masuk

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	53	Pengontro l domain pelanggan CIDR	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan
TCP & UDP	88	Pengontro l domain pelanggan CIDR	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest
TCP & UDP	389	Pengontro l domain pelanggan CIDR	LDAP	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP & UDP	464	Pengontro l domain pelanggan CIDR	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentika si komputer, kepercayaan
TCP	445	Pengontro l domain pelanggan CIDR	SMB / CIFS	Replikasi, autentikasi pengguna dan komputer, kepercayaan kebijakan grup

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	135	Pengontro I domain pelanggan CIDR	Replikasi	RPC, EPM
TCP	636	Pengontro I domain pelanggan CIDR	LDAP SSL	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP	49152 - 65535	Pengontro I domain pelanggan CIDR	RPC	Replikasi, pengguna dan autentika si komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	Pengontro I domain pelanggan CIDR	LDAP GC & LDAP GC SSL	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
UDP	123	Pengontro I domain pelanggan CIDR	Waktu Windows	Waktu Windows, kepercayaan

Aturan Keluar

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
Semua	Semua	Pengontro l domain pelanggan CIDR	Semua Lalu lintas	

AWS aplikasi dan dukungan beban kerja Active Directory asli

Akun pengguna hanya disediakan di AWS Microsoft AD Terkelola untuk digunakan dengan AWS aplikasi yang didukung, seperti berikut ini:

- Amazon Chime
- Amazon Connect
- Instans Amazon EC2
- Amazon FSx
- Cepat
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- Konsol Manajemen AWS

Anda dapat mengubah konfigurasi Grup AWS Keamanan yang disediakan untuk memblokir semua lalu lintas yang tidak penting ke pengontrol domain AWS Microsoft AD Terkelola.

Note

- Trust Active Directory tidak dapat dibuat dan dipertahankan antara direktori Microsoft AD yang AWS Dikelola dan CIDR pengontrol domain pelanggan.
- Ini mengharuskan Anda untuk memastikan jaringan “pelanggan klien CIDR” aman.
- TCP 636 hanya diperlukan ketika LDAP atas SSL sedang digunakan.
- Jika Anda ingin menggunakan Enterprise CA dengan konfigurasi ini, Anda harus membuat aturan keluar “TCP, 443, CA CIDR”.

Aturan Masuk

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	53	Klien pelanggan CIDR	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan
TCP & UDP	88	Klien pelanggan CIDR	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest
TCP & UDP	389	Klien pelanggan CIDR	LDAP	Direktori, replikasi, kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP & UDP	445	Klien pelanggan CIDR	SMB / CIFS	Replikasi, autentikasi

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
				pengguna dan komputer, kepercayaan kebijakan grup
TCP & UDP	464	Klien pelanggan CIDR	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentikasi komputer, kepercayaan
TCP	135	Klien pelanggan CIDR	Replikasi	RPC, EPM
TCP	636	Klien pelanggan CIDR	LDAP SSL	Direktori, replikasi, kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP	49152 - 65535	Klien pelanggan CIDR	RPC	Replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	3268 - 3269	Klien pelanggan CIDR	LDAP GC & LDAP GC SSL	Direktori, replikasi, kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP	9389	Klien pelanggan CIDR	SOAP	Layanan web AD DS
UDP	123	Klien pelanggan CIDR	Waktu Windows	Waktu Windows, kepercayaan
UDP	138	Klien pelanggan CIDR	DFSN & NetLogon	DFS, kebijakan grup

Aturan Keluar

Tidak ada.

AWS aplikasi dan dukungan beban kerja Active Directory asli dengan dukungan kepercayaan

Semua akun pengguna disediakan di AWS Microsoft AD yang Dikelola atau Direktori Aktif tepercaya untuk digunakan dengan AWS aplikasi yang didukung, seperti berikut ini:

- Amazon Chime
- Amazon Connect
- Instans Amazon EC2
- Amazon FSx
- Cepat
- Amazon RDS for MySQL
- Amazon RDS for Oracle

- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- Konsol Manajemen AWS

Anda dapat mengubah konfigurasi Grup AWS Keamanan yang disediakan untuk memblokir semua lalu lintas yang tidak penting ke pengontrol domain AWS Microsoft AD Terkelola.

Note

- Ini mengharuskan Anda untuk memastikan jaringan “pengontrol domain pelanggan CIDR” dan “klien pelanggan CIDR” aman.
- TCP 445 dengan “pengontrol domain pelanggan CIDR” digunakan hanya untuk pembuatan kepercayaan dan dapat dihapus setelah kepercayaan ditetapkan.
- TCP 445 dengan “klien pelanggan CIDR” harus dibiarkan terbuka karena diperlukan untuk pemrosesan Kebijakan Grup.
- TCP 636 hanya diperlukan ketika LDAP atas SSL sedang digunakan.
- Jika Anda ingin menggunakan Enterprise CA dengan konfigurasi ini, Anda harus membuat aturan keluar “TCP, 443, CA CIDR”.

Aturan Masuk

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	53	Pengontro l domain pelanggan CIDR	DNS	Autentikasi pengguna dan komputer,

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
				resolusi nama, kepercayaan
TCP & UDP	88	Pengontro I domain pelanggan CIDR	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest
TCP & UDP	389	Pengontro I domain pelanggan CIDR	LDAP	Direktori, replikasi, kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP & UDP	464	Pengontro I domain pelanggan CIDR	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentikasi komputer, kepercayaan
TCP	445	Pengontro I domain pelanggan CIDR	SMB / CIFS	Replikasi, autentikasi pengguna dan komputer, kepercayaan kebijakan grup
TCP	135	Pengontro I domain pelanggan CIDR	Replikasi	RPC, EPM

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	636	Pengontro I domain pelanggan CIDR	LDAP SSL	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP	49152 - 65535	Pengontro I domain pelanggan CIDR	RPC	Replikasi, pengguna dan autentika si komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	Pengontro I domain pelanggan CIDR	LDAP GC & LDAP GC SSL	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
UDP	123	Pengontro I domain pelanggan CIDR	Waktu Windows	Waktu Windows, kepercayaan
TCP & UDP	53	Pengontro I domain pelanggan CIDR	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	88	Pengontro I domain pelanggan CIDR	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest
TCP & UDP	389	Pengontro I domain pelanggan CIDR	LDAP	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP & UDP	445	Pengontro I domain pelanggan CIDR	SMB / CIFS	Replikasi, autentikasi pengguna dan komputer, kepercayaan kebijakan grup
TCP & UDP	464	Pengontro I domain pelanggan CIDR	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentika si komputer, kepercayaan
TCP	135	Pengontro I domain pelanggan CIDR	Replikasi	RPC, EPM

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	636	Pengontro I domain pelanggan CIDR	LDAP SSL	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP	49152 - 65535	Pengontro I domain pelanggan CIDR	RPC	Replikasi, pengguna dan autentika si komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	Pengontro I domain pelanggan CIDR	LDAP GC & LDAP GC SSL	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP	9389	Pengontro I domain pelanggan CIDR	SOAP	Layanan web AD DS
UDP	123	Pengontro I domain pelanggan CIDR	Waktu Windows	Waktu Windows, kepercayaan
UDP	138	Pengontro I domain pelanggan CIDR	DFSN & NetLogon	DFS, kebijakan grup

Aturan Keluar

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
Semua	Semua	Pengontro l domain pelanggan CIDR	Semua Lalu lintas	

Mengedit pengaturan keamanan direktori Microsoft AD yang AWS Dikelola

Anda dapat mengonfigurasi setelan direktori berbutir halus untuk AWS Microsoft AD yang Dikelola agar memenuhi persyaratan kepatuhan dan keamanan tanpa peningkatan beban kerja operasional. Dalam pengaturan direktori, Anda dapat memperbarui konfigurasi saluran aman untuk protokol dan cipher yang digunakan dalam direktori Anda. Misalnya, Anda memiliki fleksibilitas untuk menonaktifkan cipher warisan individu, seperti RC4 atau DES, dan protokol, seperti SSL 2.0/3.0 dan TLS 1.0/1.1. AWS Microsoft AD yang dikelola kemudian menyebarkan konfigurasi ke semua pengontrol domain di direktori Anda, mengelola reboot pengontrol domain, dan mempertahankan konfigurasi ini saat Anda meningkatkan skala atau menerapkan tambahan. Wilayah AWS Untuk semua pengaturan yang tersedia, lihat [Daftar pengaturan keamanan direktori](#).

Edit pengaturan keamanan direktori

Anda dapat mengonfigurasi dan mengedit pengaturan untuk direktori mana pun.

Untuk mengedit pengaturan direktori

1. Masuk ke Konsol AWS Manajemen dan buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah Jaringan & keamanan, temukan pengaturan Direktori, lalu pilih Edit pengaturan.
4. Di Pengaturan Edit, ubah Nilai untuk pengaturan yang ingin Anda edit. Saat Anda mengedit setelan, statusnya berubah dari Default menjadi Siap untuk Diperbarui. Jika Anda telah mengedit pengaturan sebelumnya, statusnya berubah dari Diperbarui menjadi Siap untuk Diperbarui. Kemudian, pilih Review.
5. Di Pengaturan tinjauan dan perbarui, lihat Pengaturan direktori dan pastikan bahwa semua nilai baru sudah benar. Jika Anda ingin membuat perubahan lain pada pengaturan Anda, pilih Edit

pengaturan. Jika Anda puas dengan perubahan dan siap menerapkan nilai baru, pilih Perbarui pengaturan. Kemudian, Anda dibawa kembali ke halaman ID direktori.

Note

Di bawah Pengaturan direktori, Anda dapat melihat Status pengaturan yang diperbarui. Saat pengaturan diimplementasikan, Status menampilkan Memperbarui. Anda tidak dapat mengedit pengaturan lain saat pengaturan menampilkan Memperbarui di bawah Status. Status menampilkan Diperbarui jika pengaturan berhasil diperbarui dengan pengeditan Anda. Status ditampilkan Gagal jika pengaturan gagal diperbarui dengan pengeditan Anda.

Pengaturan keamanan direktori gagal

Jika terjadi kesalahan selama pembaruan pengaturan, Status ditampilkan sebagai Gagal. Dalam status gagal, pengaturan tidak diperbarui ke nilai baru, dan nilai asli tetap diterapkan. Anda dapat mencoba lagi memperbarui pengaturan ini atau mengembalikannya ke nilai sebelumnya.

Untuk mengatasi setelan yang diperbarui gagal

- Di bawah Pengaturan direktori, pilih Selesaikan setelan yang gagal. Kemudian, lakukan salah satu hal berikut:
 - Untuk mengembalikan setelan Anda kembali ke nilai aslinya sebelum status kegagalan, pilih Kembalikan setelan yang gagal. Kemudian, pilih Kembalikan di modal pop-up.
 - Untuk mencoba lagi memperbarui pengaturan direktori Anda, pilih Coba lagi setelan yang gagal. Jika Anda ingin membuat perubahan tambahan pada pengaturan direktori Anda sebelum mencoba kembali pembaruan yang gagal, pilih Lanjutkan pengeditan. Pada Tinjau dan coba lagi pembaruan yang gagal, pilih Pengaturan pembaruan.

Daftar pengaturan keamanan direktori

Daftar berikut menunjukkan jenis, nama setelan, nama API, nilai potensial, dan deskripsi setelan untuk semua setelan keamanan direktori yang tersedia.

TLS 1.2 dan AES 256/256 adalah pengaturan keamanan direktori default jika semua pengaturan keamanan lainnya dinonaktifkan. Mereka tidak bisa dinonaktifkan.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
Otentikasi Berbasis Sertifikat	Komper i Backda g Sertifika t	CERTIFICA TE_BACKDA TING_COMP ENSATION	Tahun: 0 hingga 50 Bulan: 0 hingga 11 Hari: 0 hingga 30 Jam: 0 hingga 23 Menit: 0 hingga 59 Detik: 0 hingga 59	Tentukan nilai untuk menunjukkan lamanya waktu sertifikat dapat mendahului pengguna di Active Directory dan masih digunakan untuk otentikasi di Active Directory. Nilai defaultnya adalah 10 menit. Anda dapat mengatur nilai ini dari 1 detik hingga 50 tahun. Untuk mengonfigurasi pengaturan ini, Anda harus memilih jenis Kompatibilitas untuk Strong Certifica

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
				te Binding Enforcement. Untuk informasi selengkap nya, lihat KB5014754 — Perubahan autentikasi berbasis sertifikat pada pengontro l domain Windows di dokumenta si Dukungan Microsoft.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
	Sertifikat Penegakan Kuat	CERTIFICATE_STRONG_ENFORCEMENT	Kompatibilitas, Penegakan Penuh	Tentukan salah satu dari jenis penegakan berikut: • Kompatibilitas: Otentikasi diperbolehkan jika sertifikat tidak dapat dipetakan dengan kuat ke pengguna. Jika sertifikat mendahului akun pengguna di Active Directory, Anda juga harus menetapkan Certificate Backdating Compensation, atau otentikasi akan gagal. • Penegakan Penuh

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
				(default): Otentikasi tidak diizinkan jika sertifikat tidak dapat dipetakan dengan kuat ke pengguna. Jika Anda memilih jenis penegakan ini, Kompensasi Backdating Sertifikat tidak dapat dikonfigurasi. Untuk informasi selengkapnya, lihat KB5014754 —Perubahan autentikasi berbasis sertifikat pada pengontrol domain Windows di

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
				dokumentasi Dukungan Microsoft.
Saluran Aman: Ciper	AES 128/128	AES_128_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan ciper enkripsi AES 128/128 untuk komunikasi saluran aman antara pengontro l domain di direktori Anda.
	DES 56/56	DES_56_56	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan sandi enkripsi DES 56/56 untuk komunikasi saluran aman antara pengontro l domain di direktori Anda.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
	RC2_40/128	RC2_40_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan cipher enkripsi RC2 40/128 untuk komunikasi saluran aman antara pengontrol domain di direktori Anda.
	RC2_56/128	RC2_56_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan sandi enkripsi RC2 56/128 untuk komunikasi saluran aman antara pengontrol domain di direktori Anda.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
	RC2 128/128	RC2_128_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan sandi enkripsi RC2 128/128 untuk komunikasi saluran aman antara pengontrol domain di direktori Anda.
	RC4 40/128	RC4_40_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan cipher enkripsi RC4 40/128 untuk komunikasi saluran aman antara pengontrol domain di direktori Anda.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
	RC4_56/128	RC4_56_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan sandi enkripsi RC4 56/128 untuk komunikasi saluran aman antara pengontrol domain di direktori Anda.
	RC4_64/128	RC4_64_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan cipher enkripsi RC4 64/128 untuk komunikasi saluran aman antara pengontrol domain di direktori Anda.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
	RC4_128_128	RC4_128_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan sandi enkripsi RC4 128/128 untuk komunikasi saluran aman antara pengontrol domain di direktori Anda.
	Tiga DES 168/168	3DES_168_168	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan sandi enkripsi Triple DES 168/168 untuk komunikasi saluran aman antara pengontrol domain di direktori Anda.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
Saluran Aman: Protokol	PCT 1.0	PCT_1_0	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol PCT 1.0 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.
	SSL 2.0	SSL_2_0	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol SSL 2.0 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
	SSL 3.0	SSL_3_0	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol SSL 3.0 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.
	TLS 1.0	TLS_1_0	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol TLS 1.0 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.

Tipe	Nama pengaturan	Nama API	Nilai potensial	Deskripsi pengaturan
	TLS 1.1	TLS_1_1	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol TLS 1.1 untuk komunikasi saluran aman (Server dan Klien) pada pengontrol domain di direktori Anda.

Aktifkan Kriptografi Kunci Publik untuk Otentikasi Awal (PKINIT) untuk pengguna Microsoft AD yang Dikelola AWS

AWS Direktori Microsoft AD yang dikelola menggunakan pengikatan sertifikat yang kuat secara default, yang memerlukan pemetaan eksplisit antara sertifikat dan objek AD. Pemetaan berikut dianggap kuat untuk AWS Microsoft AD yang Dikelola:

- `altSecurityIdentitiesPenerbit` dan Nomor Seri
- `altSecurityIdentitiesPengidentifikasi Kunci Subjek`
- `altSecurityIdentities` SHA1 Hash Kunci Publik

Atribut ini memungkinkan pemetaan sertifikat yang kuat, yang memberikan keamanan yang lebih baik untuk otentikasi berbasis sertifikat dengan mewajibkan certificate-to-user hubungan eksplisit yang ditentukan dalam Active Directory. Ini membantu mencegah serangan eskalasi hak istimewa berbasis sertifikat

Anda dapat menggunakan prosedur ini untuk mengonfigurasi binding sertifikat yang kuat untuk membantu Anda mencegah serangan eskalasi hak istimewa sambil mempertahankan fungsionalitas otentikasi sertifikat.

Untuk informasi selengkapnya, lihat [Microsoft KB5014754: Perubahan autentikasi berbasis sertifikat](#) pada pengontrol domain Windows

Prasyarat

- Direktori Microsoft AD AWS Terkelola dengan otoritas sertifikat yang dikonfigurasi
- Akses administratif ke lingkungan Direktori Aktif
- PowerShell dengan modul Active Directory diinstal
- Sertifikat yang ingin Anda petakan ke objek AD

AltSecurityIdentity Atribut peta

1. Pilih salah satu metode AltSecurityIdentity pemetaan berikut berdasarkan informasi sertifikat Anda:

- SHA1 hash — Menggunakan SHA1 hash dari kunci publik sertifikat

Untuk pemetaan SHA1 hash, ekstrak hash sertifikat dan terapkan ke objek pengguna:

```
$Username = 'YourUsername'
$cert = certutil -dump "YourCertificate.cer"
$certHash = ($cert | Select-String -Pattern "(sha1):*" |
    Select-String -Pattern "Cert").ToString().TrimStart('Cert Hash sha1:').Replace(' ', '')
Set-ADUser -Identity $Username -Add @{'altSecurityIdentities'="X509:<SHA1-PUKEY>$CertHash"}
```

- Penerbit dan Nomor Seri — Menggunakan nama penerbit sertifikat dan nomor seri

Untuk pemetaan Emiten dan Nomor Seri, gunakan penerbit sertifikat dan nomor seri:

```
$Username = 'YourUsername'
$IssuerName = 'YourCertificateIssuer'
$SerialNumber = 'YourCertificateSerialNumber'
Set-ADUser -Identity $Username -Add @{'altSecurityIdentities'="X509:<I>$IssuerName<SR>$SerialNumber"}
```

- Pengenal Kunci Subjek - Menggunakan ekstensi pengidentifikasi kunci subjek sertifikat

Untuk pemetaan Pengenal Kunci Subjek, gunakan pengenal kunci subjek sertifikat:

```
$Username = 'YourUsername'
$SubjectKeyIdentifier = 'YourSubjectKeyIdentifier'
Set-ADUser -Identity $Username -Add @{'altSecurityIdentities'="X509:<SKI>
$SubjectKeyIdentifier"}
```

2. Verifikasi bahwa pemetaan berhasil diterapkan:

```
Get-ADUser -Identity $Username -Properties altSecurityIdentities |
Select-Object -ExpandProperty altSecurityIdentities
```

3. Tunggu replikasi Active Directory selesai (biasanya 15-30 detik) sebelum menguji otentikasi sertifikat.

Contoh: Sertifikat massal memetakan atribut AltSecurityIdentity

Contoh berikut menunjukkan cara memetakan AltSecurityIdentity atribut untuk beberapa sertifikat pengguna dari otoritas sertifikat:

```
$CertificateTemplateName = 'User'
$Now = (((Get-Date).ToString($(Get-culture).DateTimeFormat.ShortDatePattern))
$Restrict = "Disposition=20,NotAfter>=$Now,Certificate Template=
$CertificateTemplateName"
$Out = "SerialNumber,Certificate Hash,User Principal
Name,RequesterName,CommonName,CertificateTemplate,NotBefore,NotAfter"
$Certs = certutil -view -restrict $Restrict -out $Out csv | ConvertFrom-CSV
$UserSha1HashMapping = @{}

ForEach ($Cert in $Certs) {
    $UPN = $Cert.'User Principal Name'
    $Username, $Domain = $UPN.Split('@')
    $CertificateThumbprint = ($Cert.'Certificate Hash').Replace(' ', '')
    $AdUserObject = Get-ADUser -Identity $Username
    If ($AdUserObject -And $AdUserObject.Count -gt 1) {
        Write-Output "Unable to map user: $Username, multiple user objects found"
        Continue
    }
    If ($AdUserObject) {
        If ($UserSha1HashMapping.Keys -Contains $Username) {
            $UserSha1HashMapping[$Username] += $CertificateThumbprint
        } Else {
            $UserSha1HashMapping[$Username] = @($CertificateThumbprint)
```

```

    }
  }
}

ForEach ($User in $UserSha1HashMapping.Keys) {
    Write-Output "Mapping altSecurityIdentity for $User"
    $UserObject = Get-ADUser -Identity $User | Get-ADObject -Properties
    'altSecurityIdentities'
    $altSecurityIdentities = $UserObject.altSecurityIdentities
    ForEach ($thumbprint in $UserSha1HashMapping[$User]) {
        $SHA1PUKEY = "X509:<SHA1-PUKEY>$thumbprint"
        If ($altSecurityIdentities -Contains $SHA1PUKEY) {
            Write-Output "Skipping $thumbprint, already mapped."
            Continue
        }
        Write-Output "Adding $thumbprint to $User as altSecurityIdentity"
        Set-ADUser -Identity $User -Add @{'altSecurityIdentities'=$SHA1PUKEY}
    }
}

```

Langkah selanjutnya

- Uji otentikasi berbasis sertifikat dengan sertifikat yang dipetakan
- Konfigurasi aplikasi Anda untuk menggunakan sertifikat yang dipetakan untuk otentikasi
- [Pantau iklan Microsoft yang AWS Dikelola](#) untuk acara otentikasi

Mengatur AWS Private CA Konektor untuk AD untuk Microsoft AD yang AWS Dikelola

Anda dapat mengintegrasikan Microsoft AD yang AWS Dikelola dengan [AWS Private Certificate Authority \(CA\)](#) untuk menerbitkan dan mengelola sertifikat untuk pengontrol domain Direktori Aktif, pengguna yang bergabung dengan domain, grup, dan mesin. AWS Private CA Connector for Active Directory memungkinkan Anda menggunakan pengganti AWS Private CA drop-in yang dikelola sepenuhnya untuk perusahaan yang dikelola sendiri CAs tanpa perlu menyebarkan, menambal, atau memperbarui agen lokal atau server proxy.

Anda dapat mengatur AWS Private CA integrasi dengan direktori Anda melalui Directory Service konsol, konsol AWS Private CA Connector for Active Directory, atau dengan memanggil [CreateTemplate](#) API. Untuk mengatur integrasi Private CA melalui konsol AWS Private CA

Connector for Active Directory, lihat [Membuat template konektor](#). Lihat langkah-langkah berikut tentang cara mengatur integrasi ini dari Directory Service konsol.

Menyiapkan AWS Private CA Konektor untuk AD

Untuk membuat konektor CA Pribadi untuk Active Directory

1. Masuk ke Konsol Manajemen AWS dan buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah tab Manajemen Aplikasi dan bagian AWS aplikasi & layanan, pilih AWS Private CA Konektor untuk AD.
4. Pada halaman Create Private CA certificate for Active Directory, selesaikan langkah-langkah untuk membuat konektor Private CA for Active Directory.

Untuk informasi selengkapnya, lihat [Membuat konektor](#).

Melihat AWS Private CA Konektor untuk AD

Untuk melihat detail konektor CA Pribadi

1. Masuk ke Konsol Manajemen AWS dan buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah tab Manajemen Aplikasi dan bagian AWS aplikasi & layanan, lihat konektor CA Pribadi Anda dan CA Pribadi terkait. Bidang berikut menampilkan:
 - a. AWS Private CA Connector ID — Pengidentifikasi unik untuk AWS Private CA konektor. Pilih untuk melihat halaman detail.
 - b. AWS Private CA subjek — Informasi mengenai nama yang dibedakan untuk CA. Pilih untuk melihat halaman detail.
 - c. Status - Hasil pemeriksaan status untuk AWS Private CA Konektor dan AWS Private CA:
 - Aktif — Kedua cek lulus
 - 1/2 pemeriksaan gagal - Satu pemeriksaan gagal
 - Gagal - Kedua pemeriksaan gagal

Untuk detail status yang gagal, arahkan kursor ke hyperlink untuk melihat pemeriksaan mana yang gagal.

- d. Status Pendaftaran Sertifikat DC - Pemeriksaan status untuk status sertifikat pengontrol domain:
 - Diaktifkan - Pendaftaran sertifikat diaktifkan
 - Dinonaktifkan - Pendaftaran sertifikat dinonaktifkan
- e. Tanggal dibuat — Saat AWS Private CA Konektor dibuat.

Untuk informasi selengkapnya, lihat [Lihat detail konektor](#).

Tabel berikut menunjukkan status yang berbeda untuk pendaftaran sertifikat pengontrol domain untuk AWS Microsoft AD Terkelola dengan. AWS Private CA

Status pendaftar an DC	Deskripsi	Tindakan yang diperlukan
Diaktifkan	Sertifikat pengontrol domain berhasil didaftarkan ke direktori Anda.	Tidak ada tindakan diperlukan.
Gagal	Pengaktifan atau penonaktifan pendaftaran sertifikat pengontrol domain gagal untuk direktori Anda.	Jika tindakan pengaktifan Anda gagal, coba lagi dengan mematikan sertifikat pengontrol domain dan kemudian nyalakan lagi. Jika tindakan penonaktifan Anda gagal, coba lagi dengan mengaktifkan sertifikat pengontrol domain dan kemudian matikan lagi. Jika percobaan ulang gagal, hubungi AWS Support.
Terganggu	Pengontrol domain memiliki masalah konektivitas jaringan yang berkomunikasi dengan AWS Private CA titik akhir.	Periksa kebijakan endpoint AWS Private CA VPC dan bucket S3 untuk mengizinkan konektivitas jaringan dengan direktori Anda. Untuk informasi selengkapnya,

Status pendaftar an DC	Deskripsi	Tindakan yang diperlukan
		lihat Memecahkan masalah pesan pengecualian Otoritas Sertifikat AWS Pribadi dan Memecahkan masalah pencabutan AWS Private CA sertifikat.
Nonaktif	Pendaftaran sertifikat pengontro l domain berhasil dimatikan untuk direktori Anda.	Tidak ada tindakan diperlukan.
Menonaktifkan	Penonaktifan pendaftaran sertifikat pengontrol domain sedang berlangsung.	Tidak ada tindakan diperlukan.
Mengaktifkan	Pengaktifan pendaftaran sertifikat pengontrol domain sedang berlangsung.	Tidak ada tindakan diperlukan.

Mengkonfigurasi Kebijakan AD

AWS Private CA Konektor untuk AD harus dikonfigurasi sehingga pengontrol dan objek domain Microsoft AD yang AWS dikelola dapat meminta dan menerima sertifikat. Konfigurasi objek kebijakan grup ([GPO](#)) agar AWS Private CA dapat mengeluarkan sertifikat ke objek Microsoft AD yang AWS Dikelola.

Mengkonfigurasi kebijakan Direktori Aktif untuk pengontrol domain

Aktifkan kebijakan Direktori Aktif untuk pengontrol domain

1. Buka tab Jaringan & Keamanan.
2. Pilih AWS Private CA Konektor.
3. Pilih konektor yang ditautkan ke AWS Private CA subjek yang mengeluarkan sertifikat pengontrol domain ke direktori Anda.
4. Pilih Tindakan, Aktifkan sertifikat pengontrol domain.

 Important

Konfigurasi templat pengontrol domain yang valid sebelum Anda mengaktifkan sertifikat pengontrol domain untuk menghindari pembaruan yang tertunda.

Setelah Anda mengaktifkan pendaftaran sertifikat pengontrol domain, pengontrol domain direktori Anda meminta dan menerima sertifikat dari AWS Private CA Connector for AD.

Untuk mengubah penerbitan AWS Private CA sertifikat pengontrol domain, pertama-tama hubungkan yang baru AWS Private CA ke direktori Anda menggunakan AWS Private CA Konektor baru untuk AD. Sebelum Anda mengaktifkan pendaftaran sertifikat pada yang baru AWS Private CA, matikan pendaftaran sertifikat pada yang sudah ada:

Matikan sertifikat pengontrol domain

1. Buka tab Jaringan & Keamanan.
2. Pilih AWS Private CA Konektor.
3. Pilih konektor yang ditautkan ke AWS Private CA subjek yang mengeluarkan sertifikat pengontrol domain ke direktori Anda.
4. Pilih Tindakan, Nonaktifkan sertifikat pengontrol domain.

Mengkonfigurasi kebijakan Direktori Aktif untuk pengguna, komputer, dan mesin yang bergabung dengan domain

Konfigurasi objek kebijakan grup

1. Connect ke instans admin Microsoft AD yang AWS dikelola dan buka [Server Manager](#) dari menu Start.
2. Di bawah Alat, pilih Manajemen Kebijakan Grup.
3. Di bawah Hutan dan Domain, temukan unit organisasi subdomain (OU) Anda (misalnya, corp adalah unit organisasi subdomain Anda jika Anda mengikuti prosedur yang diuraikan [Membuat Microsoft AD yang AWS Dikelola](#)) dan klik kanan pada OU subdomain Anda. Pilih Buat GPO di domain ini, dan tautkan di sini dan masukkan PCA GPO untuk namanya. Pilih OK.
4. GPO yang baru dibuat muncul mengikuti nama subdomain Anda. Klik kanan PCA GPO dan pilih Edit. Jika kotak dialog terbuka dengan pesan peringatan yang menyatakan Ini adalah tautan

dan bahwa perubahan disebarkan secara global, akui pesan tersebut dengan memilih OK untuk melanjutkan. Jendela Editor Manajemen Kebijakan Grup terbuka.

5. Di jendela Editor Manajemen Kebijakan Grup, buka Konfigurasi Komputer > Kebijakan > Pengaturan Windows > Pengaturan Keamanan > Kebijakan Kunci Publik (pilih folder).
6. Di bawah Object Type, pilih Certificate Services Client - Certificate Enrollment Policy.
7. Di jendela Certificate Services Client - Certificate Enrollment Policy, ubah Model Konfigurasi menjadi Diaktifkan.
8. Konfirmasikan bahwa Kebijakan Pendaftaran Direktori Aktif dipilih dan Diaktifkan. Pilih Tambahkan.
9. Kotak dialog Server Kebijakan Pendaftaran Sertifikat terbuka. Masukkan titik akhir server kebijakan pendaftaran sertifikat yang Anda buat saat membuat konektor di bidang URI kebijakan server Enter enrollment. Biarkan Jenis Otentikasi sebagai Windows terintegrasi.
10. Pilih Validasi. Setelah validasi berhasil, pilih Tambah.
11. Kembali ke kotak dialog Certificate Services Client - Certificate Enrollment Policy dan pilih kotak di samping konektor yang baru dibuat untuk memastikan bahwa konektor adalah kebijakan pendaftaran default.
12. Pilih Kebijakan Pendaftaran Direktori Aktif dan pilih Hapus.
13. Di kotak dialog konfirmasi, pilih Ya untuk menghapus otentikasi berbasis LDAP.
14. Pilih Terapkan dan kemudian OK di jendela Certificate Services Client - Certificate Enrollment Policy. Kemudian tutup jendelanya.
15. Di bawah Object Type for the Public Key Policies folder, pilih Certificate Services Client - Auto-Enrollment.
16. Ubah opsi Model Konfigurasi ke Diaktifkan.
17. Konfirmasikan bahwa Perpanjang sertifikat kedaluwarsa dan opsi Perbarui Sertifikat keduanya dipilih. Biarkan pengaturan lain apa adanya.
18. Pilih Terapkan, lalu OK, dan tutup kotak dialog.

Selanjutnya, konfigurasikan Kebijakan Kunci Publik untuk konfigurasi pengguna dengan mengulangi langkah 6-17 di bagian Konfigurasi Pengguna> Kebijakan > Pengaturan Windows> Pengaturan Keamanan > Kebijakan Kunci Publik.

Setelah Anda selesai mengonfigurasi GPOs dan Kebijakan Kunci Publik, objek dalam domain meminta sertifikat dari AWS Private CA Connector for AD dan menerima sertifikat yang dikeluarkan oleh AWS Private CA.

Mengkonfirmasi AWS Private CA mengeluarkan sertifikat

Proses untuk memperbarui AWS Private CA untuk menerbitkan sertifikat untuk Microsoft AD yang AWS Dikelola dapat memakan waktu hingga 8 jam.

Anda dapat melakukan salah satu dari yang berikut:

- Anda bisa menunggu periode waktu ini.
- Anda dapat memulai ulang mesin gabungan domain Microsoft AD AWS Terkelola yang dikonfigurasi untuk menerima sertifikat dari AWS Private CA. Kemudian Anda dapat mengonfirmasi sertifikat yang AWS Private CA telah diterbitkan kepada anggota domain Microsoft AD AWS Terkelola Anda dengan mengikuti prosedur dalam [Microsoft dokumentasi](#).
- Anda dapat menggunakan PowerShell perintah berikut untuk memperbarui sertifikat untuk Microsoft AD yang AWS Dikelola:

```
certutil -pulse
```

Pantau iklan Microsoft yang AWS Dikelola

Anda bisa mendapatkan hasil maksimal dari iklan Microsoft AWS Terkelola dengan mempelajari lebih lanjut tentang berbagai status iklan Microsoft AWS Terkelola dan apa artinya bagi iklan Microsoft AWS Terkelola Anda. Anda juga dapat menggunakan AWS layanan seperti Amazon Simple Notification Service dan Amazon CloudWatch untuk memantau iklan Microsoft yang AWS Dikelola. Amazon Simple Notification Service dapat mengirimkan pemberitahuan status direktori Microsoft AD yang AWS Dikelola. Amazon CloudWatch dapat memantau kinerja pengontrol domain Microsoft AD AWS Terkelola Anda.

Tugas untuk memantau iklan Microsoft AWS Terkelola

- [Memahami status direktori Microsoft AD yang AWS Dikelola](#)
- [Mengaktifkan pemberitahuan status direktori Microsoft AD AWS Terkelola dengan Amazon Simple Notification Service](#)
- [Memahami log direktori Microsoft AD yang AWS Dikelola](#)
- [Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS](#)
- [Menggunakan CloudWatch untuk memantau kinerja pengontrol domain Microsoft AD yang AWS Dikelola](#)

- [Menonaktifkan penerusan CloudWatch log Amazon untuk Microsoft AD yang Dikelola AWS](#)
- [Memantau DNS Server dengan Microsoft Event Viewer](#)

Memahami status direktori Microsoft AD yang AWS Dikelola

Berikut ini adalah berbagai status untuk direktori.

Aktif

Direktori beroperasi secara normal. Tidak ada masalah yang terdeteksi oleh Directory Service untuk direktori Anda.

Creating

Direktori saat ini sedang dibuat. Pembuatan direktori biasanya memakan waktu antara 20 sampai 45 menit tetapi dapat bervariasi tergantung pada beban sistem.

Dihapus

Direktori telah dihapus. Semua sumber daya untuk direktori telah dirilis. Setelah direktori memasuki keadaan ini, direktori tidak dapat dipulihkan.

Deleting

Direktori saat ini sedang dihapus. Direktori akan tetap dalam keadaan ini sampai benar-benar dihapus. Setelah direktori memasuki keadaan ini, operasi hapus tidak dapat dibatalkan, dan direktori tidak dapat dipulihkan.

Gagal

Direktori tidak dapat dibuat. Harap hapus direktori ini. Jika masalah ini berlanjut, hubungi [Pusat AWS Dukungan](#).

Terganggu

Direktori berjalan dalam keadaan terdegradasi. Satu atau lebih masalah telah terdeteksi, dan tidak semua operasi direktori dapat bekerja pada kapasitas operasional penuh. Terdapat banyak potensi alasan untuk keadaan direktori seperti ini. Ini termasuk aktivitas pemeliharaan operasional normal seperti patching atau rotasi EC2 instance, hot spotting sementara oleh aplikasi di salah satu pengontrol domain Anda, atau perubahan yang Anda buat pada jaringan Anda yang secara tidak sengaja mengganggu komunikasi direktori. Untuk informasi selengkapnya, lihat salah satu dari [Pemecahan Masalah AWS Microsoft AD yang Dikelola](#), [Memecahkan masalah AD](#)

[Connector](#), [Pemecahan masalah Simple AD](#). Untuk masalah terkait pemeliharaan normal, AWS selesaikan masalah ini dalam waktu 40 menit. Jika setelah meninjau topik pemecahan masalah, direktori Anda dalam keadaan Terganggu lebih dari 40 menit, kami merekomendasikan Anda untuk menghubungi [Pusat AWS Dukungan](#).

 Important

Jangan memulihkan snapshot ketika direktori dalam keadaan Terganggu. Sangatlah jarang pemulihan snapshot diperlukan untuk mengatasi gangguan. Untuk informasi selengkapnya, lihat [Memulihkan iklan Microsoft AWS Terkelola Anda dengan snapshot](#).

Diminta

Permintaan untuk membuat direktori Anda sedang tertunda.

RestoreFailed

Memulihkan direktori dari snapshot gagal. Silakan coba lagi operasi pemulihan. Jika ini berlanjut, cobalah snapshot yang berbeda, atau hubungi [AWS Dukungan Pusat](#).

Memulihkan

Direktori saat ini sedang dipulihkan dari snapshot otomatis atau manual. Memulihkan dari snapshot biasanya memakan waktu beberapa menit, tergantung pada ukuran data direktori dalam snapshot.

Mengaktifkan pemberitahuan status direktori Microsoft AD AWS Terkelola dengan Amazon Simple Notification Service

Menggunakan Amazon Simple Notification Service (Amazon SNS), Anda dapat menerima pesan email atau teks (SMS) saat status direktori Anda berubah. Anda akan diberi tahu jika direktori Anda beralih dari status Aktif ke [status Gangguan](#). Anda juga menerima notifikasi ketika direktori kembali ke status Aktif.

Cara Kerjanya

Amazon SNS menggunakan “topik” untuk mengumpulkan dan mendistribusikan pesan. Setiap topik memiliki satu atau lebih pelanggan yang menerima pesan yang telah diterbitkan untuk topik tersebut.

Dengan menggunakan langkah-langkah di bawah ini, Anda dapat menambahkan Directory Service sebagai penerbit ke topik Amazon SNS. Saat Directory Service mendeteksi perubahan dalam status direktori Anda, ia menerbitkan pesan ke topik tersebut, yang kemudian dikirim ke pelanggan topik tersebut.

Anda dapat mengaitkan beberapa direktori sebagai penerbit ke satu topik. Anda juga dapat menambahkan pesan status direktori ke topik yang sebelumnya Anda buat di Amazon SNS. Anda memiliki kendali terperinci atas siapa yang dapat menerbitkan dan berlangganan topik. Untuk informasi lengkap tentang Amazon SNS, lihat [Apa yang Dimaksud dengan Amazon SNS?](#).

Note

Pemberitahuan status direktori adalah fitur Regional dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [replikasi Multi-Region](#), prosedur berikut harus diterapkan secara terpisah di setiap Wilayah. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Mengaktifkan Amazon SNS

Berikut ini memandu Anda melalui cara mengaktifkan Amazon SNS untuk AWS Microsoft AD yang Dikelola:

1. Masuk ke Konsol Manajemen AWS dan buka [Directory Service konsol](#).
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengaktifkan olahpesan SNS, lalu pilih tab Pemeliharaan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih Tindakan, dan kemudian pilih Buat notifikasi.
5. Pada halaman Buat notifikasi, pilih Pilih jenis notifikasi, lalu pilih Buat notifikasi baru. Atau, jika Anda sudah memiliki topik SNS yang ada, Anda dapat memilih Mengasosiasikan topik SNS yang ada untuk mengirim pesan status dari direktori ini ke topik tersebut.

 Note

Jika Anda memilih Buat notifikasi baru tetapi kemudian menggunakan nama topik yang sama untuk topik SNS yang sudah ada, Amazon SNS tidak membuat topik baru, tetapi hanya menambahkan informasi langganan baru ke topik yang ada.

Jika Anda memilih Mengasosiasikan topik SNS yang ada, Anda hanya akan dapat memilih topik SNS yang ada di Region yang sama dengan direktori.

6. Pilih Jenis penerima dan masukkan informasi kontak Penerima. Jika Anda memasukkan nomor telepon untuk SMS, gunakan angka saja. Jangan menyertakan tanda hubung, spasi, atau tanda kurung.
7. (Opsional) Berikan nama untuk topik Anda dan nama tampilan SNS. Nama tampilan adalah nama pendek hingga 10 karakter yang disertakan dalam semua pesan SMS dari topik ini. Bila menggunakan opsi SMS, nama tampilan diperlukan.

 Note

Jika Anda masuk menggunakan pengguna IAM atau peran yang hanya memiliki kebijakan [DirectoryServiceFullAccess](#) terkelola, nama topik Anda harus dimulai dengan "DirectoryMonitoring". Jika Anda ingin menyesuaikan lebih lanjut nama topik Anda, Anda akan memerlukan hak istimewa tambahan untuk SNS.

8. Pilih Buat.

[Jika Anda ingin menunjuk pelanggan SNS tambahan, seperti alamat email tambahan, antrian Amazon SQS AWS Lambda atau, Anda dapat melakukan ini dari konsol Amazon SNS.](#)

Menghapus pesan status direktori dari topik Amazon SNS

Berikut ini memandu Anda tentang cara menghapus pesan status direktori Microsoft AD AWS Terkelola dari topik Amazon SNS:

1. Masuk ke Konsol Manajemen AWS dan buka [Directory Service konsol](#).
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:

- Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menghapus pesan status, lalu pilih tab Pemeliharaan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih nama topik SNS dalam daftar, pilih Tindakan, dan kemudian pilih Hapus.
 5. Pilih Hapus.

Ini akan menghapus direktori Anda sebagai penerbit untuk topik SNS yang dipilih.

Menghapus topik Amazon SNS

Jika Anda ingin menghapus seluruh topik, Anda dapat melakukan ini dari konsol [Amazon SNS](#).

Sebelum menghapus topik Amazon SNS menggunakan konsol SNS, Anda harus memastikan bahwa direktori tidak mengirim pesan status untuk topik tersebut.

Jika Anda menghapus topik Amazon SNS menggunakan konsol SNS, perubahan ini tidak akan segera tercermin dalam konsol Directory Service. Anda hanya akan diberi tahu saat berikutnya direktori menerbitkan pemberitahuan ke topik yang dihapus, dalam hal ini Anda akan melihat status yang diperbarui pada tab Pemantauan direktori yang menunjukkan topik tidak dapat ditemukan.

Oleh karena itu, untuk menghindari kehilangan pesan status direktori penting, sebelum menghapus topik apa pun yang menerima pesan dari Directory Service, kaitkan direktori Anda dengan topik Amazon SNS yang berbeda.

Untuk informasi selengkapnya tentang cara menghapus topik Amazon SNS, lihat [Menghapus topik dan langganan Amazon SNS](#).

Memahami log direktori Microsoft AD yang AWS Dikelola

Log keamanan dari instans pengontrol domain Microsoft AD AWS Terkelola diarsipkan selama satu tahun. Anda juga dapat mengonfigurasi direktori Microsoft AD AWS Terkelola untuk meneruskan log pengontrol domain ke CloudWatch Log Amazon dalam waktu dekat. Untuk informasi selengkapnya, lihat [Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS](#).

AWS mencatat peristiwa berikut untuk kepatuhan.

Kategori pemantauan	Pengaturan kebijakan	Status audit
Masuk akun	Audit Validasi Kredensial	Sukses, Gagal
	Audit Peristiwa Masuk Akun Lainnya	Sukses, Gagal
	Audit Layanan Otentikasi Kerberos	Sukses, Gagal
Pengelolaan Akun	Audit Pengelolaan Akun Komputer	Sukses, Gagal
	Audit Pengelolaan Akun Lainnya	Sukses, Gagal
	Audit Pengelolaan Grup Keamanan	Sukses, Gagal
	Audit Pengelolaan Akun Pengguna	Sukses, Gagal
Pelacakan terperinci	Audit Aktivitas DPAPI	Sukses, Gagal
	Audit Aktivitas PNP	Berhasil
	Audit Pembuatan Proses	Sukses, Gagal
Akses DS	Audit Akses Directory Service	Sukses, Gagal
	Audit Perubahan Directory Service	Sukses, Gagal
Masuk/Keluar	Audit Penguncian Akun	Sukses, Gagal
	Audit Keluar	Berhasil
	Audit Masuk	Sukses, Gagal

Kategori pemantauan	Pengaturan kebijakan	Status audit
	Audit Logon/Logoff Acara Lainnya	Sukses, Gagal
	Audit Masuk Khusus	Sukses, Gagal
Akses Objek	Audit Peristiwa Akses Objek Lainnya	Sukses, Gagal
	Audit Penyimpanan yang Dapat Dihapus	Sukses, Gagal
	Audit Pementasan Kebijakan Akses Pusat	Sukses, Gagal
Perubahan Kebijakan	Audit Perubahan Kebijakan	Sukses, Gagal
	Audit Perubahan Kebijakan Autentikasi	Sukses, Gagal
	Audit Perubahan Kebijakan Otorisasi	Sukses, Gagal
	Audit Perubahan Kebijakan Tingkat Aturan MPSSVC	Berhasil
	Audit Peristiwa Perubahan Kebijakan Lainnya	Kegagalan
Penggunaan Hak Istimewa	Audit Penggunaan Hak Istimewa Sensitif	Sukses, Gagal
Sistem	IPsec Pengemudi Audit	Sukses, Gagal
	Audit Peristiwa Sistem Lainnya	Sukses, Gagal
	Audit Perubahan Status Keamanan	Sukses, Gagal

Kategori pemantauan	Pengaturan kebijakan	Status audit
	Audit Ekstensi Sistem Keamanan	Sukses, Gagal
	Audit Integritas Sistem	Sukses, Gagal

Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS

Anda dapat menggunakan Directory Service konsol atau APIs meneruskan log peristiwa keamanan pengontrol domain ke CloudWatch Log Amazon untuk iklan Microsoft yang AWS Dikelola. Hal ini membantu Anda untuk memenuhi persyaratan kebijakan pemantauan keamanan, audit, dan penyimpanan log Anda dengan menyediakan transparansi peristiwa keamanan di direktori Anda.

CloudWatch Log juga dapat meneruskan peristiwa ini ke AWS akun, AWS layanan, atau aplikasi pihak ketiga lainnya. Hal ini memudahkan Anda untuk memantau dan mengonfigurasi peringatan secara terpusat untuk mendeteksi dan merespons secara proaktif aktivitas yang tidak biasa hampir secara real time.

Setelah diaktifkan, Anda kemudian dapat menggunakan konsol CloudWatch Log untuk mengambil data dari grup log yang Anda tentukan saat Anda mengaktifkan layanan. Grup log ini berisi log keamanan dari pengendali domain Anda.

Untuk informasi selengkapnya tentang grup log dan cara membaca datanya, lihat [Bekerja dengan grup log dan aliran log](#) di Panduan Pengguna Amazon CloudWatch Logs.

Note

Penerusan log adalah fitur Regional dari AWS Microsoft AD yang Dikelola. Jika Anda menggunakan [replikasi Multi-Region](#), prosedur berikut harus diterapkan secara terpisah di setiap Wilayah. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Setelah diaktifkan, kemampuan penerusan log akan mulai mentransmisikan log dari pengontrol domain Anda ke grup log yang ditentukan. CloudWatch Setiap log yang dibuat sebelum penerusan log diaktifkan tidak akan ditransfer ke grup CloudWatch log.

Topik

- [Menggunakan Konsol Manajemen AWS untuk mengaktifkan penerusan CloudWatch log Amazon Logs](#)
- [Menggunakan CLI atau PowerShell untuk mengaktifkan penerusan CloudWatch log Amazon Logs](#)

Menggunakan Konsol Manajemen AWS untuk mengaktifkan penerusan CloudWatch log Amazon Logs

Anda dapat mengaktifkan penerusan CloudWatch log Log Amazon untuk iklan AWS Microsoft Terkelola di. Konsol Manajemen AWS

1. Pada panel navigasi [konsol Directory Service](#), pilih Direktori.
2. Pilih ID direktori direktori Microsoft AD AWS Terkelola yang ingin Anda bagikan.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengaktifkan penerusan log, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Penerusan log, pilih Aktifkan.
5. Pada Aktifkan penerusan log ke CloudWatch dialog, pilih salah satu opsi berikut:
 - a. Pilih Buat grup CloudWatch log baru, di bawah Nama grup CloudWatch log, tentukan nama yang dapat Anda rujuk di CloudWatch Log.
 - b. Pilih Pilih grup CloudWatch log yang ada, dan di bawah Grup CloudWatch log yang ada, pilih grup log dari menu.
6. Tinjau informasi harga dan tautan, lalu pilih Aktifkan.

Menggunakan CLI atau PowerShell untuk mengaktifkan penerusan CloudWatch log Amazon Logs

Sebelum Anda dapat menggunakan [ds create-log-subscription](#) perintah, Anda harus terlebih dahulu membuat grup CloudWatch log Amazon dan kemudian membuat kebijakan sumber daya IAM yang akan memberikan izin yang diperlukan untuk grup itu. Untuk mengaktifkan penerusan log menggunakan CLI atau PowerShell, selesaikan langkah-langkah berikut.

Langkah 1: Buat grup log di CloudWatch Log

Membuat grup log yang akan digunakan untuk menerima log keamanan dari pengendali domain Anda. Kami merekomendasikan pra-pending nama dengan `/aws/directoryservice/`, tapi hal tersebut tidak diperlukan. Contoh:

CLI Command

```
aws logs create-log-group --log-group-name '/aws/directoryservice/d-1111111111'
```

PowerShell Command

```
New-CWLogGroup -LogGroupName '/aws/directoryservice/d-1111111111'
```

Untuk petunjuk tentang cara membuat grup CloudWatch Log, lihat [Membuat grup CloudWatch log di Log](#) di Panduan Pengguna CloudWatch Log Amazon.

Langkah 2: Buat kebijakan sumber daya CloudWatch Log di IAM

Buat kebijakan sumber daya CloudWatch Log yang memberikan Directory Service hak untuk menambahkan log ke grup log baru yang Anda buat di Langkah 1. Anda dapat menentukan ARN yang tepat ke grup log untuk membatasi Directory Service akses ke grup log lain atau menggunakan kartu liar untuk menyertakan semua grup log. Kebijakan contoh berikut menggunakan metode wild card untuk mengidentifikasi bahwa semua grup log yang dimulai dengan `/aws/directoryservice/` untuk AWS akun tempat direktori Anda berada akan disertakan.

Anda harus menyimpan kebijakan ini ke file teks (misalnya `DSPolicy.json`) di workstation lokal Anda karena Anda harus menjalankannya dari CLI. Contoh:

CLI Command

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-document  
file://DSPolicy.json
```

PowerShell Command

```
$PolicyDocument = Get-Content .\DSPolicy.json -Raw
```

```
Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument  
$PolicyDocument
```

Langkah 3: Buat langganan Directory Service log

Dalam langkah terakhir ini, Anda sekarang dapat melanjutkan untuk mengaktifkan penerusan log dengan membuat langganan log. Contoh:

CLI Command

```
aws ds create-log-subscription --directory-id 'd-1111111111' --log-group-name '/aws/  
directoryservice/d-1111111111'
```

PowerShell Command

```
New-DSLogSubscription -DirectoryId 'd-1111111111' -LogGroupName '/aws/  
directoryservice/d-1111111111'
```

Menggunakan CloudWatch untuk memantau kinerja pengontrol domain Microsoft AD yang AWS Dikelola

Directory Service terintegrasi dengan Amazon CloudWatch untuk membantu memberi Anda metrik kinerja penting untuk setiap pengontrol domain di Direktori Aktif Anda. Ini berarti Anda dapat memantau penghitung kinerja pengontrol domain, seperti pemanfaatan CPU dan memori. Anda juga dapat mengonfigurasi alarm dan memulai tindakan otomatis untuk merespons periode pemanfaatan tinggi. Misalnya, Anda dapat mengonfigurasi alarm untuk pemanfaatan CPU pengontrol domain di atas 70 persen dan membuat topik SNS untuk memberi tahu Anda ketika ini terjadi. Anda dapat menggunakan topik SNS ini untuk memulai otomatisasi, seperti AWS Lambda fungsi, untuk meningkatkan jumlah pengontrol domain ke Direktori Aktif Anda.

Untuk informasi selengkapnya tentang memantau pengontrol domain Anda, lihat [Menentukan kapan harus menambahkan pengontrol domain dengan metrik CloudWatch](#).

Ada biaya yang terkait dengan Amazon CloudWatch. Untuk informasi lebih lanjut, lihat [CloudWatch penagihan dan biaya](#).

 Important

Metrik kinerja pengontrol domain dengan tidak CloudWatch tersedia di Wilayah Kanada Barat (Calgary).

Untuk mengaktifkan CloudWatch, lihat [Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS](#).

Menemukan metrik kinerja pengontrol domain di CloudWatch

Di CloudWatch konsol Amazon, metrik untuk layanan tertentu dikelompokkan terlebih dahulu berdasarkan namespace layanan. Anda dapat menambahkan filter metrik yang berada di bawah namespace tersebut. Gunakan prosedur berikut untuk menemukan namespace dan metrik subordinat yang benar yang diperlukan untuk menyiapkan metrik pengontrol domain AWS Microsoft AD yang Dikelola. CloudWatch

Untuk menemukan metrik pengontrol domain di konsol CloudWatch

1. Masuk ke Konsol Manajemen AWS dan buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pada panel navigasi, silakan pilih Metrik.
3. Dari daftar metrik, pilih namespace Directory Service, lalu dari daftar, pilih metrik AWS Microsoft AD yang dikelola.

Untuk petunjuk tentang cara mengatur metrik pengontrol domain menggunakan CloudWatch konsol, lihat [Cara mengotomatiskan penskalaan AWS Microsoft AD Terkelola berdasarkan metrik pemanfaatan di Blog Keamanan. AWS](#)

Menentukan kapan harus menambahkan pengontrol domain dengan metrik CloudWatch

Load balancing di semua pengontrol domain Anda penting untuk ketahanan dan kinerja Direktori Aktif Anda. Untuk membantu mengoptimalkan kinerja pengontrol domain Anda di Microsoft AD yang AWS Dikelola, sebaiknya Anda memantau metrik penting terlebih dahulu CloudWatch untuk membentuk garis dasar. Selama proses ini, Anda menganalisis Active Directory Anda dari waktu ke waktu untuk mengidentifikasi rata-rata dan puncak penggunaan Active Directory Anda. Setelah menentukan

baseline, Anda dapat memantau metrik ini secara teratur untuk membantu menentukan kapan harus menambahkan pengontrol domain ke Direktori Aktif Anda.

Metrik berikut ini penting untuk dipantau secara teratur. Untuk daftar lengkap metrik pengontrol domain yang tersedia CloudWatch, lihat [AWS Penghitung kinerja Microsoft AD yang dikelola](#).

- Metrik spesifik pengontrol domain, seperti:
 - Prosesor
 - Memori
 - Disk Logis
 - Antarmuka Jaringan
- AWS Metrik khusus direktori Microsoft AD yang dikelola, seperti:
 - Pencarian LDAP
 - Mengikat
 - Kueri DNS
 - Direktori dibaca
 - Direktori menulis

Untuk petunjuk tentang cara mengatur metrik pengontrol domain menggunakan CloudWatch konsol, lihat [Cara mengotomatiskan penskalaan AWS Microsoft AD Terkelola berdasarkan metrik pemanfaatan di](#) Blog Keamanan. AWS Untuk informasi umum tentang metrik di CloudWatch, lihat [Menggunakan CloudWatch metrik Amazon](#) di CloudWatch Panduan Pengguna Amazon.

Untuk informasi umum tentang perencanaan pengontrol domain, lihat [Perencanaan kapasitas untuk Layanan Domain Direktori Aktif](#) di situs web Microsoft.

AWS Penghitung kinerja Microsoft AD yang dikelola

Tabel berikut mencantumkan semua penghitung kinerja yang tersedia di Amazon CloudWatch untuk melacak pengontrol domain dan kinerja direktori di Microsoft AD yang AWS Dikelola.

Kategori metrik	Nama metrik
Database ==> Contoh (NTDSA)	Database Cache% Hit
	Database I/O Membaca Latensi Rata-rata

Kategori metrik	Nama metrik
DirectoryServices (NTDS)	I/O Database Reads/sec
	I/O Log Menulis Latensi Rata-rata
	Waktu Mengikat LDAP
	Operasi Replikasi Tertunda DRA
	Sinkronisasi Replikasi Tertunda DRA
DNS	Pertanyaan rekursif/detik
	Kegagalan Kueri Rekursif/detik
	Kueri TCP Diterima/detik
	Total Kueri yang Diterima/detik
	Total Respon Dikirim/detik
LogicalDisk	Kueri UDP Diterima/detik
	Rata-rata. Panjang Antrean Cakram
Memori	% Ruang Bebas
	% Byte Berkomitmen dalam Penggunaan
	Seumur Hidup Cache Siaga Rata-Rata Jangka Panjang
Antarmuka Jaringan	Byte dikirim/detik
	Byte Diterima/detik
	Bandwidth saat ini
NTDS	ATQ Estimasi Penundaan Antrian
	Latensi Permintaan ATQ

Kategori metrik	Nama metrik
	Direktori DS Membaca/Detik
	Pencarian Direktori DS/Detik
	Direktori DS Tulisan/Detik
	Sesi Klien LDAP
	Pencarian LDAP/DETIK
	Ikatan Sukses LDAP/detik
Prosesor	% Waktu Prosesor
Statistik Seluruh Sistem Keamanan	Otentikasi Kerberos
	Otentikasi NTLM

Menonaktifkan penerusan CloudWatch log Amazon untuk Microsoft AD yang Dikelola AWS

Anda dapat menonaktifkan penerusan CloudWatch log Log untuk iklan AWS Microsoft Terkelola di file. Konsol Manajemen AWS Untuk informasi lebih lanjut tentang penerusan log, lihat [the section called “Menggunakan CloudWatch untuk memantau direktori Anda”](#)

1. Pada panel navigasi [konsol Directory Service](#), pilih Direktori.
2. Pilih ID direktori direktori Microsoft AD AWS Terkelola yang ingin Anda bagikan.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menonaktifkan penerusan log, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Penerusan log, pilih Nonaktifkan.
5. Setelah Anda membaca informasi dalam dialog Nonaktifkan penerusan log, pilih Nonaktifkan.

Memantau DNS Server dengan Microsoft Event Viewer

Anda dapat mengaudit peristiwa DNS Microsoft AD AWS Terkelola, sehingga memudahkan identifikasi dan pemecahan masalah DNS. Misalnya, jika catatan DNS hilang, Anda dapat menggunakan log peristiwa audit DNS untuk membantu mengidentifikasi akar masalah dan memperbaiki masalah. Anda juga dapat menggunakan log peristiwa audit DNS untuk meningkatkan keamanan dengan mendeteksi dan memblokir permintaan dari alamat IP yang mencurigakan.

Untuk melakukan itu, Anda harus masuk dengan akun Admin atau dengan akun yang merupakan anggota dari grup Administrator Sistem Nama Domain AWS . Untuk informasi selengkapnya tentang grup ini, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).

Untuk mengakses Event Viewer untuk Microsoft AD DNS AWS Terkelola

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Di panel navigasi kiri, pilih Instans.
3. Temukan EC2 instans Amazon yang digabungkan ke direktori AD Microsoft AWS Terkelola Anda. Pilih instans, lalu pilih Hubungkan.
4. Setelah terhubung ke EC2 instans Amazon, buka menu Start dan pilih folder Windows Administrative Tools. Di dalam folder Alat Administratif, pilih Penampil Acara.
5. Di jendela Penampil peristiwa, pilih Tindakan lalu pilih Hubungkan ke Komputer Lain.
6. Pilih Komputer lain, ketik salah satu nama server Microsoft AD DNS AWS Terkelola atau alamat IP Anda, dan pilih OK.
7. Di panel sebelah kiri, arahkan ke Log Aplikasi dan Layanan>Microsoft>Windows>DNS-Server, dan kemudian pilih Audit.

Akses ke AWS aplikasi dan layanan dari Microsoft AD yang AWS Dikelola

Anda dapat memberikan akses ke pengguna Microsoft AD yang AWS Dikelola untuk mengakses AWS aplikasi dan layanan. Beberapa AWS aplikasi dan layanan ini meliputi:

- Amazon Chime
- Amazon EC2
- Cepat

- Konsol Manajemen AWS
- Amazon WorkSpaces

Anda juga dapat menggunakan akses URLs dan sistem masuk tunggal dengan AWS Microsoft AD yang Dikelola.

Tugas untuk mengakses AWS aplikasi dan layanan dari Microsoft AD yang AWS Dikelola

- [Kompatibilitas aplikasi untuk Microsoft AD yang AWS Dikelola](#)
- [Mengaktifkan akses ke AWS aplikasi dan layanan untuk Microsoft AD yang AWS Dikelola](#)
- [Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola](#)
- [Membuat URL akses untuk Microsoft AD yang AWS Dikelola](#)
- [Mengaktifkan sistem masuk tunggal untuk Microsoft AD yang Dikelola AWS](#)

Kompatibilitas aplikasi untuk Microsoft AD yang AWS Dikelola

AWS Directory Service untuk Microsoft Active Directory (AWS Managed Microsoft AD) kompatibel dengan beberapa AWS layanan dan aplikasi pihak ketiga.

Berikut ini adalah daftar AWS aplikasi dan layanan yang kompatibel:

- Amazon Chime
- Amazon Connect
- Amazon EC2
- Cepat
- Amazon RDS
- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS IAM Identity Center
- AWS License Manager
- Konsol Manajemen AWS
- FSx untuk Windows File Server
- WorkSpaces

Untuk informasi selengkapnya, lihat [Mengaktifkan akses ke AWS aplikasi dan layanan untuk Microsoft AD yang AWS Dikelola](#).

Karena besarnya off-the-shelf aplikasi kustom dan komersial yang menggunakan Active Directory, AWS tidak dan tidak dapat melakukan verifikasi formal atau luas kompatibilitas aplikasi pihak ketiga dengan AWS Directory Service untuk Microsoft Active Directory (AWS Managed Microsoft AD). Meskipun AWS bekerja dengan pelanggan dalam upaya untuk mengatasi tantangan instalasi aplikasi potensial yang mungkin mereka hadapi, kami tidak dapat menjamin bahwa aplikasi apa pun atau akan terus kompatibel dengan Microsoft AD yang AWS Dikelola.

Aplikasi pihak ketiga berikut ini kompatibel dengan Microsoft AD yang AWS Dikelola:

- Aktivasi Berbasis Direktori Aktif (ADBA)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- Application Server (.NET)
- Microsoft Entra(sebelumnya dikenal sebagai Azure Active Directory (AzureAD))
- Microsoft Entra Connect(sebelumnya dikenal sebagai) Azure Active Directory Connect
- Distributed File System Replication (DFSR)
- Distributed File System Namespaces (DFS-N)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(termasuk SQL Server Selalu Pada Grup Ketersediaan)
- Microsoft System Center Configuration Manager(SCCM) - Pengguna yang menggunakan SCCM harus menjadi anggota grup Administrator Manajemen Sistem AWS Delegasi.
- Microsoft Windows and Windows Server OS
- Office 365

Perhatikan bahwa tidak semua konfigurasi dari aplikasi-aplikasi ini mungkin didukung.

Pedoman kompatibilitas

Meskipun aplikasi mungkin memiliki konfigurasi yang tidak kompatibel, konfigurasi deployment aplikasi sering dapat mengatasi ketidakcocokan. Berikut ini menjelaskan alasan paling umum untuk

ketidakcocokan aplikasi. Pelanggan dapat menggunakan informasi ini untuk menyelidiki karakteristik kompatibilitas aplikasi yang diinginkan dan mengidentifikasi perubahan deployment yang potensial.

- Administrator domain atau izin istimewa lainnya – Beberapa aplikasi menyatakan bahwa Anda harus menginstalnya sebagai administrator domain. Karena AWS harus mempertahankan kontrol eksklusif tingkat izin ini untuk memberikan Active Directory sebagai layanan terkelola, Anda tidak dapat bertindak sebagai administrator domain untuk menginstal aplikasi tersebut. Namun, Anda sering dapat menginstal aplikasi tersebut dengan mendelegasikan izin khusus, kurang istimewa, dan AWS didukung kepada orang yang melakukan instalasi. Untuk detail selengkapnya tentang izin yang tepat yang diperlukan aplikasi Anda, tanyakan penyedia aplikasi Anda. Untuk informasi selengkapnya tentang izin yang AWS memungkinkan Anda mendelegasikan, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#)
- Akses ke container Active Directory yang memiliki hak istimewa — Di dalam direktori Anda, Microsoft AD yang AWS dikelola menyediakan Unit Organisasi (OU) di mana Anda memiliki kontrol administratif penuh. Anda tidak memiliki izin membuat atau menulis dan mungkin memiliki izin baca terbatas untuk kontainer yang lebih tinggi di pohon Direktori Aktif daripada OU Anda. Aplikasi yang membuat atau mengakses kontainer yang tidak Anda miliki izinnya mungkin tidak bekerja. Namun, aplikasi semacam itu sering memiliki kemampuan untuk menggunakan kontainer yang Anda buat di OU Anda sebagai alternatif. Periksa dengan penyedia aplikasi Anda untuk menemukan cara untuk membuat dan menggunakan kontainer di OU Anda sebagai alternatif. Untuk informasi lebih lanjut tentang OU Anda, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).
- Perubahan skema selama alur kerja instalasi — Beberapa aplikasi Direktori Aktif memerlukan perubahan skema Direktori Aktif default, dan mereka mungkin mencoba untuk menginstal perubahan tersebut sebagai bagian dari alur kerja instalasi aplikasi. Karena sifat istimewa ekstensi skema, AWS memungkinkan hal ini dengan mengimpor file Lightweight Directory Interchange Format (LDIF) melalui konsol Directory Service, CLI, atau SDK saja. Aplikasi semacam itu sering datang dengan file LDIF yang dapat Anda terapkan ke direktori melalui proses pembaruan Directory Service skema. Untuk informasi selengkapnya tentang bagaimana proses impor LDIF bekerja, lihat [Tutorial: Memperluas skema AD Microsoft AWS Terkelola Anda](#). Anda dapat menginstal aplikasi dengan cara untuk memotong instalasi skema selama proses instalasi.

Aplikasi tidak kompatibel dikenal

Berikut daftar off-the-shelf aplikasi komersial yang biasa diminta yang belum kami temukan konfigurasi yang berfungsi dengan Microsoft AD yang AWS Dikelola. AWS memperbarui daftar ini dari waktu ke waktu atas kebijakannya sendiri sebagai sopan santun untuk membantu Anda

menghindari upaya yang tidak produktif. AWS memberikan informasi ini tanpa jaminan atau klaim mengenai kompatibilitas saat ini atau masa depan.

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

Mengaktifkan akses ke AWS aplikasi dan layanan untuk Microsoft AD yang AWS Dikelola

Pengguna dapat mengotorisasi Microsoft AD yang AWS Dikelola untuk memberikan AWS aplikasi dan layanan, seperti Amazon WorkSpaces, akses ke Direktori Aktif Anda. AWS Aplikasi dan layanan berikut dapat diaktifkan atau dinonaktifkan untuk bekerja dengan Microsoft AD yang AWS Dikelola.

AWS aplikasi/layanan	Informasi selengkapnya...
Amazon Chime	Untuk informasi selengkapnya, lihat Menghubungkan ke Direktori Aktif .
Amazon Connect	Untuk informasi selengkapnya, lihat Panduan Administrasi Amazon Connect .
Amazon EC2	Untuk informasi selengkapnya, lihat Cara untuk bergabung dengan instans Amazon EC2 ke AWS Microsoft AD yang Dikelola .
Amazon FSx untuk Server File Windows	Untuk informasi selengkapnya, lihat Menggunakan Amazon FSx dengan AWS Directory Service untuk Microsoft Active Directory .
Cepat	Untuk informasi selengkapnya, lihat edisi Menggunakan Active Directory with Quick Enterprise .
Amazon Relational Database Service	Untuk informasi selengkapnya, lihat berikut ini:

AWS aplikasi/layanan	Informasi selengkapnya...
	• Menggunakan otentikasi Kerberos untuk MySQL • Menggunakan otentikasi Kerberos dengan Amazon RDS for Oracle • Menggunakan otentikasi Kerberos dengan Amazon RDS for PostgreSQL • Bekerja dengan Microsoft AD yang AWS Dikelola dengan Amazon RDS for SQL Server
Amazon WorkDocs	Untuk informasi selengkapnya, lihat Aktifkan Amazon WorkDocs untuk iklan Microsoft yang AWS Dikelola .
Amazon WorkMail	Untuk informasi selengkapnya, lihat Membuat organisasi .
Amazon WorkSpaces	Anda dapat membuat Simple AD, AWS Managed Microsoft AD, atau AD Connector langsung dari WorkSpaces. Cukup luncurkan Pengaturan Advanced saat membuat Workspace Anda. Untuk informasi selengkapnya, lihat Daftar Directory Service direktori yang ada dengan WorkSpaces Personal.
AWS Client VPN	Untuk informasi selengkapnya, lihat otentikasi Active Directory di Client VPN .
AWS IAM Identity Center	Untuk informasi selengkapnya, lihat Connect to a Microsoft AD direktori .
AWS License Manager	Untuk informasi selengkapnya, lihat Mengelola langganan berbasis pengguna di License Manager .

AWS aplikasi/layanan	Informasi selengkapnya...
Konsol Manajemen AWS	Untuk informasi selengkapnya, lihat Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola .
AWS Private Certificate Authority	Untuk informasi selengkapnya, lihat AWS Private CA Konektor untuk Direktori Aktif .
AWS Transfer Family	Untuk informasi selengkapnya, lihat Mengkonfigurasi titik akhir server SFTP, FTPS, atau FTP .

Setelah diaktifkan, Anda mengelola akses ke direktori Anda di konsol dari aplikasi atau layanan yang ingin Anda berikan akses ke direktori Anda.

Temukan AWS aplikasi dan layanan

Untuk menemukan AWS aplikasi dan layanan yang dijelaskan sebelumnya di Directory Service konsol, lakukan langkah-langkah berikut.

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Tinjau daftar di bawah bagian aplikasi & layanan AWS .

Untuk informasi selengkapnya tentang cara mengotorisasi atau membatalkan otorisasi AWS aplikasi dan layanan yang digunakan Directory Service, lihat. [Otorisasi untuk AWS aplikasi dan layanan menggunakan Directory Service](#)

Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola

Directory Service memungkinkan Anda untuk memberikan anggota direktori Anda akses ke Konsol Manajemen AWS. Secara default, anggota direktori Anda tidak memiliki akses ke AWS sumber daya apa pun. Anda menetapkan peran IAM ke anggota direktori Anda untuk memberi mereka akses ke berbagai AWS layanan dan sumber daya. IAM role menentukan layanan, sumber daya, dan tingkat akses yang dimiliki anggota direktori Anda.

Sebelum Anda dapat memberikan akses konsol ke anggota direktori Anda, direktori Anda harus memiliki URL akses. Untuk informasi selengkapnya tentang cara melihat detail direktori dan mendapatkan URL akses Anda, lihat [Melihat informasi direktori Microsoft AD yang AWS Dikelola](#). Untuk informasi selengkapnya tentang cara membuat URL akses, lihat [Membuat URL akses untuk Microsoft AD yang AWS Dikelola](#).

Untuk informasi selengkapnya tentang cara membuat dan menetapkan IAM role untuk anggota direktori Anda, lihat [Memberikan pengguna dan grup Microsoft AD AWS Terkelola akses ke AWS sumber daya dengan peran IAM](#).

Topik

- [Mengaktifkan akses Konsol Manajemen AWS](#)
- [Menonaktifkan akses Konsol Manajemen AWS](#)
- [Mengatur panjang sesi Konsol Manajemen AWS login](#)

Artikel Blog AWS Keamanan Terkait

- [Cara Mengakses Iklan Microsoft yang Konsol Manajemen AWS AWS Dikelola dan Kredensial Lokal Anda](#)

AWS re:Post Artikel terkait

- [Bagaimana cara memberikan akses ke untuk pengguna Active Directory lokal? Konsol Manajemen AWS](#)

Note

Akses ke Konsol Manajemen AWS adalah fitur Regional dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [replikasi Multi-Region](#), prosedur berikut harus diterapkan secara terpisah di setiap Wilayah. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Mengaktifkan akses Konsol Manajemen AWS

Secara default, akses konsol tidak diaktifkan untuk direktori apapun. Untuk mengaktifkan akses konsol untuk pengguna dan grup direktori Anda, lakukan langkah-langkah berikut:

Untuk mengaktifkan akses konsol

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Wilayah yang ditampilkan di bawah replikasi Multi-Region, pilih Wilayah tempat Anda ingin mengaktifkan akses ke Konsol Manajemen AWS, lalu pilih tab Manajemen aplikasi. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah bagian Konsol Manajemen AWS, pilih Aktifkan. Akses konsol sekarang diaktifkan untuk direktori Anda.

Important

Sebelum pengguna dapat masuk ke konsol dengan URL akses Anda, Anda harus terlebih dahulu menambahkan pengguna Anda ke peran IAM. Untuk informasi umum tentang menetapkan pengguna ke IAM role, lihat [Menetapkan pengguna atau grup ke peran IAM yang ada](#). Setelah IAM role telah ditetapkan, pengguna kemudian dapat mengakses konsol tersebut menggunakan URL akses Anda. Misalnya, jika URL akses direktori Anda `example-corp.awsapps.com`, URL untuk mengakses konsol adalah `https://example-corp.awsapps.com/console/`.

Menonaktifkan akses Konsol Manajemen AWS

Untuk menonaktifkan Konsol Manajemen AWS akses bagi pengguna dan grup direktori Microsoft AD AWS Terkelola, lakukan langkah-langkah berikut:

Untuk menonaktifkan akses konsol

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:

- Jika Anda memiliki beberapa Wilayah yang ditampilkan di bawah replikasi Multi-Region, pilih Wilayah tempat Anda ingin menonaktifkan akses ke Konsol Manajemen AWS, lalu pilih tab Manajemen aplikasi. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah bagian Konsol Manajemen AWS, pilih Menonaktifkan. Akses konsol sekarang dinonaktifkan untuk direktori Anda.
 5. Jika setiap IAM role telah ditetapkan untuk pengguna atau grup dalam direktori, tombol Nonaktifkan mungkin tidak tersedia. Dalam kasus ini, Anda harus menghapus semua penetapan IAM role untuk direktori sebelum melanjutkan, termasuk tugas untuk pengguna atau grup dalam direktori Anda yang telah dihapus, yang akan ditampilkan sebagai Pengguna Dihapus atau Grup Dihapus.

Setelah semua penetapan IAM role dihapus, ulangi langkah-langkah di atas.

Mengatur panjang sesi Konsol Manajemen AWS login

Secara default, pengguna memiliki waktu 1 jam untuk menggunakan sesi mereka setelah berhasil masuk Konsol Manajemen AWS sebelum mereka keluar. Setelah itu, pengguna harus masuk lagi untuk memulai sesi 1 jam berikutnya sebelum keluar lagi. Anda dapat menggunakan prosedur berikut untuk mengubah lama waktu hingga 12 jam per sesi.

Untuk mengatur panjang sesi Konsol Manajemen AWS login

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengatur lamanya sesi, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah bagian Aplikasi & layanan AWS, pilih Konsol Manajemen AWS.
5. Di kotak dialog Kelola Akses ke AWS Sumber Daya, pilih Lanjutkan.

6. Di halaman Menetapkan pengguna dan grup ke IAM role, di bawah Atur lamanya sesi masuk, edit nilai bernomor, dan kemudian pilih Simpan.

Membuat URL akses untuk Microsoft AD yang AWS Dikelola

URL akses digunakan dengan AWS aplikasi dan layanan, seperti Amazon WorkDocs, untuk mencapai halaman login yang terkait dengan direktori Anda. Anda dapat membuat URL akses untuk direktori Anda dengan melakukan langkah-langkah berikut.

Pertimbangan-pertimbangan

- URL harus unik secara global.
- URL akses hanya dapat dikonfigurasi dari Wilayah Utama saat menggunakan direktori Multi-Region.
- Setelah Anda membuat URL akses aplikasi untuk direktori ini, itu tidak dapat diubah. Setelah URL akses dibuat, tidak dapat digunakan oleh orang lain. Jika Anda menghapus direktori Anda, URL akses juga dihapus dan kemudian dapat digunakan oleh akun lain.

Untuk membuat URL akses

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Wilayah yang ditampilkan di bawah replikasi Multi-Region, pilih Wilayah Utama dan kemudian pilih tab Manajemen aplikasi. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bagian URL akses aplikasi, jika URL akses belum ditetapkan ke direktori, tombol Buat ditampilkan. Masukkan alias direktori dan pilih Buat. Jika error Entitas Sudah Ada dikembalikan, alias direktori tertentu telah dialokasikan. Pilih alias lain dan ulangi prosedur ini.

URL akses Anda ditampilkan dalam format `<alias>.awsapps.com`. Secara default, URL ini akan membawa Anda ke halaman login untuk WorkDocs.

Mengaktifkan sistem masuk tunggal untuk Microsoft AD yang Dikelola AWS

AWS Directory Service memberikan kemampuan untuk memungkinkan pengguna Anda mengakses WorkDocs dari komputer yang bergabung ke direktori tanpa harus memasukkan kredensialnya secara terpisah.

Sebelum mengaktifkan sing-on tunggal, Anda perlu mengambil langkah tambahan agar peramban web pengguna dapat mendukung sign-on tunggal. Pengguna mungkin perlu memodifikasi pengaturan peramban web mereka untuk mengaktifkan sign-on tunggal.

Note

Sign-on tunggal hanya bekerja bila digunakan pada komputer yang digabungkan ke direktori Directory Service . Ini tidak dapat digunakan pada komputer yang tidak bergabung ke direktori.

Jika direktori Anda adalah direktori AD Connector dan akun layanan AD Connector tidak memiliki izin untuk menambahkan atau menghapus atribut nama utama layanannya, maka untuk Langkah 5 dan 6 di bawah ini, Anda memiliki dua pilihan:

1. Anda dapat melanjutkan dan akan diminta untuk nama pengguna dan kata sandi untuk pengguna direktori yang memiliki izin ini untuk menambah atau menghapus atribut nama utama layanan pada akun layanan AD Connector. Kredensial ini hanya digunakan untuk mengaktifkan sign-on tunggal dan tidak disimpan oleh layanan. Izin akun layanan AD Connector tidak berubah.
2. Anda dapat mendelegasikan izin untuk mengizinkan akun layanan AD Connector menambah atau menghapus atribut nama utama layanan itu sendiri, Anda dapat menjalankan PowerShell perintah di bawah ini dari komputer yang bergabung dengan domain menggunakan akun yang memiliki izin untuk mengubah izin pada akun layanan AD Connector. Perintah di bawah ini akan memberikan akun layanan AD Connector kemampuan untuk menambah dan menghapus atribut nama utama layanan hanya untuk dirinya sendiri.

```
$AccountName = 'ConnectorAccountName'  
# DO NOT modify anything below this comment.  
# Getting Active Directory information.  
Import-Module 'ActiveDirectory'  
$RootDse = Get-ADRootDSE
```



```
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
  $RootDse.SchemaNamingContext -Filter { LDAPDisplayName -eq 'servicePrincipalName' } -
  Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
  $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
  Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
  'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
  'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Untuk mengaktifkan atau menonaktifkan sistem masuk tunggal dengan WorkDocs

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bagian URL akses aplikasi, pilih Aktifkan untuk mengaktifkan sistem masuk tunggal.
WorkDocs

Jika Anda tidak melihat tombol Aktifkan, Anda mungkin harus terlebih dahulu membuat URL Akses sebelum opsi ini akan ditampilkan. Untuk informasi selengkapnya tentang cara membuat URL akses, lihat [Membuat URL akses untuk Microsoft AD yang AWS Dikelola](#).

5. Di kotak dialog Aktifkan Sign-On Tunggal untuk direktori ini,, pilih Aktifkan. Sign-on tunggal diaktifkan untuk direktori.
6. Jika nanti Anda ingin menonaktifkan sistem masuk tunggal dengan WorkDocs, pilih Nonaktifkan, dan kemudian di kotak dialog Nonaktifkan Single Sign-On untuk direktori ini, pilih Nonaktifkan lagi.

Topik

- [Sign-on tunggal untuk IE dan Chrome](#)
- [Sign-on tunggal untuk Firefox](#)

Sign-on tunggal untuk IE dan Chrome

Untuk mengizinkan peramban Microsoft Internet Explorer (IE) dan Google Chrome untuk mendukung sign-on tunggal, tugas berikut harus dilakukan pada komputer klien:

- Tambahkan URL akses Anda (mis., <https://<alias>.awsapps.com>) ke daftar situs yang disetujui untuk sistem masuk tunggal.
- Aktifkan skrip aktif (JavaScript).
- Izinkan masuk otomatis.
- Aktifkan autentikasi terintegrasi.

Anda atau pengguna Anda dapat melakukan tugas-tugas ini secara manual, atau Anda dapat mengubah pengaturan ini menggunakan pengaturan Kebijakan Grup.

Topik

- [Pembaruan manual untuk sign-on tunggal pada Windows](#)
- [Pembaruan manual untuk sign-on tunggal pada OS X](#)
- [Pengaturan kebijakan grup untuk sign-on tunggal](#)

Pembaruan manual untuk sign-on tunggal pada Windows

Untuk mengaktifkan sign-on tunggal secara manual pada komputer Windows, lakukan langkah-langkah berikut pada komputer klien. Beberapa pengaturan ini mungkin sudah diatur dengan benar.

Cara mengaktifkan sign-on tunggal untuk Internet Explorer dan Chrome secara manual di Windows

1. Untuk membuka kotak dialog Properti internet, pilih menu Start, ketik Internet Options di kotak pencarian, lalu pilih Opsi Internet.
2. Tambahkan URL akses Anda ke daftar situs yang disetujui untuk sign-on tunggal dengan melakukan langkah-langkah berikut:
 - a. Di kotak dialog Properti internet, pilih tab Keamanan.
 - b. Pilih Intranet lokal dan pilih Situs.
 - c. Di kotak dialog Intranet lokal, pilih Advanced.
 - d. Tambahkan URL akses Anda ke daftar situs web dan pilih tutup.
 - e. Di dialog box Intranet lokal, pilih OK.

3. Untuk mengaktifkan penulisan aktif, lakukan langkah-langkah berikut ini:
 - a. Di tab Keamanan dari kotak dialog Properti internet, pilih Tingkat kustom.
 - b. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, gulir ke bawah untuk Penulisan dan pilih Aktifkan di bawah Penulisan aktif.
 - c. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.
4. Untuk mengaktifkan masuk otomatis, lakukan langkah-langkah berikut ini:
 - a. Di tab Keamanan dari kotak dialog Properti internet, pilih Tingkat kustom.
 - b. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, gulir ke bawah untuk Autentikasi Pengguna dan pilih Masuk otomatis hanya di zona Intranet di bawah Masuk.
 - c. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.
 - d. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.
5. Untuk mengaktifkan autentikasi terintegrasi, lakukan langkah-langkah berikut ini:
 - a. Di kotak dialog Properti internet, pilih tab Advanced.
 - b. Gulir ke bawah ke Keamanan dan pilih Mengaktifkan Autentikasi Windows Terintegrasi.
 - c. Di kotak dialog Properti Internet, pilih OK.
6. Tutup dan buka kembali peramban Anda agar perubahan ini berlaku.

Pembaruan manual untuk sign-on tunggal pada OS X

Untuk mengaktifkan sign-on tunggal secara manual untuk Chrome pada OS X, lakukan langkah-langkah berikut pada komputer klien. Anda memerlukan hak administrator di komputer Anda untuk menyelesaikan langkah-langkah ini.

Cara mengaktifkan sign-on tunggal untuk Chrome di OS X secara manual

1. Tambahkan URL akses Anda ke [AuthServerAllowlist](#) kebijakan dengan menjalankan perintah berikut:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Buka Preferensi Sistem, buka panel Profil, dan hapus profil Chrome Kerberos Configuration.
3. Mulai ulang Chrome dan buka `chrome://policy` di Chrome untuk mengonfirmasi bahwa pengaturan baru sudah terpasang.

Pengaturan kebijakan grup untuk sign-on tunggal

Administrator domain dapat menerapkan pengaturan Kebijakan Grup untuk membuat perubahan sign-on tunggal pada komputer klien yang digabungkan ke domain.

Note

Jika Anda mengelola browser web Chrome di komputer di domain Anda dengan kebijakan Chrome, Anda harus menambahkan URL akses ke [AuthServerAllowlist](#) kebijakan. Untuk informasi selengkapnya tentang mengatur kebijakan Chrome, kunjungi [Pengaturan Kebijakan di Chrome](#).

Cara mengaktifkan sign-on tunggal untuk Internet Explorer dan Chrome menggunakan pengaturan Kebijakan Grup

1. Membuat objek Kebijakan Grup baru dengan melakukan langkah-langkah berikut:
 - a. Buka alat Pengelolaan Kebijakan Grup, arahkan ke domain Anda, lalu pilih Objek Kebijakan Grup.
 - b. Dari menu utama, pilih Tindakan dan pilih Baru.
 - c. Di kotak dialog GPO baru, masukkan nama deskriptif untuk objek Kebijakan Grup, seperti IAM Identity Center Policy, dan biarkan Sumber Starter GPO diatur ke (tidak ada). Klik OK.
2. Tambahkan URL akses ke daftar situs yang disetujui untuk sign-on tunggal dengan melakukan langkah-langkah berikut:
 - a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.
 - b. Di pohon kebijakan, arahkan ke Konfigurasi Pengguna > Preferensi > Pengaturan Windows.
 - c. Di daftar Pengaturan Windows, buka menu konteks (klik kanan) untuk Registri dan pilih Item registri baru.
 - d. Di kotak dialog Properti Registri Baru, masukkan pengaturan berikut dan pilih OK:

Tindakan

Update

Sarang

HKEY_CURRENT_USER

Jalan

Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com*<alias>*

Nilai untuk *<alias>* berasal dari URL akses Anda. Jika URL akses Anda adalah `https://examplecorp.awsapps.com`, alias adalah `examplecorp`, dan kunci registri akan menjadi `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

Nama nilai

https

Jenis nilai

REG_DWORD

Data nilai

1

3. Untuk mengaktifkan penulisan aktif, lakukan langkah-langkah berikut ini:
 - a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.
 - b. Di pohon kebijakan, arahkan ke Konfigurasi komputer > Kebijakan > Templat Administrasi > Komponen Windows > Internet Explorer > Panel Kontrol Internet > Halaman Keamanan > Zona Intranet.
 - c. Di daftar Zona Intranet, buka menu konteks (klik kanan) untuk Izinkan penulisan aktif dan pilih Edit.
 - d. Di kotak dialog Izinkan penulisan aktif, masukkan pengaturan berikut dan pilih OK:
 - Pilih tombol radio Diaktifkan.
 - Di bawah Opsi atur Izinkan penulisan aktif ke Aktifkan.
4. Untuk mengaktifkan masuk otomatis, lakukan langkah-langkah berikut ini:

- a. Pada alat Pengelolaan Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan SSO Anda, lalu pilih Edit.
 - b. Di pohon kebijakan, arahkan ke Konfigurasi komputer > Kebijakan > Templat Administrasi > Komponen Windows > Internet Explorer > Panel Kontrol Internet > Halaman Keamanan > Zona Intranet.
 - c. Di daftar Zona Intranet, buka menu konteks (klik kanan) untuk Opsi masuk dan pilih Edit.
 - d. Di kotak dialog Opsi masuk, masukkan pengaturan berikut dan pilih OK:
 - Pilih tombol radio Diaktifkan.
 - Di bawah Opsi atur Opsi masuk ke Masuk otomatis hanya di zona Intranet.
5. Untuk mengaktifkan autentikasi terintegrasi, lakukan langkah-langkah berikut ini:
- a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.
 - b. Di pohon kebijakan, arahkan ke Konfigurasi Pengguna > Preferensi > Pengaturan Windows.
 - c. Di daftar Pengaturan Windows, buka menu konteks (klik kanan) untuk Registri dan pilih Item registri baru.
 - d. Di kotak dialog Properti Registri Baru, masukkan pengaturan berikut dan pilih OK:

Tindakan

Update

Sarang

HKEY_CURRENT_USER

Jalan

Software\Microsoft\Windows\CurrentVersion\Internet Settings

Nama nilai

EnableNegotiate

Jenis nilai

REG_DWORD

Data nilai

1

6. Tutup jendela Editor Pengelolaan Kebijakan Grup jika masih terbuka.
7. Tetapkan kebijakan baru ke domain Anda dengan mengikuti langkah-langkah berikut:
 - a. Di pohon Pengelolaan Kebijakan Grup, buka menu konteks (klik kanan) untuk domain Anda, lalu pilih Menautkan GPO yang Ada.
 - b. Dalam daftar Objek Kebijakan Grup, pilih kebijakan Pusat Identitas IAM Anda dan pilih OK.

Perubahan ini akan berlaku setelah pembaruan Kebijakan Grup berikutnya pada klien, atau waktu berikutnya pengguna masuk.

Sign-on tunggal untuk Firefox

Untuk mengizinkan browser Mozilla Firefox mendukung sistem masuk tunggal, tambahkan URL akses Anda (mis., <https://<alias>.awsapps.com>) ke daftar situs yang disetujui untuk sistem masuk tunggal. Ini bisa dilakukan secara manual, atau otomatis dengan skrip.

Topik

- [Pembaruan manual untuk sign-on tunggal](#)
- [Pembaruan otomatis untuk sign-on tunggal](#)

Pembaruan manual untuk sign-on tunggal

Untuk menambahkan URL akses Anda ke daftar situs yang disetujui di Firefox secara manual, lakukan langkah-langkah berikut pada komputer klien.

Untuk menambahkan URL akses Anda secara manual ke daftar situs yang disetujui di Firefox

1. Buka Firefox dan buka halaman `about:config`.
2. Buka preferensi `network.negotiate-auth.trusted-uris` dan tambahkan URL akses Anda ke daftar situs. Gunakan koma (,) untuk memisahkan beberapa entri.

Pembaruan otomatis untuk sign-on tunggal

Sebagai administrator domain, Anda dapat menggunakan skrip untuk menambahkan URL akses ke preferensi pengguna `network.negotiate-auth.trusted-uris` Firefox pada semua komputer di jaringan Anda. Untuk informasi lebih lanjut, kunjungi <https://support.mozilla.org/en-US/questions/939037>.

Memberikan pengguna dan grup Microsoft AD AWS Terkelola akses ke AWS sumber daya dengan peran IAM

AWS Directory Service menyediakan kemampuan untuk memberi pengguna dan grup Microsoft AD AWS Terkelola Anda akses ke AWS layanan dan sumber daya, seperti akses ke konsol Amazon EC2. Mirip dengan memberikan akses kepada pengguna IAM untuk mengelola direktori seperti yang dijelaskan dalam [Kebijakan berbasis identitas \(kebijakan IAM\)](#), agar pengguna di direktori Anda memiliki akses ke AWS sumber daya lain, seperti Amazon EC2, Anda harus menetapkan peran dan kebijakan IAM kepada pengguna dan grup tersebut. Untuk informasi selengkapnya, lihat [peran IAM](#) dalam Panduan Pengguna IAM.

Untuk informasi tentang cara memberi pengguna akses ke Konsol Manajemen AWS, lihat [Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola](#).

Topik

- [Membuat peran IAM baru](#)
- [Mengedit hubungan kepercayaan untuk peran IAM yang ada](#)
- [Menetapkan pengguna atau grup ke peran IAM yang ada](#)
- [Melihat pengguna dan grup yang ditetapkan ke peran](#)
- [Menghapus pengguna atau grup dari peran IAM](#)
- [Menggunakan kebijakan AWS terkelola dengan Directory Service](#)

Membuat peran IAM baru

Jika Anda perlu membuat peran IAM baru untuk digunakan Directory Service, Anda harus membuatnya menggunakan konsol IAM. Setelah peran dibuat, Anda kemudian harus mengatur hubungan kepercayaan dengan peran itu sebelum Anda dapat melihat peran itu di Directory Service konsol. Untuk informasi selengkapnya, lihat [Mengedit hubungan kepercayaan untuk peran IAM yang ada](#).

 Note

Pengguna yang melakukan tugas ini harus memiliki izin untuk melakukan tindakan IAM berikut. Untuk informasi selengkapnya, lihat [Kebijakan berbasis identitas \(kebijakan IAM\)](#).

- saya: PassRole
- saya: GetRole
- saya: CreateRole
- saya: PutRolePolicy

Untuk membuat peran baru di konsol IAM

1. Di panel navigasi konsol IAM, pilih Peran. Untuk informasi selengkapnya, lihat [Membuat Peran \(Konsol Manajemen AWS\)](#) dalam Panduan Pengguna IAM.
2. Pilih Buat peran.
3. Di bawah Pilih layanan yang akan menggunakan peran ini, pilih Directory Service, lalu pilih Berikutnya.
4. Pilih kotak centang di samping kebijakan (misalnya, Amazon EC2 FullAccess) yang ingin Anda terapkan ke pengguna direktori, lalu pilih Berikutnya.
5. Jika perlu, tambahkan tanda ke peran, lalu pilih Selanjutnya.
6. Berikan Nama peran dan opsional Deskripsi, lalu pilih Buat peran.

Contoh: Buat peran untuk mengaktifkan Konsol Manajemen AWS akses

Daftar periksa berikut memberikan contoh tugas yang harus Anda selesaikan untuk membuat peran IAM baru yang akan memberi pengguna AWS Microsoft AD Terkelola tertentu akses ke konsol Amazon EC2.

1. Buat peran dengan konsol IAM menggunakan prosedur di atas. Saat diminta untuk kebijakan, pilih Amazon EC2 FullAccess.
2. Gunakan langkah-langkah di [Mengedit hubungan kepercayaan untuk peran IAM yang ada](#) untuk mengedit peran yang baru saja Anda buat, dan kemudian tambahkan informasi hubungan kepercayaan yang diperlukan ke dokumen kebijakan. Langkah ini diperlukan agar peran terlihat segera setelah Anda mengaktifkan akses ke Konsol Manajemen AWS langkah berikutnya.

- Ikuti langkah-langkah di [Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola](#) untuk mengkonfigurasi akses umum ke Konsol Manajemen AWS.
- Ikuti langkah-langkah di [Menetapkan pengguna atau grup ke peran IAM yang ada](#) untuk menambahkan pengguna yang membutuhkan akses penuh ke sumber daya EC2 untuk peran baru.

Mengedit hubungan kepercayaan untuk peran IAM yang ada

Anda dapat menetapkan peran IAM yang ada untuk Directory Service pengguna dan grup Anda. Untuk melakukan ini, bagaimanapun, peran tersebut harus memiliki hubungan kepercayaan dengan Directory Service. Saat Anda menggunakan Directory Service untuk membuat peran menggunakan prosedur di [Membuat peran IAM baru](#), hubungan kepercayaan ini diatur secara otomatis.

Note

Anda hanya perlu membangun hubungan kepercayaan ini untuk IAM role yang tidak dibuat oleh Directory Service.

Untuk membangun hubungan kepercayaan untuk peran IAM yang ada Directory Service

- Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
- Di panel navigasi konsol IAM, di bawah Manajemen akses, pilih Peran.

Konsol tersebut menampilkan peran di akun Anda.

- Pilih nama peran yang ingin Anda ubah, dan sekali di halaman peran, pilih tab Trust relationship.
- Pilih Edit kebijakan kepercayaan.
- Di bawah Edit kebijakan kepercayaan, tempel yang berikut ini, lalu pilih Perbarui kebijakan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
```

```
"Principal": {  
  "Service": "ds.amazonaws.com"  
},  
"Action": "sts:AssumeRole"  
}  
]  
}
```

Anda juga dapat memperbarui dokumen kebijakan ini menggunakan AWS CLI. Untuk informasi selengkapnya, lihat [perbarui kepercayaan](#) di Referensi Perintah.AWS CLI

Menetapkan pengguna atau grup ke peran IAM yang ada

Anda dapat menetapkan peran IAM yang ada ke pengguna atau grup AWS Microsoft AD yang Dikelola. Untuk melakukan ini, pastikan Anda telah menyelesaikan yang berikut ini.

Prasyarat

- [Buat iklan Microsoft yang AWS Dikelola](#).
- [Buat pengguna IAM](#) atau [buat grup IAM](#).
- [Ciptakan peran](#) yang memiliki hubungan kepercayaan dengan Directory Service. Untuk peran IAM yang ada, Anda perlu [mengedit hubungan kepercayaan untuk peran yang ada](#).

Important

Akses untuk pengguna Microsoft AD AWS Terkelola dalam grup bersarang dalam direktori Anda tidak didukung. Anggota grup induk memiliki akses konsol, tetapi anggota grup anak tidak.

Untuk menetapkan pengguna atau grup Microsoft AD yang AWS Dikelola ke peran IAM yang ada

1. Di panel navigasi [AWS Directory Service konsol](#), di bawah Active Directory, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - a. Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.

- b. Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin membuat tugas Anda, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
4. Gulir ke bawah ke Konsol Manajemen AWS bagian, pilih Tindakan dan Aktifkan.
5. Di bawah bagian Akses konsol delegasi, pilih nama peran IAM untuk peran IAM yang ada yang ingin Anda tetapkan kepada pengguna.
6. Pada halaman Peran yang dipilih, di bawah Mengelola pengguna dan grup untuk peran ini, pilih Tambahkan.
7. Pada halaman Menambahkan pengguna dan grup ke peran, di bawah Pilih Forest Direktori Aktif, pilih salah satu forest Microsoft AD yang Dikelola AWS (forest ini) atau forest on-premise (forest terpercaya), mana saja yang berisi di mana akun yang memerlukan akses ke Konsol Manajemen AWS. Untuk informasi selengkapnya tentang cara mengatur forest terpercaya, lihat [Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri](#).
8. Di bawah Tentukan pengguna atau grup mana yang akan ditambahkan, pilih salah satu Temukan dengan pengguna atau Temukan dengan grup, dan kemudian ketik nama pengguna atau grup. Dalam daftar kecocokan yang mungkin, pilih pengguna atau grup yang ingin Anda tambahkan.
9. Pilih Tambahkan untuk menyelesaikan penetapan pengguna dan grup ke peran.

Melihat pengguna dan grup yang ditetapkan ke peran

Untuk melihat pengguna dan grup AD Microsoft AWS Terkelola yang ditetapkan ke peran IAM, lakukan langkah-langkah berikut.

Prasyarat

- [Buat iklan Microsoft yang AWS Dikelola](#).
- [Buat pengguna IAM](#) atau [buat grup IAM](#).
- [Ciptakan peran](#) yang memiliki hubungan kepercayaan dengan Directory Service. Untuk peran IAM yang ada, Anda perlu [mengedit hubungan kepercayaan untuk peran yang ada](#).
- [Tetapkan pengguna atau grup Anda ke peran IAM yang ada](#).

Untuk melihat pengguna Microsoft AD AWS terkelola dan grup yang ditetapkan ke peran IAM

1. Di panel navigasi [AWS Directory Service konsol](#), di bawah Active Directory, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - a. Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin melihat tugas Anda, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - b. Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Gulir ke bawah ke Konsol Manajemen AWS bagian. Status harus diaktifkan. Jika tidak, pilih Actions dan Enable. Untuk informasi selengkapnya, lihat [Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola](#).

 Note

Anda tidak akan melihat grup atau pengguna apa pun jika Konsol Manajemen AWS dinonaktifkan.

5. Di bawah bagian Akses Konsol Delegasi, pilih hyperlink peran IAM yang ingin Anda lihat. Atau, Anda dapat memilih Lihat kebijakan di IAM untuk melihat kebijakan IAM di konsol IAM.
6. Pada halaman Peran yang dipilih, di bagian Kelola pengguna dan grup untuk peran ini, Anda dapat melihat pengguna dan grup yang ditetapkan ke peran IAM.

Menghapus pengguna atau grup dari peran IAM

Untuk menghapus pengguna atau grup Microsoft AD AWS Terkelola dari peran IAM, lakukan langkah-langkah berikut.

Untuk menghapus pengguna atau grup dari peran IAM

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:

- a. Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menghapus tugas Anda, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - b. Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah Konsol Manajemen AWS bagian ini, pilih peran IAM yang ingin Anda hapus pengguna dan grup.
 5. Pada halaman Peran yang dipilih, di bawah Mengelola pengguna dan grup untuk peran ini, pilih pengguna atau grup untuk menghapus peran dan pilih Hapus. Peran dihapus dari pengguna dan grup tertentu, namun peran tersebut tidak dihapus dari akun Anda.

 Note

Jika Anda ingin menghapus peran, lihat [Menghapus peran atau profil instance](#).

Menggunakan kebijakan AWS terkelola dengan Directory Service

Directory Service menyediakan kebijakan AWS terkelola berikut untuk memberi pengguna dan grup Anda akses ke AWS layanan dan sumber daya, seperti akses ke EC2 konsol Amazon. Anda harus masuk ke Konsol Manajemen AWS sebelum Anda dapat melihat kebijakan ini.

- [Akses hanya baca](#)
- [Akses pengguna daya](#)
- [Directory Service akses penuh](#)
- [Directory Service akses baca saja](#)
- [AWS Directory Service Data akses penuh](#)
- [AWS Directory Service Data hanya membaca akses](#)
- [Akses penuh Amazon Cloud Directory](#)
- [Akses hanya baca Amazon Cloud Directory](#)
- [Akses EC2 penuh Amazon](#)
- [Akses hanya EC2 baca Amazon](#)
- [Amazon VPC akses penuh](#)
- [Akses hanya baca Amazon VPC](#)

- [Amazon RDS akses penuh](#)
- [Akses hanya baca Amazon RDS](#)
- [Amazon DynamoDB akses penuh](#)
- [Amazon DynamoDB hanya membaca akses](#)
- [Amazon S3 akses penuh](#)
- [Akses hanya baca Amazon S3](#)
- [AWS CloudTrail akses penuh](#)
- [AWS CloudTrail akses baca saja](#)
- [Akses CloudWatch penuh Amazon](#)
- [Akses hanya CloudWatch baca Amazon](#)
- [Amazon CloudWatch Logs akses penuh](#)
- [Amazon CloudWatch Logs hanya membaca akses](#)

Untuk informasi selengkapnya tentang cara membuat kebijakan Anda sendiri, lihat [Contoh kebijakan untuk mengelola AWS sumber daya](#) di Panduan Pengguna IAM.

Konfigurasi replikasi Multi-Wilayah untuk AWS Microsoft AD yang Dikelola

Replikasi Multi-Region dapat digunakan untuk secara otomatis mereplikasi data direktori AWS Microsoft AD Terkelola Anda di beberapa Wilayah AWS Replikasi ini dapat meningkatkan kinerja bagi pengguna dan aplikasi di lokasi geografis yang tersebar. AWS Microsoft AD yang dikelola menggunakan replikasi Active Directory asli untuk mereplikasi data direktori Anda dengan aman ke Wilayah baru.

Replikasi Multi-Region hanya didukung untuk Edisi Perusahaan AWS Microsoft AD yang Dikelola.

Anda dapat menggunakan replikasi Multi-wilayah otomatis di sebagian besar Wilayah tempat AWS Microsoft AD Terkelola tersedia.

Note

Replikasi Multi-Wilayah tidak tersedia di Wilayah keikutsertaan berikut:

- Middle East (Bahrain) me-south-1

- Timur Tengah (UEA) me-central-1

Untuk informasi selengkapnya tentang opt-in Regions dan cara mengaktifkannya, lihat [Menentukan yang dapat digunakan akun Wilayah AWS Anda](#) dalam AWS Account Management Panduan.

Important

Anda hanya dapat memperluas replikasi Multi-Region ke Wilayah tambahan jika Region utama Anda adalah Region AWS default. Jika Wilayah utama Anda adalah Wilayah keikutsertaan, Anda tidak dapat menambahkan Wilayah tambahan ke replikasi Multi-Wilayah Anda. Pastikan direktori Anda awalnya dibuat di Wilayah AWS default sebelum mencoba memperluas replikasi.

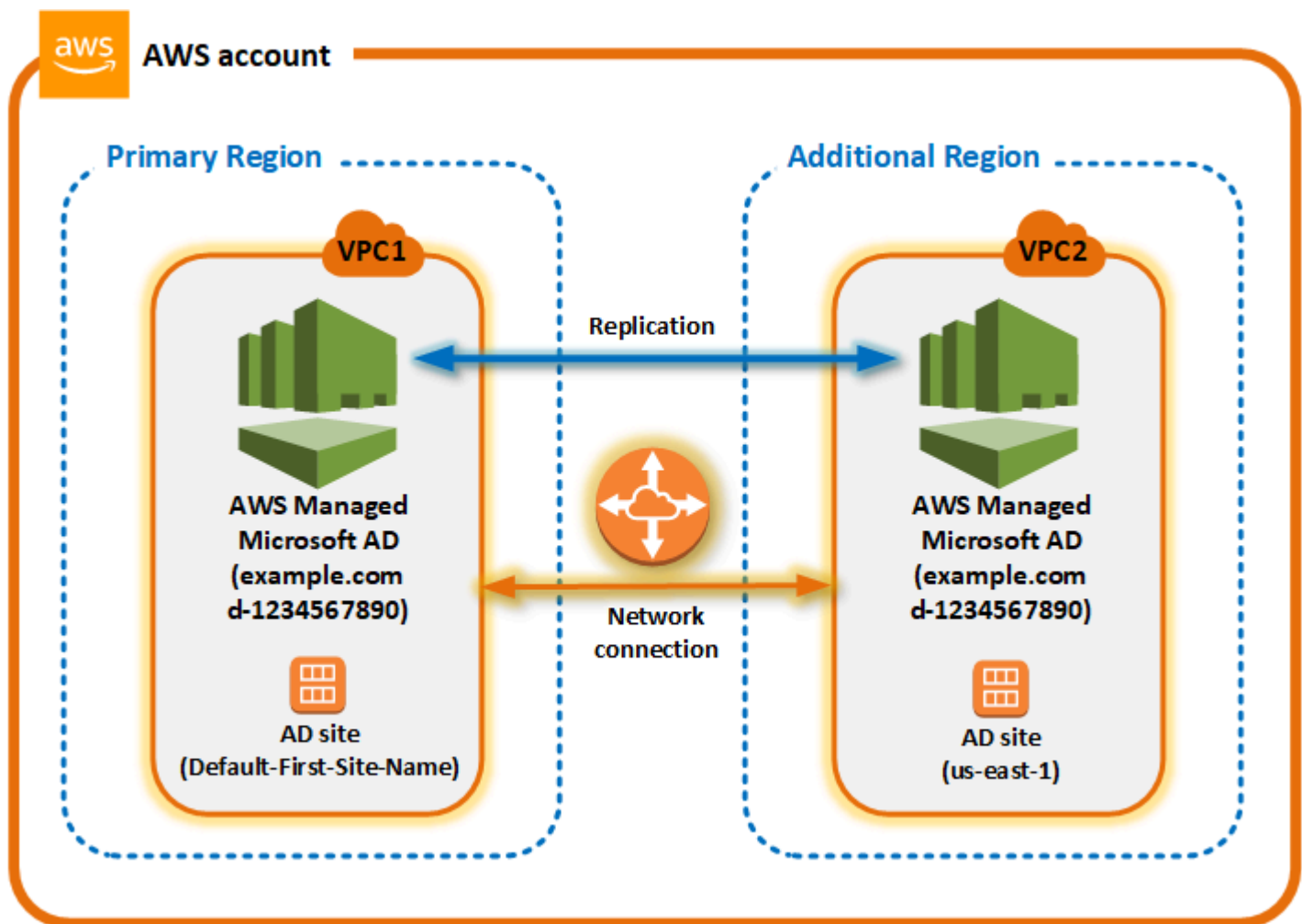
Cara kerja replikasi Multi-Region

Dengan fitur replikasi Multi-Region, AWS Microsoft AD yang Dikelola menghilangkan beban berat yang tidak terdiferensiasi dalam mengelola infrastruktur Direktori Aktif global. Saat dikonfigurasi, AWS mereplikasi semua data direktori pelanggan termasuk pengguna, grup, kebijakan grup, dan skema di beberapa Wilayah AWS.

Setelah Region baru telah ditambahkan, operasi berikut secara otomatis terjadi seperti yang ditunjukkan dalam ilustrasi:

- AWS Microsoft AD yang dikelola membuat dua pengontrol domain di VPC yang dipilih dan menerapkannya ke Wilayah baru di akun yang sama. AWS Pengidentifikasi direktori Anda (`directory_id`) tetap sama di semua Region. Anda dapat menambahkan pengendali domain tambahan nanti jika Anda ingin.
- AWS Microsoft AD yang dikelola mengonfigurasi koneksi jaringan antara Wilayah utama dan Wilayah baru.
- AWS Microsoft AD yang dikelola membuat situs Direktori Aktif baru dan memberinya nama yang sama dengan Wilayah, seperti `us-east-1`. Anda juga dapat mengubah nama ini nanti menggunakan Situs dan Alat layanan Direktori Aktif.

- AWS Microsoft AD yang dikelola mereplikasi semua objek dan konfigurasi Direktori Aktif ke Wilayah baru, termasuk pengguna, grup, kebijakan grup, kepercayaan Direktori Aktif, unit organisasi, dan skema Direktori Aktif. Tautan situs Direktori Aktif dikonfigurasi untuk menggunakan [Notifikasi Perubahan](#). Dengan perubahan notifikasi antara situs diaktifkan, perubahan menyebar ke situs jarak jauh dengan frekuensi yang sama yang mereka sebar dalam situs sumber, termasuk perubahan yang menjamin replikasi urgen.
- Jika ini adalah Wilayah pertama yang Anda tambahkan, Microsoft AD yang AWS Dikelola membuat semua fitur Multi-wilayah sadar. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).



Situs Direktori Aktif

Replikasi Multi-Region mendukung beberapa situs Direktori Aktif (satu situs Direktori Aktif per Wilayah). Ketika Region baru ditambahkan, itu diberi nama yang sama dengan Region tersebut

—sebagai contoh, us-east-1. Anda juga dapat mengubah nama ini nanti menggunakan Situs dan Layanan Direktori Aktif.

AWS layanan

AWS layanan seperti Amazon RDS for SQL Server dan FSx Amazon terhubung ke instance lokal direktori global. Hal ini memungkinkan pengguna Anda untuk masuk sekali ke aplikasi Active Directory-aware yang berjalan serta AWS layanan seperti Amazon RDS for SQL Server di AWS Wilayah mana pun. AWS Untuk melakukannya, pengguna memerlukan kredensial dari AWS Microsoft AD yang Dikelola atau Direktori Aktif lokal jika Anda memiliki kepercayaan dengan iklan AWS Microsoft Terkelola.

Anda dapat menggunakan AWS layanan berikut dengan fitur replikasi Multi-wilayah.

- Amazon EC2
- Amazon FSx untuk Server File Windows
- Amazon Relational Database Service untuk SQL Server
- Amazon RDS for Oracle
- Amazon RDS for MySQL
- Amazon RDS for PostgreSQL
- Amazon RDS for MariaDB
- Amazon Aurora for MySQL
- Amazon Aurora for PostgreSQL

Failover

Jika semua pengontrol domain di satu Wilayah sedang down, Microsoft AD yang AWS Dikelola memulihkan pengontrol domain dan mereplikasi data direktori secara otomatis. Sementara itu pengendali domain di Region lain tetap aktif dan berjalan.

Manfaat replikasi Multi-wilayah

Dengan replikasi Multi-wilayah di AWS Microsoft AD yang Dikelola, aplikasi yang sadar Direktori Aktif menggunakan direktori secara lokal untuk kinerja tinggi dan fitur Multi-wilayah untuk ketahanan. Anda dapat menggunakan replikasi Multi-wilayah dengan aplikasi Active Directory-aware seperti SharePoint dan SQL Server Always On serta AWS layanan seperti Amazon RDS for SQL Server dan untuk Windows File Server. FSx Berikut ini adalah manfaat tambahan dari replikasi multi-Region.

- Ini memungkinkan Anda menerapkan satu instans Microsoft AD AWS Terkelola secara global, cepat, dan menghilangkan beban berat pengelolaan mandiri infrastruktur Direktori Aktif global.
- Ini membuatnya lebih mudah dan lebih hemat biaya bagi Anda untuk menyebarkan dan mengelola beban kerja Windows dan Linux di beberapa Wilayah. AWS Replikasi Multi-wilayah otomatis memungkinkan kinerja optimal dalam aplikasi sadar Direktori Aktif global Anda. Semua aplikasi yang digunakan di instans Windows atau Linux menggunakan AWS Microsoft AD yang Dikelola secara lokal di Wilayah, yang memungkinkan respons terhadap permintaan pengguna dari Wilayah terdekat.
- Ini memberikan ketahanan multi-Region. Diterapkan dalam infrastruktur AWS terkelola yang sangat tersedia, Microsoft AD yang AWS dikelola menangani pembaruan perangkat lunak otomatis, pemantauan, pemulihan, dan keamanan infrastruktur Direktori Aktif yang mendasarinya di semua Wilayah. Hal ini memungkinkan Anda untuk fokus membangun aplikasi Anda.

Topik

- [Fitur Global vs Regional](#)
- [Region utama vs tambahan](#)
- [Menambahkan Wilayah yang direplikasi untuk Microsoft AD yang AWS Dikelola](#)
- [Menghapus Wilayah yang direplikasi untuk AWS Microsoft AD yang Dikelola](#)

Fitur Global vs Regional

Saat Anda menambahkan AWS Wilayah ke direktori Anda menggunakan replikasi Multi-wilayah, Directory Service tingkatkan cakupan semua fitur sehingga menjadi sadar Wilayah. Fitur-fitur ini tercantum pada berbagai tab pada halaman detail yang muncul ketika Anda memilih ID dari direktori di konsol Directory Service . Ini berarti bahwa semua fitur diaktifkan, dikonfigurasi, atau dikelola berdasarkan Region yang Anda pilih di bagian Replikasi multi-Region dari konsol tersebut. Perubahan yang Anda buat pada fitur di setiap Region diterapkan secara global atau per Region.

Replikasi Multi-Region hanya didukung untuk Edisi Perusahaan AWS Microsoft AD yang Dikelola.

Fitur global

Setiap perubahan yang Anda buat untuk fitur global saat [Region primer](#) dipilih akan diterapkan di seluruh Region.

Anda dapat mengidentifikasi fitur yang digunakan secara global pada halaman Detail direktori karena mereka menampilkan Diterapkan untuk semua Region yang direplikasi di sampingnya. Atau, jika Anda memilih Region lain dalam daftar yang bukan Region primer, Anda dapat mengidentifikasi fitur yang digunakan secara global karena mereka menampilkan Diwarisi dari Region primer.

Fitur regional

Setiap perubahan yang Anda buat pada fitur di suatu fitur hanya [Regional tambahan](#) akan diterapkan ke Wilayah tersebut.

Anda dapat mengidentifikasi fitur yang digunakan secara global pada halaman Detail direktori karena mereka tidak menampilkan Diterapkan untuk semua Region yang direplikasi atau Diwarisi dari Region primer di sampingnya.

Region utama vs tambahan

Dengan replikasi Multi-wilayah, AWS Microsoft AD yang Dikelola menggunakan dua jenis Wilayah berikut untuk membedakan bagaimana fitur global atau Regional harus diterapkan di seluruh direktori Anda.

Region primer

Region awal tempat Anda pertama kali membuat direktori Anda disebut sebagai Region primer. Anda dapat melakukan operasi tingkat direktori global saja seperti membuat kepercayaan Active Directory dan memperbarui skema AD dari Region primer.

Region primer selalu dapat diidentifikasi sebagai Region pertama yang ditampilkan di bagian atas daftar di bagian Replikasi multi-Region, dan diakhiri dengan - Primer. Sebagai contoh, US East (N. Virginia) - Primer.

Setiap perubahan yang Anda buat untuk [Fitur global](#) saat Region primer dipilih akan diterapkan di seluruh Region.

Anda hanya dapat menambahkan Region saat Region primer dipilih. Untuk informasi selengkapnya, lihat [Menambahkan Wilayah yang direplikasi untuk Microsoft AD yang AWS Dikelola](#).

Regional tambahan

Setiap Daerah yang telah Anda tambahkan ke direktori Anda disebut sebagai Region Tambahan.

Meskipun beberapa fitur dapat dikelola secara global untuk semua Region, yang lainnya dikelola secara individual per Region. Untuk mengelola fitur untuk Region tambahan (Region non-primer), Anda harus terlebih dahulu memilih Region tambahan dari daftar di bagian Replikasi multi-Region pada halaman Detail direktori. Kemudian Anda dapat melanjutkan untuk mengelola fitur tersebut.

Setiap perubahan yang Anda buat untuk [Fitur regional](#) saat Region tambahan dipilih hanya akan diterapkan pada Region tersebut.

Menambahkan Wilayah yang direplikasi untuk Microsoft AD yang AWS Dikelola

Saat Anda menambahkan Wilayah menggunakan [Konfigurasi replikasi Multi-Wilayah untuk AWS Microsoft AD yang Dikelola](#) fitur tersebut, Microsoft AD yang AWS Dikelola akan membuat dua pengontrol domain di AWS Wilayah yang dipilih, Amazon Virtual Private Cloud (VPC), dan subnet. AWS Microsoft AD yang dikelola juga membuat grup keamanan terkait yang memungkinkan beban kerja Windows terhubung ke direktori Anda di Wilayah baru. Hal tersebut juga membuat sumber daya ini menggunakan akun AWS yang sama di mana direktori Anda sudah di-deploy. Anda melakukan ini dengan memilih Region, menentukan VPC, dan menyediakan konfigurasi untuk Region baru.

Replikasi Multi-Region hanya didukung untuk Edisi Perusahaan AWS Microsoft AD yang Dikelola.

Prasyarat

Sebelum melanjutkan langkah-langkah untuk menambahkan Region replikasi baru, kami rekomendasikan Anda terlebih dahulu meninjau tugas prasyarat berikut.

- Verifikasi bahwa Anda memiliki izin AWS Identity and Access Management (IAM) yang diperlukan, penyiapan Amazon VPC, dan pengaturan subnet di Wilayah baru tempat Anda ingin mereplikasi direktori.
- Jika Anda ingin menggunakan kredensial Direktori Aktif lokal yang ada untuk mengakses dan mengelola beban kerja yang sadar Direktori Aktif AWS, Anda harus membuat kepercayaan Direktori Aktif antara AWS Microsoft AD yang Dikelola dan infrastruktur AD lokal Anda. Untuk informasi selengkapnya tentang kepercayaan, lihat [Connect Microsoft AD AWS Terkelola ke infrastruktur Direktori Aktif yang ada](#).
- Jika Anda memiliki hubungan kepercayaan yang ada antara Active Directory lokal dan ingin menambahkan wilayah yang direplikasi, Anda perlu memverifikasi bahwa Anda memiliki pengaturan VPC dan subnet Amazon yang diperlukan di Wilayah baru tempat Anda ingin mereplikasi direktori.

Anda juga dapat membuat kepercayaan antara AD Microsoft AWS Terkelola dan infrastruktur AD lokal, sehingga Anda dapat menggunakan kredensial Direktori Aktif lokal yang ada untuk mengelola beban kerja yang sadar iklan. Untuk informasi selengkapnya, lihat [Connect Microsoft AD AWS Terkelola ke infrastruktur Direktori Aktif yang ada](#).

Tambahkan Region.

Gunakan prosedur berikut untuk menambahkan Wilayah yang direplikasi untuk direktori Microsoft AD AWS Terkelola Anda.

Untuk menambahkan Region yang direplikasi

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, di bawah Replikasi multi-Region, pilih Region Primer dari daftar, dan kemudian pilih Tambahkan Region.

Note

Anda hanya dapat menambahkan Region saat Region Primer dipilih. Untuk informasi selengkapnya, lihat [Region primer](#).

4. Pada halaman Tambahkan Region, di bawah Region, pilih Region yang ingin Anda tambahkan dari daftar.
5. Di bawah VPC, pilih VPC yang akan digunakan untuk Region ini.

Note

VPC ini tidak boleh memiliki Classless Inter-Domain Routing (CIDR) yang tumpang tindih dengan VPC yang digunakan oleh direktori ini di Region lain.

6. Di bawah Subnet, pilih subnet yang akan digunakan untuk Region ini.
7. Tinjau informasi di bawah Harga, lalu pilih Tambahkan.
8. Saat Microsoft AD yang AWS Dikelola menyelesaikan proses penyebaran pengontrol domain, Wilayah akan menampilkan status Aktif. Sekarang Anda dapat melakukan pembaruan ke Wilayah ini sesuai kebutuhan.

Langkah selanjutnya

Setelah menambahkan Region baru, Anda harus pertimbangkan untuk melakukan langkah-langkah berikut:

- Men-deploy pengendali domain tambahan (hingga 20) ke Region baru Anda sesuai kebutuhan. Jumlah pengendali domain ketika Anda menambahkan Region baru adalah 2 secara default, yang merupakan minimum yang diperlukan untuk toleransi kesalahan dan tujuan ketersediaan tinggi. Untuk informasi selengkapnya, lihat [Menambahkan atau menghapus pengontrol domain tambahan dengan Konsol Manajemen AWS](#).

Note

Saat Anda menambahkan yang direplikasi AWS Region ke Microsoft AD AWS Terkelola, dua pengontrol domain dibuat secara default, yang merupakan jumlah minimum pengontrol domain yang diperlukan untuk toleransi kesalahan dan ketersediaan tinggi.

- Bagikan direktori Anda dengan lebih banyak AWS akun per Wilayah. Konfigurasi berbagi direktori tidak direplikasi dari Region primer secara otomatis. Untuk informasi selengkapnya, lihat [Bagikan iklan Microsoft yang AWS Dikelola](#).

Note

Konfigurasi berbagi direktori tidak secara otomatis direplikasi di primer. AWS Region

- Aktifkan penerusan log untuk mengambil log keamanan direktori Anda menggunakan CloudWatch Log Amazon dari Wilayah baru. Saat Anda mengaktifkan penerusan log, Anda harus memberikan nama grup log di setiap Region di mana Anda mereplikasikan direktori Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS](#).

Note

Ketika Anda mengaktifkan penerusan log, Anda harus memberikan nama untuk grup log di setiap AWS Region tempat Anda mereplikasi direktori Anda.

- Aktifkan pemantauan Amazon Simple Notification Service (Amazon SNS) untuk Region baru untuk melacak status kondisi direktori Anda per Wilayah. Untuk informasi selengkapnya, lihat

[Mengaktifkan pemberitahuan status direktori Microsoft AD AWS Terkelola dengan Amazon Simple Notification Service.](#)

Menghapus Wilayah yang direplikasi untuk AWS Microsoft AD yang Dikelola

Gunakan prosedur berikut untuk menghapus Wilayah untuk direktori Microsoft AD yang AWS Dikelola. Sebelum Anda menghapus Region, pastikan tidak memiliki salah satu dari berikut ini:

- Aplikasi otorisasi yang melekat padanya.
- Direktori bersama yang terkait dengannya.

Untuk menghapus Region yang direplikasi

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Dari bilah navigasi, pilih pemilih Wilayah dan pilih wilayah tempat direktori Anda disimpan.
3. Pada halaman Direktori, pilih ID direktori Anda.
4. Pada halaman Detail direktori, di bawah Replikasi multi-Region pilih Hapus Region.
5. Di kotak dialog Hapus Region, tinjau informasi, dan kemudian masukkan dalam nama wilayah untuk mengkonfirmasi. Lalu pilih Hapus.

Note

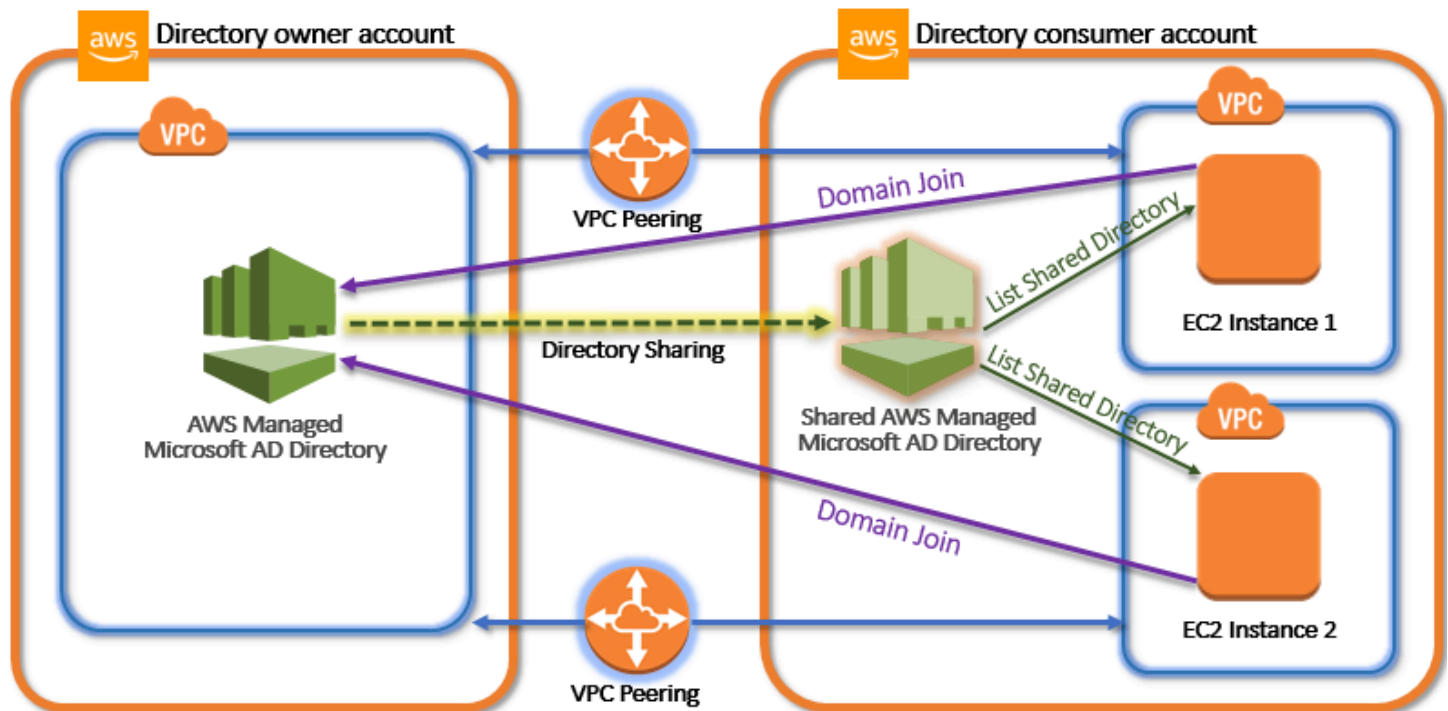
Anda tidak dapat membuat pembaruan ke Region saat sedang dihapus.

Bagikan iklan Microsoft yang AWS Dikelola

AWS Microsoft AD yang dikelola terintegrasi erat dengan AWS Organizations untuk memungkinkan berbagi direktori yang mulus di beberapa. Akun AWS Anda dapat berbagi satu direktori dengan tepercaya lainnya Akun AWS dalam organisasi yang sama atau berbagi direktori dengan direktori lain Akun AWS yang berada di luar organisasi Anda. Anda juga dapat membagikan direktori Anda ketika Anda saat Akun AWS ini bukan anggota organisasi.

Konsep berbagi direktori kunci

Anda akan mendapatkan lebih banyak dari fitur berbagi direktori jika Anda terbiasa dengan konsep-konsep kunci berikut.



Akun pemilik direktori

Pemilik direktori adalah Akun AWS pemegang yang memiliki direktori asal dalam hubungan direktori bersama. Administrator di akun ini memulai alur kerja berbagi direktori dengan menentukan mana Akun AWS untuk berbagi direktori mereka. Pemilik direktori dapat melihat siapa yang telah mereka bagikan direktori dengan menggunakan tab Skala & Bagikan untuk direktori yang diberikan dalam konsol Directory Service .

Akun konsumen direktori

Dalam hubungan direktori bersama, konsumen direktori mewakili Akun AWS yang di mana pemilik direktori berbagi direktori. Tergantung pada metode berbagi yang digunakan, administrator di akun ini mungkin perlu menerima undangan yang dikirim dari pemilik direktori sebelum mereka dapat mulai menggunakan direktori bersama.

Proses berbagi direktori membuat direktori bersama di akun konsumen direktori. Direktori bersama ini berisi metadata yang memungkinkan instans EC2 untuk menggabungkan domain secara mulus, yang

menempatkan direktori asal di akun pemilik direktori. Setiap direktori bersama dalam akun konsumen direktori memiliki pengenalan unik (ID direktori bersama).

Metode berbagi

AWS Microsoft AD yang dikelola menyediakan dua metode berbagi direktori berikut:

- **AWS Organizations** – Metode ini memudahkan untuk berbagi direktori dalam organisasi Anda karena Anda dapat menelusuri dan memvalidasi akun konsumen direktori. Untuk menggunakan opsi ini, organisasi Anda harus memiliki Semua fitur, dan direktori Anda harus berada dalam akun pengelolaan organisasi. Metode berbagi ini menyederhanakan penyiapan Anda karena tidak memerlukan akun konsumen direktori untuk menerima permintaan berbagi direktori Anda. Di konsol, metode ini disebut sebagai Bagikan direktori ini dengan Akun AWS di dalam organisasi Anda.
- **Handshake** - Metode ini memungkinkan berbagi direktori saat Anda tidak menggunakan AWS Organizations. Metode jabat tangan memerlukan akun konsumen direktori untuk menerima permintaan berbagi direktori. Di konsol tersebut, metode ini disebut sebagai Bagikan direktori ini dengan Akun AWS lain.

Konektivitas jaringan

Konektivitas jaringan adalah prasyarat untuk menggunakan hubungan berbagi direktori di seluruh. Akun AWS AWS [mendukung banyak solusi untuk menghubungkan Anda VPCs, beberapa di antaranya termasuk VPC peering, Transit Gateway, dan VPN](#). Untuk memulai, lihat [Tutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus](#).

Pertimbangan-pertimbangan

Berikut ini adalah beberapa pertimbangan saat menggunakan direktori berbagi dengan Microsoft AD yang AWS Dikelola:

Harga

- AWS membebankan biaya tambahan untuk berbagi direktori. Akun AWS Yang menggunakan iklan Microsoft AWS Terkelola bersama adalah akun yang dikenakan biaya berbagi. Untuk mempelajari lebih lanjut, lihat halaman [Harga](#) di Directory Service situs web.
- Berbagi direktori membuat Microsoft AD yang AWS Dikelola menjadi cara yang lebih hemat biaya untuk mengintegrasikan dengan Amazon EC2 di beberapa akun dan VPCs

Ketersediaan wilayah

- Berbagi direktori tersedia di semua [AWS wilayah tempat Microsoft AD yang AWS Dikelola](#) ditawarkan.
- Di AWS Tiongkok (Ningxia), fitur ini hanya tersedia saat [AWS Systems Manager](#) menggunakan (SSM) untuk bergabung dengan instans Amazon EC2 Anda dengan mulus.

Untuk informasi selengkapnya tentang berbagi direktori dan cara memperluas jangkauan direktori Microsoft AD AWS Terkelola di seluruh batas AWS akun, lihat topik berikut.

Topik

- [Tutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus](#)
- [Membatalkan berbagi direktori Anda](#)

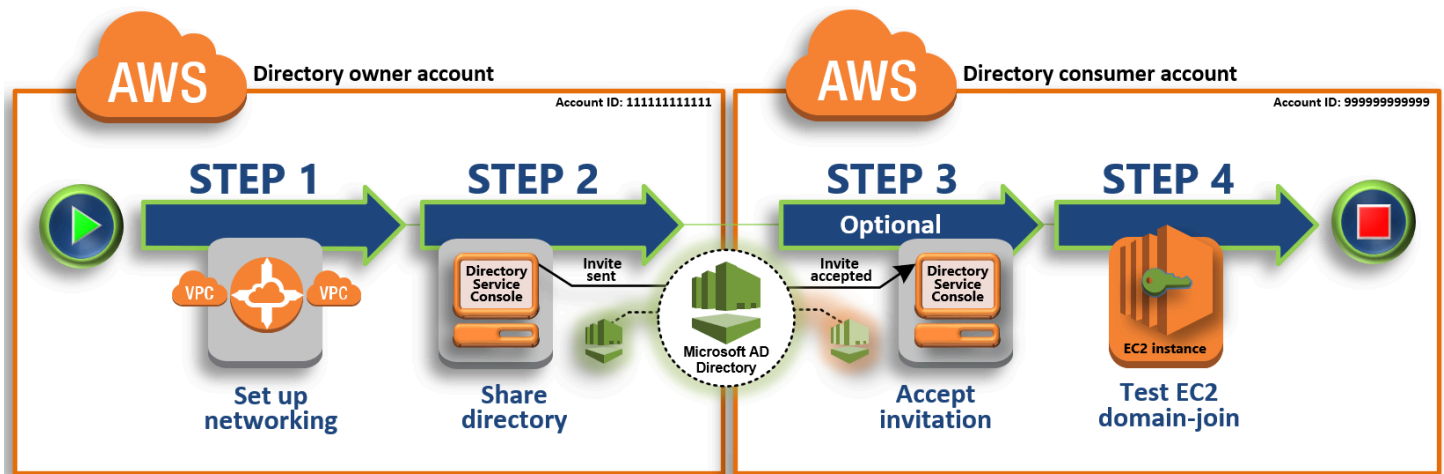
Tutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus

Tutorial ini menunjukkan cara berbagi direktori Microsoft AD AWS Terkelola Anda (akun pemilik direktori) dengan yang lain Akun AWS (akun konsumen direktori). Setelah prasyarat jaringan selesai, Anda akan berbagi direktori antara dua. Akun AWS Kemudian Anda akan belajar cara menggabungkan instans EC2 dengan mulus ke domain di akun konsumen direktori.

Kami merekomendasikan Anda untuk terlebih dahulu meninjau konsep kunci berbagi direktori dan menggunakan konten kasus sebelum Anda mulai bekerja pada tutorial ini. Untuk informasi selengkapnya, lihat [Konsep berbagi direktori kunci](#).

Proses untuk berbagi direktori berbeda tergantung pada apakah Anda berbagi direktori dengan yang lain Akun AWS di AWS organisasi yang sama atau dengan akun yang berada di luar AWS organisasi. Untuk informasi selengkapnya tentang cara berbagi, lihat [Metode berbagi](#).

Alur kerja ini memiliki empat langkah dasar.



Langkah 1: Atur lingkungan jaringan Anda

Di akun pemilik direktori, Anda mengatur semua prasyarat jaringan yang diperlukan untuk proses berbagi direktori.

Langkah 2: Bagikan direktori Anda

Saat masuk dengan kredensial administrator pemilik direktori, Anda membuka konsol Directory Service dan memulai alur kerja berbagi direktori, yang mengirimkan undangan ke akun konsumen direktori.

Langkah 3: Terima undangan direktori bersama - Opsional

Saat masuk dengan kredensi administrator konsumen direktori, Anda membuka Directory Service konsol dan menerima undangan berbagi direktori.

Langkah 4: Uji menggabungkan instans EC2 secara mulus untuk Windows Server ke domain

Akhirnya, sebagai administrator direktori konsumen, Anda mencoba untuk menggabungkan instans EC2 untuk domain Anda dan memverifikasi bahwa itu bekerja.

Sumber daya tambahan

- [Kasus penggunaan: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 dengan mulus ke domain di seluruh Akun AWS](#)
- [AWS Artikel Blog Keamanan: Cara Bergabung dengan Instans Amazon EC2 Dari Beberapa Akun dan VPCs ke Satu Direktori AWS Microsoft AD yang Dikelola](#)

Langkah 1: Atur lingkungan jaringan Anda

Anda perlu membuat koneksi peering VPC Amazon untuk membagikan direktori AWS Microsoft AD Terkelola (pemilik akun direktori) Anda dengan yang lain Akun AWS (akun konsumen direktori). Lihat prosedur berikut untuk langkah-langkah menyiapkan lingkungan jaringan Anda untuk iklan Microsoft AWS Terkelola bersama.

Prasyarat

Sebelum Anda mulai langkah-langkah dalam tutorial ini, Anda harus terlebih dahulu melakukan hal berikut ini:

- Buat dua yang baru Akun AWS untuk tujuan pengujian di Wilayah yang sama. Saat Anda membuat Akun AWS, secara otomatis membuat cloud pribadi virtual (VPC) khusus di setiap akun. Perhatikan ID VPC di setiap akun. Anda akan membutuhkan ini nanti.
- [Buat iklan Microsoft yang AWS Dikelola](#).
- Saat membuat koneksi peering VPC, pemilik akun direktori dan akun konsumen direktori akan memerlukan izin yang diperlukan untuk membuat dan menerima koneksi peering. Untuk informasi selengkapnya, lihat [Contoh: Membuat koneksi peering VPC dan Contoh: Menerima koneksi peering VPC](#).

Note

Meskipun ada banyak cara untuk menghubungkan pemilik Direktori dan akun konsumen Direktori VPCs, tutorial ini akan menggunakan metode peering VPC. Untuk opsi konektivitas VPC tambahan, lihat [Konektivitas jaringan](#).

Mengkonfigurasi koneksi peering VPC antara pemilik direktori dan akun konsumen direktori

Koneksi peering VPC yang akan Anda buat adalah antara konsumen direktori dan pemilik direktori. VPCs Ikuti langkah-langkah berikut untuk mengkonfigurasi koneksi peering VPC untuk konektivitas dengan akun konsumen direktori. Dengan koneksi ini Anda dapat merutekan lalu lintas antara keduanya VPCs menggunakan alamat IP pribadi.

Untuk membuat koneksi peering VPC antara pemilik direktori dan akun konsumen direktori

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/> Pastikan untuk masuk sebagai pengguna dengan kredensi administrator di akun pemilik direktori dengan izin yang diperlukan untuk membuat koneksi peering VPC. Untuk informasi selengkapnya, lihat [Prasyarat](#).
2. Di panel navigasi, pilih Koneksi Peering. Lalu pilih Buat Koneksi Peering.
3. Konfigurasi informasi berikut:
 - Label nama koneksi peering: Menyediakan nama yang jelas mengidentifikasi hubungan ini dengan VPC di akun konsumen direktori.
 - VPC (Peminta): Pilih ID VPC untuk akun pemilik direktori.
 - Di bawah Pilih VPC lain untuk di-peer, pastikan bahwa Akun saya dan Region ini dipilih.
 - VPC (Penerima): Pilih ID VPC untuk akun konsumen direktori.
4. Pilih Buat Koneksi Peering. Di kotak dialog konfirmasi, pilih OK.

Untuk menerima permintaan peering atas nama akun konsumen direktori

1. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/> Pastikan untuk masuk sebagai pengguna dengan izin yang diperlukan untuk menerima permintaan peering. Untuk informasi selengkapnya, lihat [Prasyarat](#).
2. Di panel navigasi, pilih Koneksi Peering.
3. Pilih koneksi peering VPC yang tertunda. (Statusnya adalah Penerimaan Tertunda.) Pilih Tindakan, Terima Permintaan.
4. Dalam dialog konfirmasi, pilih Ya, Terima. Di kotak dialog konfirmasi berikutnya, pilih Modifikasi tabel rute saya sekarang untuk pergi langsung ke halaman tabel rute.

Sekarang koneksi peering VPC Anda aktif, Anda harus menambahkan entri ke tabel rute VPC Anda di akun pemilik direktori. Melakukan hal ini memungkinkan lalu lintas untuk diarahkan ke VPC dalam akun direktori konsumen.

Untuk menambahkan entri ke tabel rute VPC di akun pemilik direktori

1. Saat di bagian Tabel rute dari konsol Amazon VPC, pilih tabel rute untuk VPC pemilik direktori.
2. Pilih tab Rute, pilih Edit rute, dan kemudian pilih Tambahkan rute.
3. Di kolom Tujuan, masukkan blok CIDR untuk VPC konsumen direktori.

4. Di kolom Target, masukkan ID koneksi peering VPC (seperti **pcx-123456789abcde000**) untuk koneksi peering yang Anda buat sebelumnya di akun pemilik direktori.
5. Pilih Simpan perubahan.

Untuk menambahkan entri ke tabel rute VPC di akun konsumen direktori

1. Saat di bagian Tabel rute dari konsol Amazon VPC, pilih tabel rute untuk VPC konsumen direktori.
2. Pilih tab Rute, pilih Edit rute, dan kemudian pilih Tambahkan rute.
3. Di kolom Tujuan, masukkan blok CIDR untuk VPC pemilik direktori.
4. Di kolom Target, ketik ID koneksi peering VPC (seperti **pcx-123456789abcde001**) untuk koneksi peering yang Anda buat sebelumnya di akun konsumen direktori.
5. Pilih Simpan perubahan.

Tambahkan protokol dan port Active Directory ke aturan keluar untuk grup keamanan di konsumen direktori. VPCs Untuk informasi selengkapnya, lihat [Grup keamanan untuk VPC Anda](#) dan [AWS Prasyarat Microsoft AD yang dikelola](#).

Langkah Selanjutnya

[Langkah 2: Bagikan direktori Anda](#)

Langkah 2: Bagikan direktori Anda

Gunakan prosedur berikut untuk memulai alur kerja berbagi direktori dari dalam akun pemilik direktori.

Note

Berbagi direktori adalah fitur Regional dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [replikasi Multi-Region](#), prosedur berikut harus diterapkan secara terpisah di setiap Wilayah. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Untuk berbagi direktori Anda dari akun pemilik direktori

1. Masuk ke kredensi administrator Konsol Manajemen AWS dengan di akun pemilik direktori dan buka [AWS Directory Service konsol](https://console.aws.amazon.com/directoryservicev2/) di. <https://console.aws.amazon.com/directoryservicev2/>

2. Di panel navigasi, pilih Direktori.
3. Pilih ID direktori direktori Microsoft AD AWS Terkelola yang ingin Anda bagikan.
4. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin membagikan direktori Anda, lalu pilih tab Menskalakan & bagikan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Menskalakan & bagikan.
5. Di bagian Direktori bersama, pilih Tindakan, lalu pilih Buat direktori bersama baru.
6. Pada halaman Pilih mana Akun AWS yang akan dibagikan, pilih salah satu metode berbagi berikut tergantung pada kebutuhan bisnis Anda:
 - a. Bagikan direktori ini dengan Akun AWS di dalam organisasi Anda — Dengan opsi ini Akun AWS Anda dapat memilih direktori yang ingin Anda bagikan dari daftar yang menunjukkan semua bagian Akun AWS dalam AWS organisasi Anda. Anda harus mengaktifkan akses tepercaya dengan Directory Service sebelum Anda berbagi direktori. Untuk informasi selengkapnya, lihat [Cara mengaktifkan atau menonaktifkan akses tepercaya](#).
 - i. Akun AWS Di bawah di organisasi Anda, pilih direktori Akun AWS yang ingin Anda bagikan dan klik Tambah.
 - ii. Tinjau detail harga, lalu pilih Bagikan.
 - iii. Lanjutkan ke [Langkah 4](#) dalam panduan ini. Karena semua Akun AWS berada di organisasi yang sama, Anda tidak perlu mengikuti Langkah 3.
 - b. Bagikan direktori ini dengan yang lain Akun AWS - Dengan opsi ini, Anda dapat berbagi direktori dengan akun di dalam atau di luar AWS organisasi Anda. Anda juga dapat menggunakan opsi ini ketika direktori Anda bukan anggota AWS organisasi dan Anda ingin berbagi dengan yang lain Akun AWS.

 Note

Untuk menggunakan opsi ini, organisasi Anda harus memiliki Semua fitur, dan direktori Anda harus berada dalam akun pengelolaan organisasi.

- i. Di Akun AWS ID, masukkan semua direktori Akun AWS IDs yang ingin Anda bagikan, lalu klik Tambah.
- ii. Di Kirim catatan, ketik pesan ke administrator di Akun AWS lain.
- iii. Tinjau detail harga, lalu pilih Bagikan.
- iv. Lanjutkan ke Langkah 3.

Langkah Selanjutnya

[Langkah 3: Terima undangan direktori bersama - Opsional](#)

Langkah 3: Terima undangan direktori bersama - Opsional

Jika Anda memilih Bagikan direktori ini dengan Akun AWS (metode jabat tangan) pilihan dalam prosedur sebelumnya, Anda harus menggunakan prosedur ini untuk menyelesaikan alur kerja direktori bersama. Jika Anda memilih opsi Bagikan direktori ini dengan Akun AWS di dalam organisasi Anda, lewati langkah ini dan lanjutkan ke Langkah 4.

Untuk menerima undangan direktori bersama

1. Masuk ke kredensi administrator Konsol Manajemen AWS dengan di akun konsumen direktori dan buka [AWS Directory Service konsol](https://console.aws.amazon.com/directoryservicev2/) di. <https://console.aws.amazon.com/directoryservicev2/>
2. Di panel navigasi, pilih Direktori yang dibagikan dengan saya.
3. Di kolom ID Direktori bersama, pilih ID direktori yang ada dalam keadaan Penerimaan tertunda.
4. Pada halaman Detail direktori bersama, pilih Tinjauan.
5. Di dialog Undangan direktori bersama tertunda, tinjau catatan, detail pemilik direktori, dan informasi tentang harga. Jika Anda setuju, pilih Terima untuk mulai menggunakan direktori.

Langkah Selanjutnya

[Langkah 4: Uji menggabungkan instans EC2 secara mulus untuk Windows Server ke domain](#)

Langkah 4: Uji menggabungkan instans EC2 secara mulus untuk Windows Server ke domain

Anda dapat menggunakan salah satu dari dua metode berikut untuk menguji dengan mulus menggabungkan instans EC2 ke domain.

Metode 1: Menguji penggabungan domain menggunakan konsol Amazon EC2

Gunakan langkah-langkah ini di direktori akun konsumen.

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. <https://console.aws.amazon.com/ec2/>
2. Di bilah navigasi, pilih yang AWS Region sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Nama dan Tag, masukkan nama yang ingin Anda gunakan untuk instans Windows EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih Windows di panel Mulai Cepat. Anda dapat mengubah Windows Amazon Machine Image (AMI) dari daftar dropdown Amazon Machine Image (AMI).
7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada.
 - a. Untuk membuat key pair baru, pilih Create new key pair.
 - b. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format.
 - c. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk.
 - d. Pilih create key pair.
 - e. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

Important

Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.

10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat [Connect to the internet menggunakan gateway internet](#) di Panduan Pengguna Amazon VPC.

11. Di bawah Auto-assign IP publik, pilih Aktifkan.

Untuk informasi selengkapnya tentang pengalamatan IP publik dan pribadi, lihat pengalamatan [IP instans Amazon EC2](#) di Panduan Pengguna Amazon EC2.

12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

Note

Setelah memilih direktori Gabung Domain, Anda mungkin melihat:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu hal berikut:

- Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
- Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, Anda dapat memilih profil instans IAM yang ada atau membuat yang baru. Pilih profil instans IAM yang memiliki kebijakan AWS terkelola Amazon SSMManged InstanceCore dan Amazon yang SSMDirectory ServiceAccess dilampirkan padanya dari daftar

dropdown profil instans IAM. Untuk membuat yang baru, pilih Buat tautan profil IAM baru, lalu lakukan hal berikut:

1. Pilih Buat peran.
2. Di bawah Pilih entitas tepercaya, pilih AWS layanan.
3. Di bawah Kasus penggunaan, pilih EC2.
4. Di bawah Tambahkan izin, dalam daftar kebijakan, pilih SSMDirectory ServiceAccess kebijakan Amazon SSMManged InstanceCore dan Amazon. Untuk memfilter daftar, **SSM** ketik kotak pencarian. Pilih Berikutnya.

 Note

Amazon SSMDirectory ServiceAccess menyediakan izin untuk menggabungkan instance ke Active Directory yang dikelola oleh Directory ServiceAmazon SSMManged InstanceCore memberikan izin minimum yang diperlukan untuk menggunakan AWS Systems Manager layanan ini. Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat [Buat profil instans IAM untuk Systems Manager](#) di Panduan Pengguna AWS Systems Manager .

5. Pada halaman Nama, tinjau, dan buat, masukkan nama Peran. Anda akan memerlukan nama peran ini untuk melampirkan ke instans EC2.
 6. (Opsional) Anda dapat memberikan deskripsi profil instans IAM di bidang Deskripsi.
 7. Pilih Buat peran.
 8. Kembali ke Luncurkan halaman instans dan pilih ikon penyegaran di sebelah profil instans IAM. Profil instans IAM baru Anda harus terlihat di daftar dropdown profil instans IAM. Pilih profil baru dan biarkan pengaturan lainnya dengan nilai defaultnya.
16. Pilih Luncurkan instans.

Metode 2: Uji domain bergabung menggunakan AWS Systems Manager

Gunakan langkah-langkah ini di direktori akun konsumen. Untuk menyelesaikan prosedur ini, Anda akan memerlukan beberapa informasi tentang akun pemilik direktori seperti ID Direktori, nama direktori, dan alamat IP DNS.

Prasyarat

- Pengaturan AWS Systems Manager.
 - Untuk informasi selengkapnya tentang Systems Manager, lihat [Penyiapan umum untuk AWS Systems Manager](#).
- Instans yang ingin Anda gabungkan dengan domain Direktori Aktif Microsoft AWS Terkelola harus memiliki peran IAM terlampir yang berisi kebijakan SSMDirectory ServiceAccess terkelola SSMMManagedInstanceCoreAmazon dan Amazon.
- Untuk informasi selengkapnya tentang kebijakan terkelola ini dan kebijakan lain yang dapat Anda lampirkan ke profil instans IAM untuk Systems Manager, lihat [Membuat profil instans IAM untuk Systems Manager](#) di AWS Systems Manager Panduan Pengguna. Untuk informasi selengkapnya tentang kebijakan terkelola, lihat [Kebijakan yang dikelola AWS](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang penggunaan Systems Manager untuk menggabungkan instans EC2 ke domain Direktori Aktif AWS Microsoft Terkelola, lihat [Bagaimana cara menggunakan AWS Systems Manager instans Windows EC2 yang sedang berjalan ke domain AWS Directory Service saya?](#).

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Di panel navigasi, di bawah Manajemen Node, pilih Jalankan Perintah.
3. Pilih Run command.
4. Pada halaman Run command, cari AWS-JoinDirectoryServiceDomain. Ketika ditampilkan dalam hasil pencarian, pilih pilihan AWS-JoinDirectoryServiceDomain.
5. Scroll ke bawah ke bagian Parameter perintah. Anda harus memberikan parameter berikut:

 Note

Anda dapat menemukan ID Direktori, nama direktori, dan alamat IP DNS dengan kembali ke Directory Service konsol, memilih Direktori yang dibagikan dengan saya, dan memilih direktori Anda. ID Direktori Anda dapat ditemukan di bagian Detail direktori bersama. Anda dapat menemukan nilai untuk nama Direktori dan alamat IP DNS di bawah bagian detail direktori Pemilik.

- Untuk ID Direktori, masukkan nama Direktori Aktif Microsoft yang AWS Dikelola.

- Untuk Nama Direktori, masukkan nama Direktori Aktif Microsoft AWS Terkelola (untuk akun pemilik direktori).
 - Untuk Alamat IP DNS, masukkan alamat IP server DNS di Direktori Aktif AWS Microsoft Terkelola (untuk akun pemilik direktori).
6. Untuk Target, pilih instance secara manual, lalu pilih instance yang ingin Anda gabungkan dengan domain.
 7. Biarkan sisa formulir diatur ke nilai default mereka, scroll ke bawah halaman, dan kemudian pilih Jalankan.
 8. Status perintah akan berubah dari Pending menjadi Success setelah instance berhasil bergabung dengan domain. Anda dapat melihat output perintah dengan memilih ID Instance dari instance yang bergabung dengan domain dan View output.

Setelah menyelesaikan salah satu dari langkah-langkah ini, Anda sekarang dapat menggabungkan instans EC2 Anda ke domain. Setelah melakukannya, Anda dapat masuk ke instans menggunakan klien Remote Desktop Protocol (RDP) dengan kredensial dari akun pengguna AWS Microsoft AD yang Dikelola.

Membatalkan berbagi direktori Anda

Gunakan prosedur berikut untuk membatalkan berbagi direktori Microsoft AD yang AWS Dikelola.

Untuk membatalkan berbagi direktori Anda

1. Di panel navigasi [Konsol AWS Directory Service](#), di bawah Direktori Aktif, pilih Direktori.
2. Pilih ID direktori direktori Microsoft AD AWS Terkelola yang ingin Anda hapus bagikannya.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Daerah yang ditampilkan di bawah Replikasi multi-Region, pilih Region tempat Anda ingin membatalkan berbagi direktori Anda, lalu pilih tab Menskalakan & bagikan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Menskalakan & bagikan.
4. Di Direktori bersama, pilih direktori bersama yang ingin Anda batalkan berbagi, pilih Tindakan, lalu pilih Batalkan Berbagi.
5. Di kotak dialog Batalkan berbagi direktori, pilih Batalkan Berbagi.

Sumber daya tambahan

- [Kasus penggunaan: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 dengan mulus ke domain di seluruh akun AWS](#)
- [AWS artikel blog keamanan: Cara bergabung dengan instans Amazon EC2 dari beberapa akun dan VPCs ke satu direktori AD AWS Microsoft Terkelola](#)
- [Bergabung dengan instans Amazon RDS DB Anda di seluruh akun ke satu domain bersama](#)

Memigrasi pengguna Active Directory ke Microsoft AD yang AWS Dikelola

Anda dapat menggunakan Active Directory Migration Toolkit (ADMT) bersama dengan Layanan Ekspor Kata Sandi (PES) untuk memigrasikan pengguna dari Direktori Aktif yang dikelola sendiri ke direktori AWS Microsoft AD yang dikelola sendiri. Ini memungkinkan Anda untuk memigrasi objek Active Directory dan kata sandi terenkripsi untuk pengguna Anda dengan lebih mudah.

Untuk petunjuk selengkapnya, lihat [Cara memigrasikan domain lokal Anda ke AWS Microsoft AD yang Dikelola menggunakan ADMT di Blog Keamanan.AWS](#)

Connect Microsoft AD AWS Terkelola ke infrastruktur Direktori Aktif yang ada

Bagian ini menjelaskan cara mengonfigurasi hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan infrastruktur Direktori Aktif yang ada.

Tugas untuk menghubungkan AD Microsoft AWS Terkelola ke Direktori Aktif yang ada:

- [Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri](#)
- [Menambahkan rute IP saat menggunakan alamat IP publik dengan Microsoft AD yang AWS Dikelola](#)
- [Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri](#)
- [Tutorial: Buat hubungan kepercayaan antara dua domain Microsoft AD yang AWS Dikelola](#)

Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri

Anda dapat mengonfigurasi hubungan kepercayaan eksternal dan hutan satu dan dua arah antara AWS Directory Service for Microsoft Active Directory dan direktori yang dikelola sendiri (lokal), serta di antara beberapa direktori AWS Microsoft AD Terkelola di cloud. AWS AWS Microsoft AD yang dikelola mendukung ketiga arah hubungan kepercayaan: Masuk, Keluar, dan Dua arah (Bi-directional).

Untuk informasi selengkapnya tentang hubungan kepercayaan, lihat [Semua yang ingin Anda ketahui tentang kepercayaan dengan Microsoft AD yang AWS Dikelola](#).

Note

Saat mengatur hubungan kepercayaan, Anda harus memastikan bahwa direktori yang dikelola sendiri dan tetap kompatibel dengan Directory Service s. Untuk informasi selengkapnya tentang tanggung jawab Anda, silakan lihat [model tanggung jawab bersama](#) kami.

AWS Microsoft AD yang dikelola mendukung perwalian eksternal dan hutan. Untuk menelusuri contoh skenario yang menunjukkan cara membuat kepercayaan forest, lihat [Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri](#).

Kepercayaan dua arah diperlukan untuk Aplikasi AWS Perusahaan seperti Amazon Chime, Amazon Connect, Quick, AWS IAM Identity Center, WorkDocs, Amazon WorkMail, dan WorkSpaces Amazon. Konsol Manajemen AWS AWS Microsoft AD yang dikelola harus dapat menanyakan pengguna dan grup di Direktori Aktif yang dikelola sendiri.

Anda dapat mengaktifkan otentikasi selektif sehingga hanya akun layanan khusus AWS aplikasi yang dapat menanyakan Direktori Aktif yang dikelola sendiri. Untuk informasi selengkapnya, lihat [Meningkatkan keamanan integrasi AWS aplikasi Anda dengan Microsoft AD yang AWS Dikelola](#).

Amazon EC2, Amazon RDS, dan Amazon FSx akan bekerja dengan kepercayaan satu arah atau dua arah.

Prasyarat

Membuat kepercayaan hanya memerlukan beberapa langkah, tetapi Anda harus terlebih dahulu menyelesaikan beberapa langkah prasyarat sebelum mengatur kepercayaan.

 Note

AWS Microsoft AD yang dikelola tidak mendukung kepercayaan dengan [Domain Label Tunggal](#).

Menghubungkan ke VPC

Jika Anda membuat hubungan kepercayaan dengan direktori yang dikelola sendiri, Anda harus terlebih dahulu menghubungkan jaringan yang dikelola sendiri ke VPC Amazon yang berisi iklan Microsoft Terkelola AWS. Firewall untuk jaringan Microsoft AD yang AWS dikelola sendiri dan dikelola harus membuka port jaringan yang terdaftar di [WindowsServer 2008 dan versi yang lebih baru](#) dalam Microsoft dokumentasi.

Untuk menggunakan nama NetBIOS Anda alih-alih nama domain lengkap Anda untuk otentikasi dengan aplikasi Anda AWS seperti Amazon WorkDocs atau Amazon Quick, Anda harus mengizinkan port 9389. Untuk informasi selengkapnya tentang port dan protokol Direktori Aktif, lihat [Ringkasan layanan dan persyaratan port jaringan untuk dokumentasi Windows](#). Microsoft

Ini adalah port-port minimum yang diperlukan untuk dapat terhubung ke direktori Anda. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

Mengkonfigurasi VPC Anda

VPC yang berisi iklan AWS Microsoft Terkelola Anda harus memiliki aturan keluar dan masuk yang sesuai.

Untuk mengkonfigurasi aturan keluar VPC Anda

1. Di [AWS Directory Service konsol](#), pada halaman Detail Direktori, catat ID direktori Microsoft AD AWS Terkelola Anda.
2. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
3. Pilih Grup Keamanan.
4. Cari ID direktori Microsoft AD AWS Terkelola Anda. Dalam hasil pencarian, pilih item dengan deskripsi "AWS membuat grup keamanan untuk pengontrol direktori ID direktori".

 Note

Grup keamanan yang dipilih adalah grup keamanan yang dibuat secara otomatis ketika Anda awalnya membuat direktori Anda.

5. Pergi ke tab Aturan Keluar dari grup keamanan tersebut. Pilih Edit, kemudian Tambahkan aturan lain. Untuk aturan baru, masukkan nilai berikut:

- Jenis: Semua Lalu lintas
- Protokol: Semua
- Tujuan menentukan lalu lintas yang dapat meninggalkan pengontrol domain Anda dan ke mana ia dapat pergi di jaringan yang dikelola sendiri. Tentukan alamat IP tunggal atau cakupan alamat IP dalam notasi CIDR (misalnya, 203.0.113.5/32). Anda juga dapat menentukan nama atau ID grup keamanan lain di Region yang sama. Untuk informasi selengkapnya, lihat [Memahami konfigurasi dan penggunaan grup AWS keamanan direktori Anda](#).

6. Pilih Simpan.

Aktifkan pra-autentikasi Kerberos

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Untuk informasi selengkapnya tentang setelan ini, tinjau [Preauthentication](#) di Microsoft. TechNet

Konfigurasikan forwarder bersyarat DNS pada domain yang dikelola sendiri

Anda harus menyiapkan forwarder bersyarat DNS pada domain yang dikelola sendiri. Lihat [Menetapkan Forwarder Bersyarat untuk Nama Domain di Microsoft TechNet untuk detail tentang penerusan bersyarat](#).

Untuk melakukan langkah-langkah berikut, Anda harus memiliki akses ke alat Windows Server berikut untuk domain yang dikelola sendiri:

- Alat AD DS dan AD LDS
- DNS

Untuk mengonfigurasi forwarder bersyarat pada domain yang dikelola sendiri

1. Pertama, Anda harus mendapatkan beberapa informasi tentang AWS Managed Microsoft AD Anda. Masuk ke Konsol Manajemen AWS dan buka [AWS Directory Service konsol](#).
2. Di panel navigasi, pilih Direktori.
3. Pilih ID direktori iklan Microsoft AWS Terkelola Anda.
4. Perhatikan nama domain yang memenuhi syarat (FQDN) dan alamat DNS dari direktori Anda.
5. Sekarang, kembali ke pengontrol domain yang dikelola sendiri. Buka Pengelola Server
6. Pada menu Alat, pilih DNS.
7. Pada pohon konsol, perluas server DNS dari domain di mana Anda mengatur kepercayaan.
8. Pada pohon konsol, pilih Penerusan Bersyarat.
9. Pada menu Tindakan, pilih Penerusan bersyarat baru.
10. Di domain DNS, ketik nama domain yang memenuhi syarat penuh (FQDN) dari AWS Microsoft AD Terkelola Anda, yang Anda sebutkan sebelumnya.
11. Pilih alamat IP server utama dan ketik alamat DNS direktori Microsoft AD AWS Terkelola Anda, yang Anda catat sebelumnya.

Setelah memasukkan alamat DNS, Anda mungkin mendapatkan error “timeout” atau “tidak dapat menyelesaikan”. Anda biasanya dapat mengabaikan error ini.

12. Pilih Menyimpan penerusan bersyarat ini di Direktori Aktif dan mereplikasi sebagai berikut:
Semua server DNS di domain ini. Pilih OK.

Kata sandi hubungan Kepercayaan

Jika Anda membuat hubungan kepercayaan dengan domain yang ada, atur hubungan kepercayaan pada domain tersebut menggunakan alat Administrasi Server Windows. Saat Anda melakukannya, perhatikan kata sandi kepercayaan yang Anda gunakan. Anda harus menggunakan kata sandi yang sama ini saat mengatur hubungan kepercayaan pada iklan Microsoft yang AWS Dikelola. Untuk informasi selengkapnya, lihat [Mengelola Trust](#) di Microsoft TechNet.

Anda sekarang siap untuk menciptakan hubungan kepercayaan pada iklan Microsoft yang AWS Dikelola.

NetBIOS dan Nama Domain

NetBIOS dan nama domain harus unik dan tidak bisa sama untuk membangun hubungan kepercayaan.

Membuat, memverifikasi, atau menghapus hubungan kepercayaan

Note

Hubungan kepercayaan adalah fitur global dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [Konfigurasi replikasi Multi-Wilayah untuk AWS Microsoft AD yang Dikelola](#), prosedur berikut harus dilakukan di [Region primer](#). Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Untuk membuat hubungan kepercayaan dengan Microsoft AD yang AWS Dikelola

1. Buka [konsol AWS Directory Service](#).
2. Pada halaman Direktori, pilih ID AD Microsoft yang AWS Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. Pada halaman Tambahkan hubungan kepercayaan, berikan informasi yang diperlukan, termasuk jenis kepercayaan, fully qualified domain name (FQDN) dari domain tepercaya Anda, kata sandi kepercayaan dan arah kepercayaan.
6. (Opsional) Jika Anda hanya ingin mengizinkan pengguna yang berwenang untuk mengakses sumber daya di direktori Microsoft AD AWS Terkelola, Anda dapat memilih kotak centang Autentikasi selektif secara opsional. Untuk informasi umum tentang otentikasi selektif, lihat [Pertimbangan Keamanan untuk Trusts](#) di Microsoft. TechNet

7. Untuk Conditional forwarder, ketikkan alamat IP server DNS yang dikelola sendiri. Jika sebelumnya Anda telah membuat forwarder bersyarat, Anda dapat mengetik FQDN domain yang dikelola sendiri alih-alih alamat IP DNS.
8. (Opsional) Pilih Tambahkan alamat IP lain dan ketik alamat IP server DNS tambahan yang dikelola sendiri. Anda dapat mengulangi langkah ini untuk setiap alamat server DNS yang berlaku untuk total empat alamat.
9. Pilih Tambahkan.
10. Jika server DNS atau jaringan untuk domain yang dikelola sendiri menggunakan ruang alamat IP publik (non-RFC 1918), buka bagian perutean IP, pilih Tindakan, lalu pilih Tambahkan rute. Ketik blok alamat IP server DNS Anda atau jaringan yang dikelola sendiri menggunakan format CIDR, misalnya 203.0.113.0/24. Langkah ini tidak diperlukan jika server DNS Anda dan jaringan yang dikelola sendiri menggunakan ruang alamat IP RFC 1918.

 Note

Saat menggunakan ruang alamat IP publik, pastikan bahwa Anda tidak menggunakan salah satu dari [Rentang alamat IP AWS](#) karena ini tidak dapat digunakan.

11. (Opsional) Kami merekomendasikan bahwa saat Anda berada di halaman Tambahkan rute Anda juga pilih Menambahkan rute ke grup keamanan untuk VPC direktori ini. Ini akan mengkonfigurasi grup keamanan seperti yang dijelaskan di atas dalam “Konfigurasi VPC Anda.” Aturan keamanan ini memengaruhi antarmuka jaringan internal yang tidak terbuka secara publik. Jika opsi ini tidak tersedia, Anda akan melihat pesan yang menunjukkan bahwa Anda telah menyesuaikan grup keamanan Anda.

Anda harus mengatur hubungan kepercayaan pada kedua domain. Hubungan harus saling melengkapi. Misalnya, jika Anda membuat kepercayaan keluar pada satu domain, Anda harus membuat kepercayaan masuk di sisi lain.

Jika Anda membuat hubungan kepercayaan dengan domain yang ada, atur hubungan kepercayaan pada domain tersebut menggunakan alat Administrasi Server Windows.

Anda dapat membuat beberapa kepercayaan antara Microsoft AD yang AWS Dikelola dan berbagai domain Direktori Aktif. Namun, hanya satu hubungan kepercayaan per pasangan dapat eksis pada suatu waktu. Misalnya, jika Anda memiliki kepercayaan satu arah yang ada pada “Arah masuk” dan Anda kemudian ingin mengatur hubungan kepercayaan lain di “Arah keluar,” Anda harus menghapus hubungan kepercayaan yang ada, dan menciptakan kepercayaan “Dua arah” yang baru.

Untuk memverifikasi hubungan kepercayaan keluar

1. Buka [konsol AWS Directory Service](#).
2. Pada halaman Direktori, pilih ID AD Microsoft yang AWS Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih kepercayaan yang ingin Anda verifikasi, pilih Tindakan, dan kemudian pilih Verifikasi hubungan kepercayaan.

Proses ini hanya memverifikasi arah keluar dari kepercayaan dua arah. AWS tidak mendukung verifikasi trust yang masuk. Untuk informasi selengkapnya tentang cara memverifikasi kepercayaan ke atau dari Direktori Aktif yang dikelola sendiri, lihat [Verifikasi Kepercayaan](#) di Microsoft TechNet.

Untuk menghapus hubungan kepercayaan yang ada

1. Buka [konsol AWS Directory Service](#).
2. Pada halaman Direktori, pilih ID AD Microsoft yang AWS Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih kepercayaan yang ingin Anda hapus, pilih Tindakan, dan kemudian pilih Hapus hubungan kepercayaan.
5. Pilih Hapus.

Menambahkan rute IP saat menggunakan alamat IP publik dengan Microsoft AD yang AWS Dikelola

Anda dapat menggunakan AWS Directory Service untuk Microsoft Active Directory untuk memanfaatkan banyak fitur Active Directory yang kuat, termasuk membangun kepercayaan dengan direktori lain. Namun, jika server DNS untuk jaringan direktori lain menggunakan alamat IP publik (non-RFC 1918), Anda harus menentukan alamat IP tersebut sebagai bagian dari konfigurasi kepercayaan. Petunjuk untuk melakukan ini dapat ditemukan di [Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri](#).

Demikian pula, Anda juga harus memasukkan informasi alamat IP saat merutekan lalu lintas dari iklan Microsoft yang AWS Dikelola AWS ke VPC rekan, jika AWS VPC menggunakan rentang IP publik.

Saat Anda menambahkan alamat IP seperti yang dijelaskan di [Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri](#), Anda memiliki pilihan untuk memilih Menambahkan rute ke grup keamanan untuk VPC direktori ini. Opsi ini harus dipilih kecuali Anda sebelumnya telah menyesuaikan [Grup keamanan](#) Anda untuk memungkinkan lalu lintas yang diperlukan seperti yang ditunjukkan di bawah. Lihat informasi yang lebih lengkap di [Memahami konfigurasi dan penggunaan grup AWS keamanan direktori Anda](#).

Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri

Tutorial ini memandu Anda melalui semua langkah yang diperlukan untuk mengatur hubungan kepercayaan antara AWS Directory Service untuk Microsoft Active Directory dan Microsoft Active Directory yang dikelola sendiri (lokal). Meskipun membuat kepercayaan hanya memerlukan beberapa langkah, Anda harus terlebih dahulu menyelesaikan langkah-langkah prasyarat berikut.

Topik

- [Prasyarat](#)
- [Langkah 1: Siapkan Domain AD yang dikelola sendiri](#)
- [Langkah 2: Siapkan Microsoft AD yang AWS Dikelola](#)
- [Langkah 3: Buat hubungan kepercayaan](#)

Lihat Juga

Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri

Prasyarat

Tutorial ini mengasumsikan bahwa Anda telah memiliki hal berikut:

Note

AWS Microsoft AD yang dikelola tidak mendukung kepercayaan dengan [domain label tunggal](#).

- Direktori Microsoft AD AWS Terkelola yang dibuat pada AWS. Jika Anda memerlukan bantuan untuk melakukannya, lihat [Memulai dengan Microsoft AD yang AWS Dikelola](#).
- Instans EC2 yang berjalan Windows ditambahkan ke Microsoft AD yang AWS Dikelola. Jika Anda memerlukan bantuan untuk melakukannya, lihat [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#).

Important

Akun admin untuk Microsoft AD yang AWS Dikelola harus memiliki akses administratif ke instans ini.

- Alat Windows Server berikut diinstal pada contoh itu:
 - Alat AD DS dan AD LDS
 - DNS

Jika Anda memerlukan bantuan untuk melakukannya, lihat [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#).

- Microsoft Active Directory yang dikelola sendiri (lokal)

Anda harus memiliki akses administratif ke direktori ini. Alat Windows Server yang sama seperti yang tercantum di atas juga harus tersedia untuk direktori ini.

- Sambungan aktif antara jaringan yang dikelola sendiri dan VPC yang berisi iklan Microsoft AWS Terkelola Anda. Jika Anda memerlukan bantuan untuk melakukannya, lihat [Pilihan Konektivitas Amazon Virtual Private Cloud](#).

- Kebijakan keamanan lokal yang ditetapkan dengan benar. Periksa Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously dan pastikan bahwa itu berisi setidaknya tiga pipa bernama berikut:
 - netlogon
 - samr
 - lsarpc
- NetBIOS dan nama domain harus unik dan tidak bisa sama untuk membangun hubungan kepercayaan

Untuk informasi lebih lanjut tentang prasyarat untuk menciptakan hubungan kepercayaan, lihat.

[Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri](#)

Konfigurasi tutorial

Untuk tutorial ini, kami telah membuat iklan Microsoft yang AWS Dikelola dan domain yang dikelola sendiri. Jaringan yang dikelola sendiri terhubung ke VPC Microsoft AD yang AWS Dikelola. Berikut ini adalah properti dari dua direktori tersebut:

AWS Microsoft AD terkelola berjalan AWS

- Nama domain (FQDN): Ad.example.com MyManaged
- Nama NetBIOS: AD MyManaged
- Alamat DNS: 10.0.10.246, 10.0.20.121
- VPC CIDR: 10.0.0.0/16

Microsoft AD yang AWS Dikelola berada di ID VPC: vpc-12345678.

Domain Microsoft AD yang AWS dikelola sendiri atau Dikelola

- Nama domain (FQDN): corp.example.com
- Nama NetBIOS: CORP
- Alamat DNS: 172.16.10.153
- CIDR yang dikelola sendiri: 172.16.0.0/16

Langkah Selanjutnya

Langkah 1: Siapkan Domain AD yang dikelola sendiri

Langkah 1: Siapkan Domain AD yang dikelola sendiri

Pertama, Anda perlu menyelesaikan beberapa langkah prasyarat pada domain yang dikelola sendiri (lokal) Anda.

Konfigurasi firewall yang dikelola sendiri

Anda harus mengonfigurasi firewall yang dikelola sendiri sehingga port berikut terbuka CIDRs untuk semua subnet yang digunakan oleh VPC yang berisi iklan Microsoft Terkelola AWS Anda. Dalam tutorial ini, kami mengizinkan lalu lintas masuk dan keluar dari 10.0.0.0/16 (blok CIDR dari VPC AWS Microsoft AD Terkelola kami) pada port berikut:

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Autentikasi Kerberos
- TCP/UDP 389 - Protokol Akses Direktori Ringan (LDAP)
- TCP 445 - Blok Pesan Server (SMB)
- TCP 9389 - Active Directory Web Services (ADWS) (Opsional - Port ini harus terbuka jika Anda ingin menggunakan nama NetBIOS Anda alih-alih nama domain lengkap Anda untuk otentikasi dengan aplikasi seperti AWS Amazon atau Amazon Quick.) WorkDocs

Note

SMBv1 tidak lagi didukung.

Ini adalah port minimum yang diperlukan untuk menghubungkan VPC ke direktori yang dikelola sendiri. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

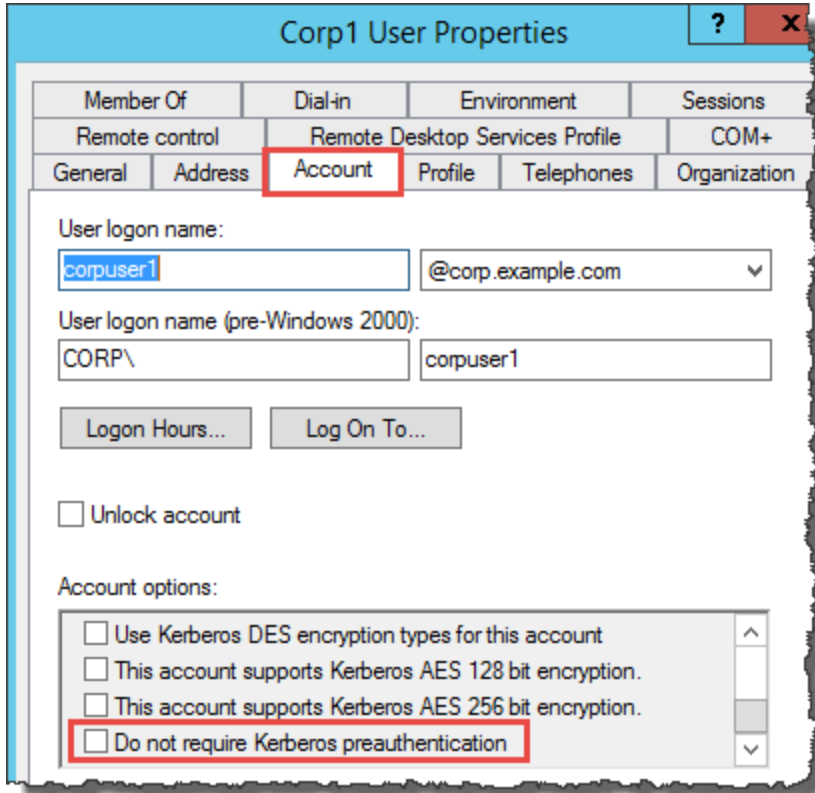
Pastikan bahwa Kerberos pra-autentikasi diaktifkan

Akun pengguna di kedua direktori harus mengaktifkan praaotentikasi Kerberos. Ini adalah default, tapi mari kita periksa properti dari setiap pengguna acak untuk memastikan tidak ada yang berubah.

Untuk melihat pengaturan Kerberos pengguna

1. Pada pengontrol domain yang dikelola sendiri, buka Server Manager.

2. Pada menu Alat, pilih Pengguna dan komputer Direktori Aktif.
3. Pilih folder Pengguna dan buka menu konteks (klik kanan). Pilih akun pengguna acak yang tercantum dalam panel kanan. Pilih Properti.
4. Pilih tab Akun. Di daftar Opsi akun, gulir ke bawah dan pastikan bahwa Tidak memerlukan preautentikasi Kerberos tidak dicentang.



Konfigurasi forwarder bersyarat DNS untuk domain yang dikelola sendiri

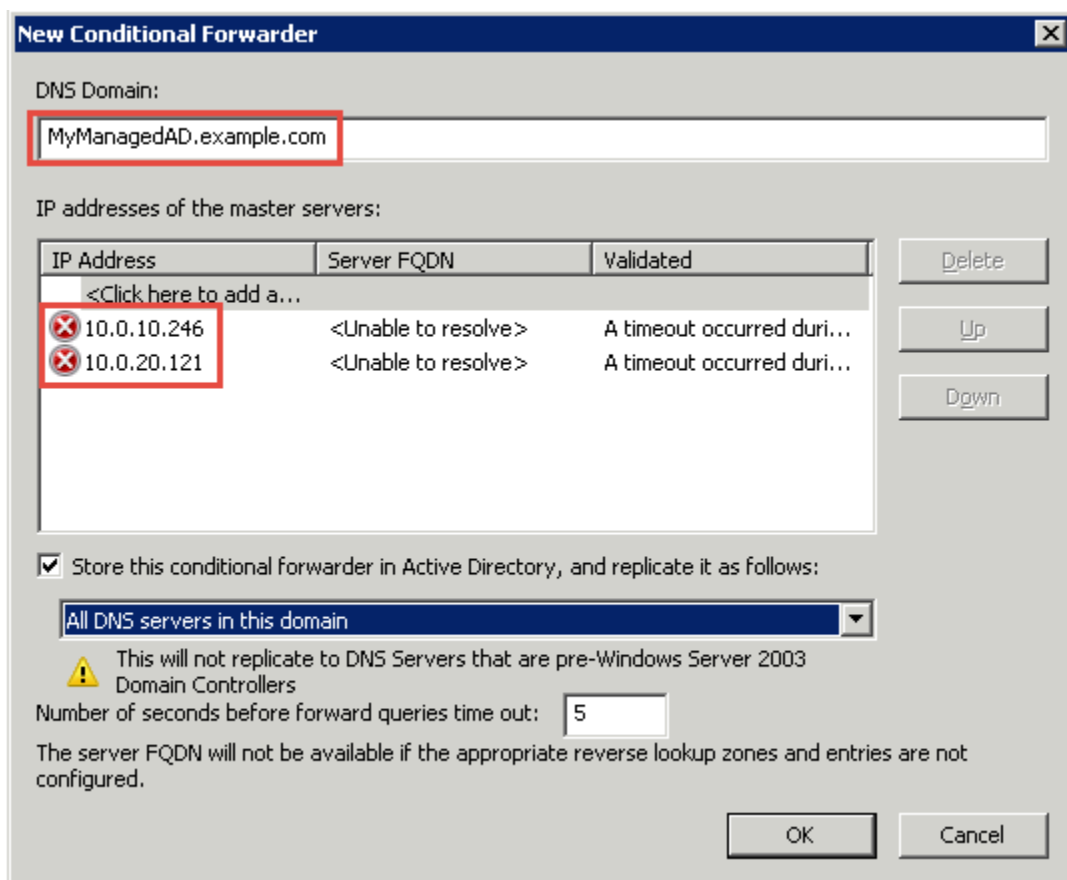
Anda harus mengatur penerusan bersyarat DNS pada setiap domain. Sebelum melakukan ini di domain yang dikelola sendiri, pertama-tama Anda akan mendapatkan beberapa informasi tentang iklan Microsoft yang AWS Dikelola.

Untuk mengonfigurasi forwarder bersyarat pada domain yang dikelola sendiri

1. Masuk ke Konsol Manajemen AWS dan buka [AWS Directory Service konsol](#).
2. Di panel navigasi, pilih Direktori.
3. Pilih ID direktori iklan Microsoft AWS Terkelola Anda.
4. Pada halaman Detail, perhatikan nilai-nilai dalam Nama direktori dan Alamat DNS dari direktori Anda.

5. Sekarang, kembali ke pengontrol domain yang dikelola sendiri. Buka Pengelola Server
6. Pada menu Alat, pilih DNS.
7. Pada pohon konsol, perluas server DNS dari domain di mana Anda mengatur kepercayaan. Server kami adalah CN7 VJ0 WIN-5V70 .corp.example.com.
8. Pada pohon konsol, pilih Penerusan Bersyarat.
9. Pada menu Tindakan, pilih Penerusan bersyarat baru.
10. Di domain DNS, ketik nama domain yang memenuhi syarat penuh (FQDN) dari AWS Microsoft AD Terkelola Anda, yang Anda sebutkan sebelumnya. Dalam contoh ini, FQDN adalah Ad.example.com. MyManaged
11. Pilih alamat IP server utama dan ketik alamat DNS direktori Microsoft AD AWS Terkelola Anda, yang Anda catat sebelumnya. Dalam contoh ini yaitu: 10.0.10.246, 10.0.20.121

Setelah memasukkan alamat DNS, Anda mungkin mendapatkan error “timeout” atau “tidak dapat menyelesaikan”. Anda biasanya dapat mengabaikan error ini.



12. Pilih Menyimpan penerusan bersyarat ini di Direktori Aktif dan mereplikasi sebagai berikut.
13. Pilih Semua server DNS dalam domain ini, lalu pilih OK.

Langkah Selanjutnya

[Langkah 2: Siapkan Microsoft AD yang AWS Dikelola](#)

Langkah 2: Siapkan Microsoft AD yang AWS Dikelola

Sekarang mari kita siapkan iklan Microsoft AWS Terkelola Anda untuk hubungan kepercayaan. Banyak dari langkah-langkah berikut hampir identik dengan apa yang baru saja Anda selesaikan untuk domain yang dikelola sendiri. Kali ini, bagaimanapun, Anda bekerja dengan Microsoft AD yang AWS Dikelola.

Mengkonfigurasi subnet VPC dan grup keamanan Anda

Anda harus mengizinkan lalu lintas dari jaringan yang dikelola sendiri ke VPC yang berisi iklan Microsoft yang AWS Dikelola. Untuk melakukan ini, Anda harus memastikan bahwa yang ACLs terkait dengan subnet yang digunakan untuk menyebarkan AD AWS Microsoft Terkelola dan aturan grup keamanan yang dikonfigurasi pada pengontrol domain Anda, keduanya memungkinkan lalu lintas yang diperlukan untuk mendukung trust.

Persyaratan port bervariasi berdasarkan versi Windows Server yang digunakan oleh pengendali domain Anda dan layanan atau aplikasi yang akan memanfaatkan kepercayaan. Untuk tujuan tutorial ini, Anda harus membuka port-port berikut ini:

Ke dalam

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Autentikasi Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 464 - Autentikasi Kerberos
- TCP 636 - LDAPS (LDAP melalui TLS/SSL)
- TCP 3268-3269 - Katalog Global
- TCP/UDP 49152-65535 - Port-port sementara untuk RPC

Note

SMBv1 tidak lagi didukung.

Ke luar

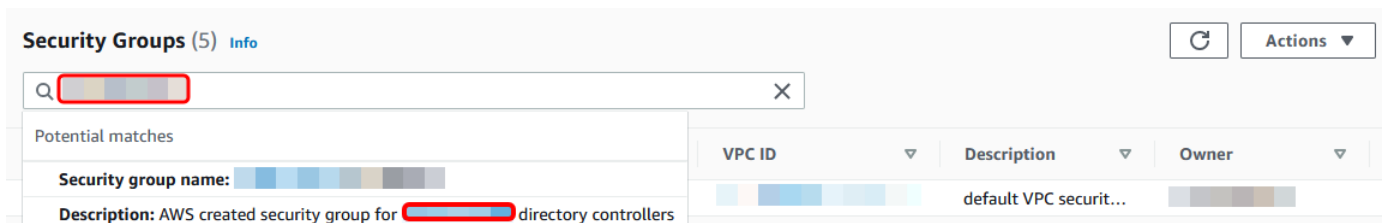
- SEMUA

Note

Ini adalah port minimum yang diperlukan untuk dapat menghubungkan VPC dan direktori yang dikelola sendiri. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

Untuk mengonfigurasi aturan keluar dan masuk pengontrol domain Microsoft AD AWS Terkelola

1. Kembali ke [Konsol AWS Directory Service](#). Dalam daftar direktori, perhatikan ID direktori untuk direktori Microsoft AD AWS Terkelola Anda.
2. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>
3. Pada panel navigasi, pilih Grup Keamanan.
4. Gunakan kotak pencarian untuk mencari ID direktori Microsoft AD AWS Terkelola Anda. Dalam hasil pencarian, pilih Grup Keamanan dengan deskripsi **AWS created security group for *yourdirectoryID* directory controllers**.



5. Pergi ke tab Aturan Keluar untuk grup keamanan tersebut. Pilih Edit aturan keluar, lalu Tambahkan aturan. Untuk aturan baru, masukkan nilai berikut:
- Jenis: SEMUA Lalu lintas
 - Protokol: SEMUA

- Tujuan menentukan lalu lintas yang dapat meninggalkan pengendali domain Anda dan ke mana ia akan pergi. Tentukan alamat IP tunggal atau cakupan alamat IP dalam notasi CIDR (misalnya, 203.0.113.5/32). Anda juga dapat menentukan nama atau ID grup keamanan lain di Region yang sama. Untuk informasi selengkapnya, lihat [Memahami konfigurasi dan penggunaan grup AWS keamanan direktori Anda](#).

6. Pilih Simpan Aturan.

Edit outbound rules info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules info

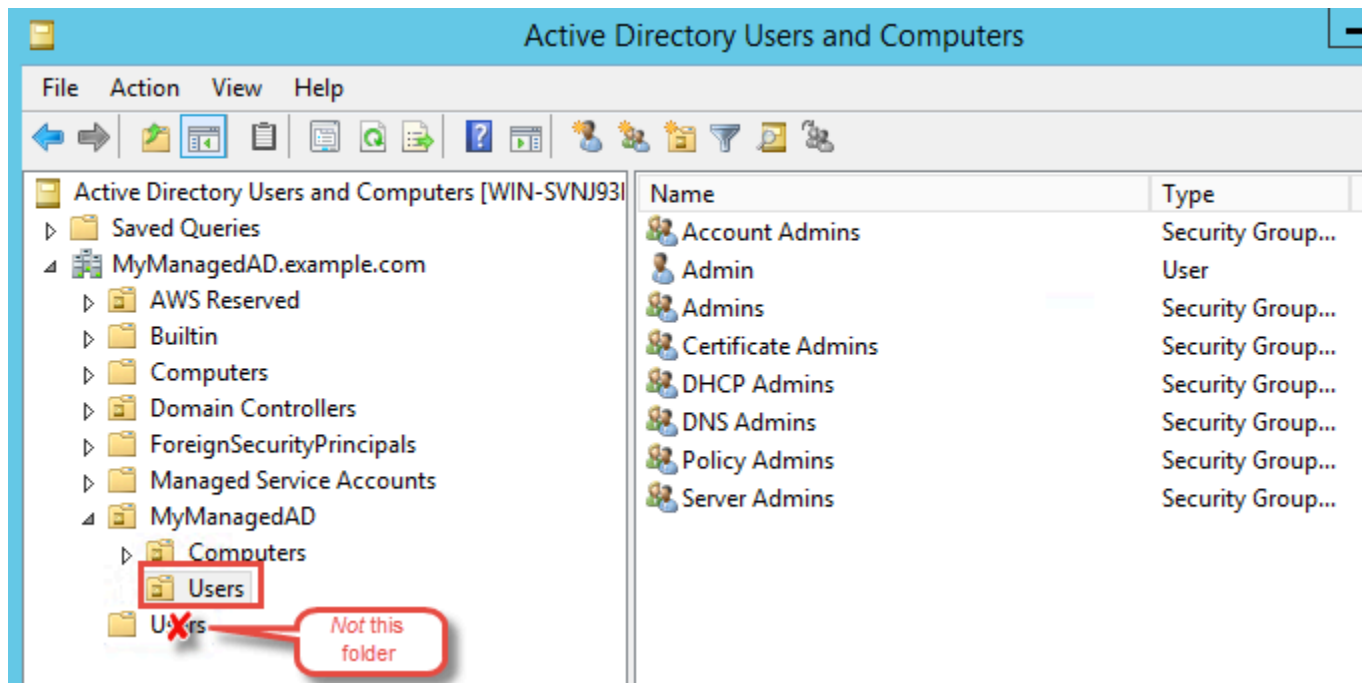
Security group rule ID	Type info	Protocol info	Port range info	Destination info	Description - optional info	
	All traffic	All	All	Anywhere...		Delete

Pastikan bahwa Kerberos pra-autentikasi diaktifkan

Sekarang Anda ingin mengonfirmasi bahwa pengguna di Microsoft AD AWS Terkelola Anda juga mengaktifkan pra-otentikasi Kerberos. Ini adalah proses yang sama yang Anda selesaikan untuk direktori yang dikelola sendiri. Ini adalah default, tapi mari kita periksa untuk memastikan tidak ada yang berubah.

Untuk melihat pengaturan kerberos pengguna

1. Masuk ke instans yang merupakan anggota direktori Microsoft AD AWS Terkelola menggunakan domain [AWS Akun Administrator Microsoft AD yang dikelola dan izin grup](#) untuk atau akun yang telah didelegasikan izin untuk mengelola pengguna di domain.
2. Jika mereka belum diinstal, instal alat Pengguna dan Komputer Direktori Aktif dan alat DNS. Pelajari cara memasang alat ini di [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#).
3. Buka Pengelola Server Pada menu Alat, pilih Pengguna dan komputer Direktori Aktif.
4. Pilih folder Pengguna di domain Anda. Perhatikan bahwa ini adalah folder Pengguna di bawah nama NetBIOS Anda, bukan folder Pengguna di bawah nama domain yang memenuhi syarat (FQDN).



5. Dalam daftar pengguna, klik kanan pada pengguna, dan kemudian pilih Properti.
6. Pilih tab Akun. Di daftar Opsi akun, pastikan bahwa Tidak memerlukan preautentikasi Kerberos tidak dicentang.

Langkah Selanjutnya

[Langkah 3: Buat hubungan kepercayaan](#)

Langkah 3: Buat hubungan kepercayaan

Sekarang setelah persiapan selesai, langkah-langkah terakhir adalah membuat kepercayaan.

Pertama, Anda membuat kepercayaan pada domain yang dikelola sendiri, dan akhirnya di Microsoft AD yang AWS Dikelola. Jika Anda memiliki masalah selama proses pembuatan kepercayaan, lihat [Alasan status pembuatan kepercayaan](#) untuk bantuan.

Konfigurasi kepercayaan pada Direktori Aktif yang dikelola sendiri

Dalam tutorial ini, Anda mengkonfigurasi kepercayaan forest dua arah. Namun, jika Anda membuat kepercayaan forest satu arah, ketahui bahwa arah kepercayaan pada masing-masing domain Anda harus saling melengkapi. Misalnya, jika Anda membuat kepercayaan keluar satu arah pada domain yang dikelola sendiri, Anda perlu membuat kepercayaan masuk satu arah pada iklan AWS Microsoft yang Dikelola.

 Note

AWS Microsoft AD yang dikelola juga mendukung kepercayaan eksternal. Namun, untuk tujuan tutorial ini, Anda akan membuat kepercayaan forest dua arah.

Untuk mengonfigurasi kepercayaan pada Direktori Aktif yang dikelola sendiri

1. Buka Pengelola Server dan pada menu Alat, pilih Domain Direktori Aktif dan Kepercayaan.
2. Buka menu konteks (klik kanan) dari domain Anda dan pilih Properties.
3. Pilih tab Kepercayaan dan pilih Kepercayaan baru. Ketik nama iklan Microsoft AWS Terkelola Anda dan pilih Berikutnya.
4. Pilih Kepercayaan forest. Pilih Berikutnya.
5. Pilih Dua arah. Pilih Berikutnya.
6. Pilih Hanya domain ini. Pilih Berikutnya.
7. Pilih Autentikasi seluruh forest. Pilih Berikutnya.
8. Ketik Kata sandi kepercayaan. Pastikan untuk mengingat kata sandi ini karena Anda akan membutuhkannya saat menyiapkan kepercayaan untuk iklan Microsoft AWS Terkelola Anda.
9. Di kotak dialog berikutnya, konfirmasi pengaturan Anda dan pilih Selanjutnya. Konfirmasikan bahwa kepercayaan telah dibuat dengan sukses dan pilih lagi Selanjutnya.
10. Pilih Tidak, jangan konfirmasi kepercayaan keluar. Pilih Berikutnya.
11. Pilih Tidak, jangan konfirmasi kepercayaan masuk. Pilih Berikutnya.

Konfigurasi kepercayaan di direktori Microsoft AD AWS Terkelola Anda

Terakhir, Anda mengonfigurasi hubungan trust hutan dengan direktori Microsoft AD AWS Terkelola Anda. Karena Anda membuat trust hutan dua arah pada domain yang dikelola sendiri, Anda juga membuat kepercayaan dua arah menggunakan direktori AWS Microsoft AD yang Dikelola.

 Note

Hubungan kepercayaan adalah fitur global dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [Konfigurasi replikasi Multi-Wilayah untuk AWS Microsoft AD yang Dikelola](#), prosedur berikut harus dilakukan di [Region primer](#). Perubahan akan diterapkan di semua

Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Untuk mengonfigurasi kepercayaan di direktori Microsoft AD yang AWS Dikelola

1. Kembali ke [Konsol AWS Directory Service](#).
2. Pada halaman Direktori, pilih ID AD Microsoft yang AWS Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. Pada halaman Tambahkan hubungan kepercayaan, tentukan jenis Trust. Dalam hal ini, kami memilih kepercayaan Hutan. Ketik FQDN domain yang dikelola sendiri (dalam tutorial ini). **corp.example.com** Ketik kata sandi kepercayaan yang sama dengan yang Anda gunakan saat membuat kepercayaan pada domain yang dikelola sendiri. Tentukan arah. Dalam hal ini, kami memilih Dua arah.
6. Di bidang Conditional forwarder, masukkan alamat IP server DNS yang dikelola sendiri. Dalam contoh ini, masukkan 172.16.10.153.
7. (Opsional) Pilih Tambahkan alamat IP lain dan masukkan alamat IP kedua untuk server DNS yang dikelola sendiri. Anda dapat menentukan hingga total empat server DNS.
8. Pilih Tambahkan.

Selamat. Anda sekarang memiliki hubungan kepercayaan antara domain yang dikelola sendiri (corp.example.com) dan iklan AWS Microsoft Terkelola (Ad.example.com). MyManaged Hanya satu hubungan yang dapat diatur antara kedua domain ini. Jika misalnya, Anda ingin mengubah arah kepercayaan ke satu arah, Anda harus terlebih dahulu menghapus hubungan kepercayaan yang ada ini dan membuat yang baru.

Untuk informasi selengkapnya, termasuk petunjuk tentang memverifikasi atau menghapus kepercayaan, lihat [Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri](#).

Tutorial: Buat hubungan kepercayaan antara dua domain Microsoft AD yang AWS Dikelola

Tutorial ini memandu Anda melalui semua langkah yang diperlukan untuk mengatur hubungan kepercayaan antara dua domain AWS Directory Service untuk Microsoft Active Directory.

Topik

- [Langkah 1: Siapkan Microsoft AD yang AWS Dikelola](#)
- [Langkah 2: Buat hubungan kepercayaan dengan domain Microsoft AD AWS Terkelola lainnya](#)

Lihat Juga

[Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri](#)

Langkah 1: Siapkan Microsoft AD yang AWS Dikelola

Di bagian ini, Anda akan menyiapkan iklan Microsoft AWS Terkelola untuk hubungan kepercayaan dengan iklan Microsoft AWS Terkelola lainnya. Banyak dari langkah-langkah berikut hampir identik dengan apa yang Anda lakukan [Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri](#). Namun, kali ini, Anda mengonfigurasi lingkungan Microsoft AD yang AWS Dikelola agar berfungsi satu sama lain.

Mengonfigurasi subnet VPC dan grup keamanan Anda

Anda harus mengizinkan lalu lintas dari satu jaringan Microsoft AD AWS Terkelola ke VPC yang berisi iklan AWS Microsoft Terkelola lainnya. Untuk melakukan ini, Anda harus memastikan bahwa yang ACLs terkait dengan subnet yang digunakan untuk menyebarkan AD AWS Microsoft Terkelola dan aturan grup keamanan yang dikonfigurasi pada pengontrol domain Anda, keduanya memungkinkan lalu lintas yang diperlukan untuk mendukung trust.

Persyaratan port bervariasi berdasarkan versi Windows Server yang digunakan oleh pengendali domain Anda dan layanan atau aplikasi yang akan memanfaatkan kepercayaan. Untuk tujuan tutorial ini, Anda harus membuka port-port berikut ini:

Ke dalam

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Autentikasi Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

Note

SMBv1 tidak lagi didukung.

- TCP/UDP 464 - Autentikasi Kerberos
- TCP 636 - LDAPS (LDAP melalui TLS/SSL)
- TCP 3268-3269 - Katalog Global
- TCP/UDP 1024-65535 - Port sementara untuk RPC

Ke luar

- SEMUA

Note

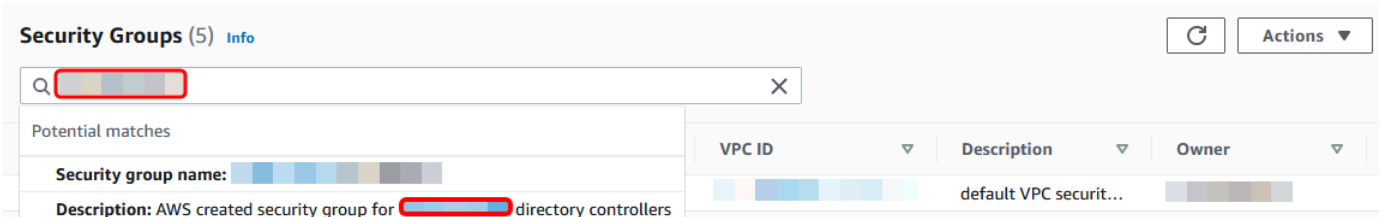
Ini adalah port minimum yang diperlukan untuk dapat menghubungkan VPCs dari kedua Microsoft AD yang AWS Dikelola. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka. Untuk informasi selengkapnya, lihat [Cara mengonfigurasi firewall untuk domain dan trust Active Directory di situs](#) web Microsoft.

Untuk mengonfigurasi aturan keluar pengontrol domain Microsoft AD AWS Terkelola

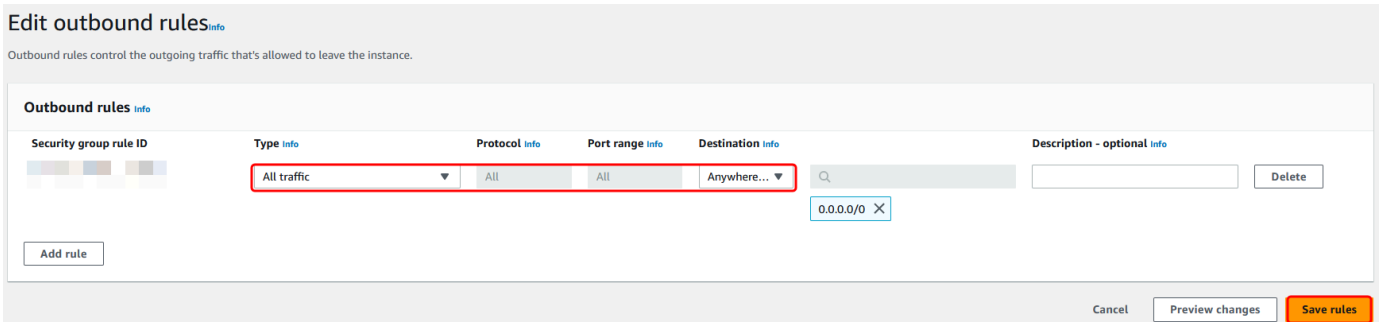
Note

Ulangi langkah 1-6 di bawah ini untuk setiap direktori.

1. Pergi ke [AWS Directory Service konsol](#). Dalam daftar direktori, perhatikan ID direktori untuk direktori Microsoft AD AWS Terkelola Anda.
2. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>
3. Pada panel navigasi, pilih Grup Keamanan.
4. Gunakan kotak pencarian untuk mencari ID direktori Microsoft AD AWS Terkelola Anda. Dalam hasil pencarian, pilih item dengan deskripsi **AWS created security group for *yourdirectoryID* directory controllers**.



5. Pergi ke tab Aturan Keluar untuk grup keamanan tersebut. Pilih Edit, kemudian Tambahkan aturan lain. Untuk aturan baru, masukkan nilai berikut:
 - Jenis: SEMUA Lalu lintas
 - Protokol: SEMUA
 - Tujuan menentukan lalu lintas yang dapat meninggalkan pengendali domain Anda dan ke mana ia akan pergi. Tentukan alamat IP tunggal atau cakupan alamat IP dalam notasi CIDR (misalnya, 203.0.113.5/32). Anda juga dapat menentukan nama atau ID grup keamanan lain di Region yang sama. Untuk informasi selengkapnya, lihat [Memahami konfigurasi dan penggunaan grup AWS keamanan direktori Anda](#).
6. Pilih Simpan.



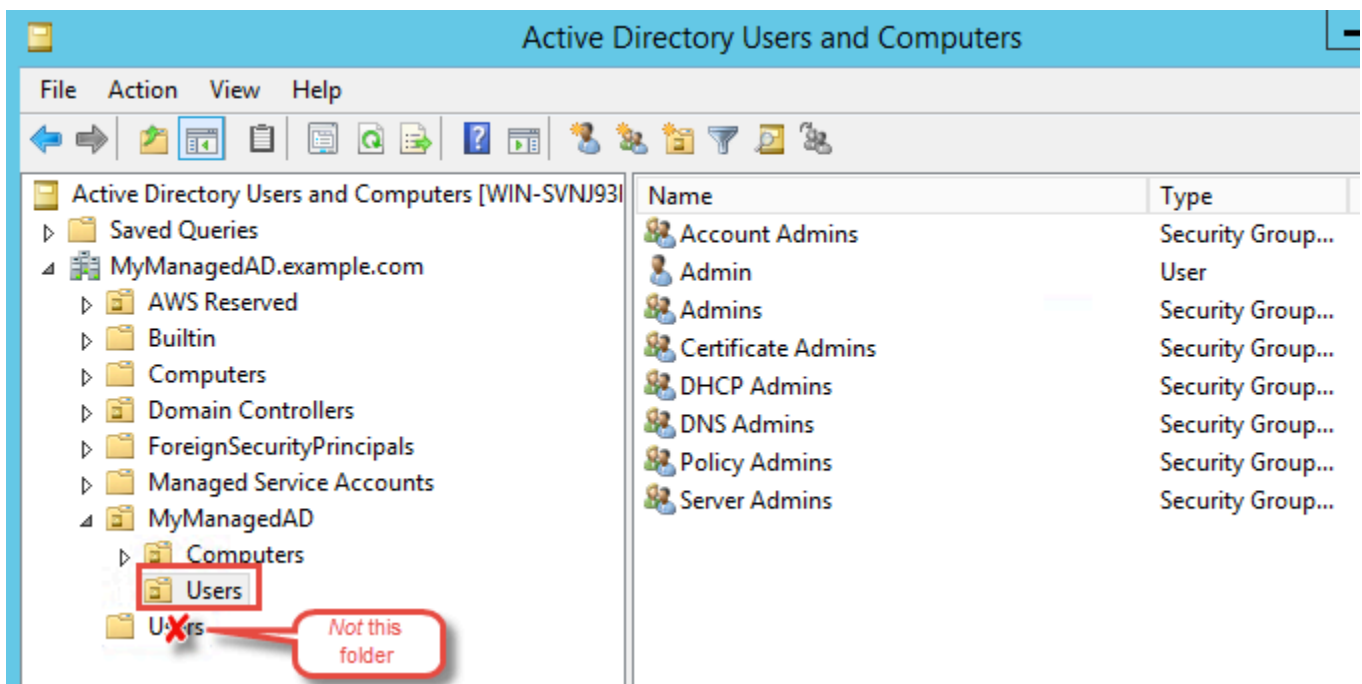
Pastikan bahwa Kerberos pra-autentikasi diaktifkan

Sekarang Anda ingin mengonfirmasi bahwa pengguna di Microsoft AD AWS Terkelola Anda juga mengaktifkan pra-otentikasi Kerberos. Ini adalah proses yang sama yang Anda selesaikan untuk

direktori on-premise Anda. Ini adalah default, tapi mari kita periksa untuk memastikan tidak ada yang berubah.

Untuk melihat pengaturan kerberos pengguna

1. Masuk ke instans yang merupakan anggota direktori Microsoft AD AWS Terkelola Anda menggunakan domain [AWS Akun Administrator Microsoft AD yang dikelola dan izin grup](#) untuk atau akun yang telah didelegasikan izin untuk mengelola pengguna di domain.
2. Jika mereka belum diinstal, instal alat Pengguna dan Komputer Direktori Aktif dan alat DNS. Pelajari cara memasang alat ini di [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#).
3. Buka Pengelola Server Pada menu Alat, pilih Pengguna dan komputer Direktori Aktif.
4. Pilih folder Pengguna di domain Anda. Perhatikan bahwa ini adalah folder Pengguna di bawah nama NetBIOS Anda, bukan folder Pengguna di bawah nama domain yang memenuhi syarat (FQDN).



5. Dalam daftar pengguna, klik kanan pada pengguna, dan kemudian pilih Properti.
6. Pilih tab Akun. Di daftar Opsi akun, pastikan bahwa Tidak memerlukan preautentikasi Kerberos tidak dicentang.

Langkah Selanjutnya

[Langkah 2: Buat hubungan kepercayaan dengan domain Microsoft AD AWS Terkelola lainnya](#)

Langkah 2: Buat hubungan kepercayaan dengan domain Microsoft AD AWS Terkelola lainnya

Sekarang setelah pekerjaan persiapan selesai, langkah terakhir adalah membuat kepercayaan antara dua domain Microsoft AD AWS Terkelola Anda. Jika Anda memiliki masalah selama proses pembuatan kepercayaan, lihat [Alasan status pembuatan kepercayaan](#) untuk bantuan.

Konfigurasi kepercayaan pada domain Microsoft AD AWS Terkelola pertama Anda

Dalam tutorial ini, Anda mengkonfigurasi kepercayaan forest dua arah. Namun, jika Anda membuat kepercayaan forest satu arah, ketahui bahwa arah kepercayaan pada masing-masing domain Anda harus saling melengkapi. Misalnya, jika Anda membuat kepercayaan keluar satu arah pada domain pertama ini, Anda perlu membuat kepercayaan masuk satu arah pada domain AWS Microsoft AD Terkelola kedua Anda.

Note

AWS Microsoft AD yang dikelola juga mendukung kepercayaan eksternal. Namun, untuk tujuan tutorial ini, Anda akan membuat kepercayaan forest dua arah.

Untuk mengonfigurasi kepercayaan pada domain Microsoft AD AWS Terkelola pertama Anda

1. Buka [konsol AWS Directory Service](#).
2. Pada halaman Direktori, pilih ID AD Microsoft AWS Terkelola pertama Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. Pada halaman Tambahkan hubungan kepercayaan, Ketik FQDN domain AWS Microsoft AD Terkelola kedua Anda. Pastikan untuk mengingat kata sandi ini karena Anda akan membutuhkannya saat menyiapkan kepercayaan untuk iklan Microsoft AWS Terkelola kedua Anda. Tentukan arah. Dalam hal ini, pilih Dua arah.

6. Di bidang Conditional forwarder, masukkan alamat IP server DNS AWS Microsoft AD terkelola kedua Anda.
7. (Opsional) Pilih Tambahkan alamat IP lain dan masukkan alamat IP kedua untuk server DNS Microsoft AD AWS Terkelola kedua Anda. Anda dapat menentukan hingga total empat server DNS.
8. Pilih Tambahkan. Kepercayaan akan gagal pada titik ini yang diharapkan sampai kita menciptakan sisi lain dari kepercayaan.

Konfigurasi kepercayaan di domain Microsoft AD AWS Terkelola kedua Anda

Sekarang, Anda mengonfigurasi hubungan trust hutan dengan direktori Microsoft AD AWS Terkelola kedua Anda. Karena Anda membuat trust hutan dua arah pada domain Microsoft AD AWS Terkelola pertama, Anda juga membuat kepercayaan dua arah menggunakan domain AWS Microsoft AD Terkelola ini.

Untuk mengonfigurasi kepercayaan pada domain Microsoft AD AWS Terkelola kedua Anda

1. Kembali ke [Konsol AWS Directory Service](#).
2. Pada halaman Direktori, pilih ID AD Microsoft AWS Terkelola kedua Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. Pada halaman Tambahkan hubungan kepercayaan, Ketik FQDN domain AWS Microsoft AD Terkelola pertama Anda. Ketik kata sandi kepercayaan yang sama yang Anda gunakan saat membuat kepercayaan pada domain on-premise Anda. Tentukan arah. Dalam hal ini, pilih Dua arah.
6. Di bidang Conditional forwarder, masukkan alamat IP server DNS AWS Microsoft AD terkelola pertama Anda.

7. (Opsional) Pilih Tambahkan alamat IP lain dan masukkan alamat IP kedua untuk server DNS Microsoft AD AWS Terkelola pertama Anda. Anda dapat menentukan hingga total empat server DNS.
8. Pilih Tambahkan. Kepercayaan harus diverifikasi segera setelah itu.
9. Sekarang, kembali ke kepercayaan yang Anda buat di domain pertama dan verifikasi kembali hubungan kepercayaan.

Selamat. Anda sekarang memiliki hubungan kepercayaan antara dua domain Microsoft AD yang AWS Dikelola. Hanya satu hubungan yang dapat diatur antara kedua domain ini. Jika misalnya, Anda ingin mengubah arah kepercayaan ke satu arah, Anda harus terlebih dahulu menghapus hubungan kepercayaan yang ada ini dan membuat yang baru.

Perluas skema AD Microsoft AWS Terkelola Anda

AWS Microsoft AD yang dikelola menggunakan skema untuk mengatur dan menegakkan bagaimana data direktori disimpan. Proses menambahkan definisi ke skema disebut sebagai “memperluas skema.” Ekstensi skema memungkinkan Anda mengubah skema direktori AWS Microsoft AD Terkelola menggunakan file LDAP Data Interchange Format (LDIF) yang valid. Untuk informasi lebih lanjut tentang skema AD dan cara untuk memperluas skema Anda, lihat topik yang tercantum di bawah ini.

Kapan harus memperpanjang skema AD Microsoft AWS Terkelola

Anda dapat memperluas skema Microsoft AD AWS Terkelola dengan menambahkan kelas dan atribut objek baru. Misalnya, Anda mungkin melakukan ini jika Anda memiliki aplikasi yang memerlukan perubahan pada skema Anda untuk mendukung kemampuan sign-on tunggal.

Anda juga dapat menggunakan ekstensi skema untuk mengaktifkan dukungan untuk aplikasi yang bergantung pada kelas objek Direktori Aktif tertentu dan atribut. Ini dapat sangat berguna dalam kasus di mana Anda perlu memigrasikan aplikasi perusahaan yang bergantung pada Microsoft AD yang AWS Dikelola, ke AWS cloud.

Setiap atribut atau kelas yang ditambahkan ke skema Direktori Aktif yang ada harus didefinisikan dengan ID unik. Dengan begitu ketika perusahaan menambahkan ekstensi ke skema, mereka dapat dijamin unik dan tidak bertentangan satu sama lain. Ini IDs disebut sebagai AD Object Identifiers (OIDs) dan disimpan di Microsoft AD yang AWS Dikelola.

Untuk memulai, lihat [Tutorial: Memperluas skema AD Microsoft AWS Terkelola Anda](#).

Topik terkait

- [Perluas skema AD Microsoft AWS Terkelola Anda](#)
- [Elemen skema](#)

Topik

- [Tutorial: Memperluas skema AD Microsoft AWS Terkelola Anda](#)

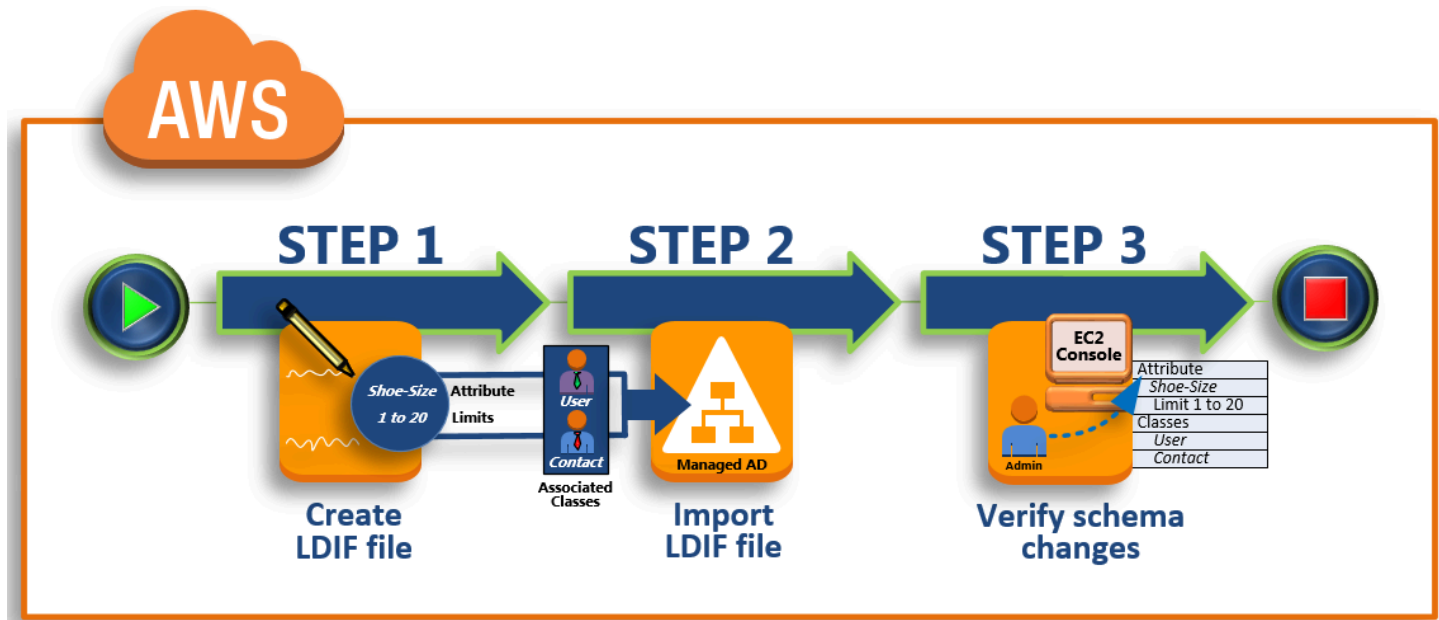
Tutorial: Memperluas skema AD Microsoft AWS Terkelola Anda

Dalam tutorial ini, Anda akan belajar cara memperluas skema untuk AWS direktori Directory Service for Microsoft Active Directory Anda, juga dikenal sebagai AWS Managed Microsoft AD, dengan menambahkan atribut dan kelas unik yang memenuhi persyaratan spesifik Anda. AWS Ekstensi skema Microsoft AD yang dikelola hanya dapat diunggah dan diterapkan menggunakan file skrip LDIF (Lightweight Directory Interchange Format) yang valid.

Atribut (attributeSchema) menentukan bidang dalam database sementara kelas (classSchema) menentukan tabel dalam database. Sebagai contoh, semua objek pengguna di Direktori Aktif ditentukan oleh kelas skema Pengguna sedangkan properti individu pengguna, seperti alamat email atau nomor telepon, masing-masing ditentukan oleh atribut.

Jika Anda ingin menambahkan properti baru, seperti Shoe-Size, Anda akan menentukan atribut baru, yang akan menjadi tipe integer. Anda juga bisa menentukan batas bawah dan atas seperti 1 sampai 20. Setelah objek Shoe-size attributeSchema telah dibuat, Anda kemudian akan mengubah objek classSchema Pengguna untuk memuat atribut itu. Atribut dapat ditautkan ke beberapa kelas. Shoe-size juga dapat ditambahkan ke kelas Kontak misalnya. Untuk informasi selengkapnya tentang skema Direktori Aktif, lihat [Kapan harus memperpanjang skema AD Microsoft AWS Terkelola](#).

Alur kerja ini memiliki tiga langkah dasar.



Langkah 1: Buat file LDIF Anda

Pertama, Anda membuat file LDIF dan tentukan atribut baru dan setiap kelas yang atribut harus ditambahkan ke. Anda menggunakan file ini untuk tahap berikutnya dari alur kerja.

Langkah 2: Impor file LDIF Anda

Pada langkah ini, Anda menggunakan AWS Directory Service konsol untuk mengimpor file LDIF ke lingkungan Microsoft Active Directory Anda.

Langkah 3: Verifikasi apakah ekstensi skema berhasil

Akhirnya, sebagai administrator, Anda menggunakan instans EC2 untuk memverifikasi bahwa ekstensi baru muncul di Snap-in skema Direktori Aktif.

Langkah 1: Buat file LDIF Anda

Sebuah file LDIF adalah format pertukaran data teks biasa standar untuk mewakili konten direktori [LDAP](#) (Lightweight Directory Access Protocol) dan permintaan pembaruan. LDIF menyampaikan konten direktori sebagai satu set catatan, satu catatan untuk setiap objek (atau entri). Hal ini juga merupakan permintaan pembaruan, seperti Menambahkan, Memodifikasi, Menghapus, dan Mengubah nama, sebagai satu set catatan, satu catatan untuk setiap permintaan pembaruan.

AWS Directory Service Mengimpor file LDIF Anda dengan skema berubah dengan menjalankan `ldifde.exe` aplikasi di direktori AWS Microsoft AD Terkelola Anda. Oleh karena itu, Anda akan

merasa terbantu untuk memahami sintaks skrip LDIF. Untuk informasi selengkapnya, lihat [Skrip LDIF](#).

Beberapa alat LDIF pihak ketiga dapat mengekstrak, membersihkan, dan memperbarui pembaruan skema Anda. Terlepas dari alat yang Anda gunakan, penting untuk memahami bahwa semua pengidentifikasi yang digunakan dalam file LDIF Anda harus unik.

Kami sangat menyarankan Anda meninjau konsep-konsep berikut dan tips sebelum membuat file LDIF Anda.

- Elemen skema - Pelajari tentang elemen skema seperti atribut, kelas, objek IDs, dan atribut terkait. Untuk informasi selengkapnya, lihat [Elemen skema](#).
- Urutan item – Pastikan bahwa urutan di mana item dalam file LDIF Anda ditata mengikuti [Pohon Informasi Direktori \(DIT\)](#) dari atas ke bawah. Aturan umum untuk pengurutan dalam file LDIF meliputi hal berikut ini:
 - Pisahkan item dengan garis kosong.
 - Buat daftar item anak setelah item induknya.
 - Pastikan bahwa item seperti atribut atau kelas objek ada di dalam skema. Jika mereka tidak ada, Anda harus menambahkannya ke skema sebelum mereka dapat digunakan. Misalnya, sebelum Anda dapat menetapkan atribut ke kelas, atribut harus dibuat.
- Format DN – Untuk setiap instruksi baru dalam file LDIF, tentukan nama yang dibedakan (DN) sebagai baris pertama dari instruksi. DN mengidentifikasi objek Active Directory dalam pohon objek Active Directory dan harus berisi komponen domain untuk direktori Anda. Sebagai contoh, komponen domain untuk direktori dalam tutorial ini adalah DC=example,DC=com.

DN harus menyertakan nama umum objek Active Directory (CN). Entri CN pertama mewakili atribut atau nama kelas. Untuk memperluas skema Active Directory, gunakan CN=Schema,CN=Configuration. Ingat bahwa Anda tidak dapat mengubah konten objek Active Directory. Format DN umum berikut.

```
dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
```

Untuk tutorial ini, DN untuk atribut Shoe-Size baru akan terlihat seperti:

```
dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
```

- Peringatan – Tinjau peringatan di bawah ini sebelum Anda memperpanjang skema Anda.
 - Sebelum Anda memperpanjang skema Direktori Aktif Anda, penting untuk meninjau peringatan Microsoft pada dampak operasi ini. Untuk informasi selengkapnya, lihat [Apa yang Harus Anda Ketahui Sebelum Memperluas Skema](#).
 - Anda tidak dapat menghapus atribut skema atau kelas. Karena itu, jika Anda membuat kesalahan dan tidak ingin memulihkan dari cadangan, Anda hanya dapat menonaktifkan objek. Untuk informasi selengkapnya, lihat [Menonaktifkan Kelas dan Atribut yang Ada](#).
 - Perubahan defaultSecurityDescriptor tidak didukung.

Untuk mempelajari lebih lanjut tentang cara file LDIF dibuat dan melihat contoh file LDIF yang dapat digunakan untuk menguji ekstensi skema AWS Microsoft AD Terkelola, lihat artikel [Cara Memperluas Skema Direktori AWS Microsoft AD Terkelola Anda](#) di Blog Keamanan. AWS

Langkah Selanjutnya

[Langkah 2: Impor file LDIF Anda](#)

Langkah 2: Impor file LDIF Anda

Anda dapat memperluas skema Anda dengan mengimpor file LDIF dari AWS Directory Service konsol atau dengan menggunakan API. Untuk informasi selengkapnya tentang cara melakukannya dengan ekstensi skema APIs, lihat [Referensi AWS Directory Service API](#). Pada saat ini, AWS tidak mendukung aplikasi eksternal, seperti Microsoft Exchange, untuk melakukan pembaruan skema secara langsung.

Important

Saat Anda membuat pembaruan ke skema direktori Microsoft AD AWS Terkelola, operasi tidak dapat dibalik. Dengan kata lain, setelah Anda membuat kelas atau atribut baru, Active Directory tidak mengizinkan Anda untuk menghapusnya. Namun, Anda dapat menonaktifkannya.

Jika Anda harus menghapus perubahan skema, salah satu pilihan adalah untuk memulihkan direktori dari snapshot sebelumnya. Memulihkan snapshot mengembalikan skema dan data direktori kembali ke titik sebelumnya, bukan hanya skema. Perhatikan, usia maksimum yang didukung dari snapshot adalah 180 hari. Untuk informasi selengkapnya, lihat [Masa simpan yang berguna dari backup keadaan sistem Direktori Aktif](#) di situs web Microsoft.

Sebelum proses pembaruan dimulai, Microsoft AD yang AWS dikelola mengambil snapshot untuk mempertahankan status direktori Anda saat ini.

 Note

Ekstensi skema adalah fitur global dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [Konfigurasi replikasi Multi-Wilayah untuk AWS Microsoft AD yang Dikelola](#), prosedur berikut harus dilakukan di [Region primer](#). Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Untuk mengimpor file LDIF Anda

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Pemeliharaan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pemeliharaan.
4. Di bagian Ekstensi skema, pilih Tindakan, dan kemudian pilih Unggah dan perbarui skema.
5. Di kotak dialog, klik Browse, pilih file LDIF yang valid, ketik deskripsi, dan kemudian pilih Memperbarui skema.

 Important

Memperpanjang skema adalah operasi kritis. Jangan menerapkan pembaruan skema apa pun di lingkungan produksi tanpa terlebih dahulu mengujinya dengan aplikasi Anda di lingkungan pengembangan atau pengujian.

Bagaimana file LDIF diterapkan

Setelah file LDIF Anda diunggah, AWS Microsoft AD yang Dikelola mengambil langkah-langkah untuk melindungi direktori Anda dari kesalahan karena menerapkan perubahan dalam urutan berikut.

1. Memvalidasi file LDIF. Karena skrip LDIF dapat memanipulasi objek apa pun di domain, AWS Microsoft AD yang Dikelola menjalankan pemeriksaan tepat setelah Anda mengunggah untuk membantu memastikan bahwa operasi impor tidak akan gagal. Hal ini termasuk pemeriksaan untuk memastikan hal berikut:
 - Objek yang akan diperbarui hanya diadakan dalam kotainer skema
 - Bagian DC (pengendali domain) cocok dengan nama domain di mana skrip LDIF berjalan
2. Mengambil snapshot dari direktori Anda. Anda dapat menggunakan snapshot tersebut untuk memulihkan direktori Anda jika Anda mengalami masalah dengan aplikasi Anda setelah memperbarui skema.
3. Menerapkan perubahan ke DC tunggal. AWS Microsoft AD yang dikelola mengisolasi salah satu dari Anda DCs dan menerapkan pembaruan dalam file LDIF ke DC yang terisolasi. Kemudian memilih salah satu dari Anda DCs untuk menjadi skema utama, menghapus DC itu dari replikasi direktori, dan menerapkan file LDIF Anda menggunakan `Ldifde.exe`
4. Replikasi terjadi pada semua DCs. AWS Microsoft AD yang dikelola menambahkan DC yang terisolasi kembali ke replikasi untuk menyelesaikan pembaruan. Saat ini semua terjadi, direktori Anda terus menyediakan layanan Direktori Aktif untuk aplikasi Anda tanpa gangguan.

Langkah selanjutnya

[Langkah 3: Verifikasi apakah ekstensi skema berhasil](#)

Langkah 3: Verifikasi apakah ekstensi skema berhasil

Setelah Anda menyelesaikan proses impor, penting untuk memverifikasi bahwa pembaruan skema diterapkan ke direktori Anda. Hal ini sangat penting sebelum Anda bermigrasi atau memperbarui aplikasi yang bergantung pada pembaruan skema. Anda dapat melakukannya dengan menggunakan berbagai alat LDAP yang berbeda atau dengan menulis alat uji yang mengeluarkan perintah LDAP yang sesuai.

Prosedur ini menggunakan Active Directory Schema Snap-in and/or PowerShell untuk memverifikasi bahwa pembaruan skema diterapkan. Anda harus menjalankan alat ini dari komputer yang merupakan domain yang bergabung dengan iklan Microsoft AWS Terkelola Anda. Ini bisa berupa server Windows yang berjalan di jaringan on-premise Anda dengan akses ke virtual private cloud (VPC) Anda atau melalui koneksi virtual private network (VPN). Anda juga dapat menjalankan alat ini pada instans Windows Amazon EC2 (lihat [Cara untuk meluncurkan instans EC2 baru dengan bergabung domain mulus](#)).

Untuk memverifikasi menggunakan Snap-in skema Direktori Aktif

1. Instal Skema Direktori Aktif Snap-In menggunakan instruksi di situs web. [TechNet](#)
2. Buka Konsol Manajemen Microsoft (MMC) dan perluas pohon Skema AD untuk direktori Anda.
3. Navigasikan melalui folder Kelas dan Atribut sampai Anda menemukan perubahan skema yang Anda buat sebelumnya.

Untuk memverifikasi menggunakan PowerShell

1. Buka PowerShell jendela.
2. Gunakan Get-ADObject seperti yang ditunjukkan di bawah ini untuk memverifikasi perubahan skema. Contoh:

```
get-adobject -Identity 'CN=Shoe-  
Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

Langkah opsional

[Tambahkan nilai ke atribut baru - Opsional](#)

Tambahkan nilai ke atribut baru - Opsional

Gunakan langkah opsional ini ketika Anda telah membuat atribut baru dan ingin menambahkan nilai baru ke atribut di direktori Microsoft AD yang AWS Dikelola.

Untuk menambahkan nilai ke atribut

1. Buka utilitas baris PowerShell perintah dan atur atribut baru dengan perintah berikut. Dalam contoh ini, kita akan menambahkan nilai EC2 InstanceId baru ke atribut untuk komputer tertentu.

```
PS C:\> set-adcomputer -Identity computer name -add @{example-  
EC2InstanceId = 'EC2 instance ID'}
```

2. Anda dapat memvalidasi jika nilai EC2 InstanceId ditambahkan ke objek komputer dengan menjalankan perintah berikut:

```
PS C:\> get-adcomputer -Identity computer name -Property example-  
EC2InstanceId
```


Sumber daya terkait

Tautan sumber daya berikut terletak di situs web Microsoft dan memberikan informasi terkait.

- [Memperluas Skema \(Windows\)](#)
- [Skema Direktori Aktif \(Windows\)](#)
- [Skema Direktori Aktif](#)
- [Administrasi Windows: Memperluas Skema Direktori Aktif](#)
- [Pembatasan pada Ekstensi Skema \(Windows\)](#)
- [Ldifde](#)

Cara untuk bergabung dengan instans Amazon EC2 ke AWS Microsoft AD yang Dikelola

Anda dapat menggabungkan instans Amazon EC2 dengan mulus ke domain Direktori Aktif saat instans diluncurkan. Untuk informasi selengkapnya, lihat [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#). Anda juga dapat meluncurkan instans EC2 dan menggabungkannya ke domain Active Directory langsung dari Directory Service konsol dengan [AWS Systems Manager Automation](#).

Jika Anda perlu menggabungkan instans EC2 secara manual ke domain Active Directory, Anda harus meluncurkan instance di Region yang tepat dan grup keamanan atau subnet, lalu gabungkan instance ke domain.

Untuk dapat terhubung dari jarak jauh ke instans ini, Anda harus memiliki konektivitas IP ke instans dari jaringan di mana Anda menghubungkannya dari. Dalam kebanyakan kasus, ini mengharuskan gateway internet dilampirkan ke VPC Anda dan instans tersebut memiliki alamat IP publik.

Topik

- [Meluncurkan instans administrasi direktori di Direktori Aktif Microsoft AD AWS Terkelola](#)
- [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#)
- [Bergabung dengan instans Amazon EC2 Linux ke Direktori Aktif AWS Microsoft AD Terkelola](#)
- [Bergabung dengan instans Amazon EC2 Mac ke Direktori Aktif AWS Microsoft AD Terkelola](#)
- [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#)
- [Membuat atau mengubah opsi DHCP yang disetel untuk Microsoft AD yang AWS Dikelola](#)

Meluncurkan instans administrasi direktori di Direktori Aktif Microsoft AD AWS Terkelola

Prosedur ini meluncurkan instans Windows administrasi direktori Amazon EC2 di Konsol Manajemen AWS Otomatisasi AWS Systems Manager menggunakan untuk mengelola direktori Anda. Anda juga dapat melakukannya dengan menjalankan otomatisasi [AWS-Create DSManagement Instance](#) di konsol AWS Systems Manager Otomasi secara langsung.

Untuk informasi selengkapnya, lihat tautan berikut:

- [Menyederhanakan domain Direktori Aktif bergabung dengan AWS Systems Manager](#)
- [Bagaimana cara saya bergabung AWS Systems Manager dengan Windows instans EC2 yang sedang berjalan ke domain saya? Directory Service](#)

Prasyarat

Prasyarat berikut diperlukan untuk menyelesaikan tutorial ini:

- Anda harus mengatur AWS Systems Manager. Untuk informasi selengkapnya, lihat [Menyiapkan AWS Systems Manager](#).
- Anda akan memerlukan [peran profil instans IAM](#) yang memungkinkan Systems Manager dan Microsoft AD yang AWS Dikelola.
 - Untuk informasi selengkapnya tentang Systems Manager, lihat [Mengonfigurasi izin instans yang diperlukan untuk Systems Manager](#).
 - Peran instans IAM memerlukan kebijakan AWS terkelola berikut agar Windows instans administrasi direktori EC2 Anda dapat bergabung dengan domain AWS Microsoft AD yang Dikelola:
 - **AmazonSSMManagedInstanceCore**
 - **AmazonSSMDirectoryServiceAccess**
- VPC yang terhubung ke AWS Microsoft AD Terkelola Anda harus mengizinkan akses ke titik akhir publik Directory Service . Untuk informasi selengkapnya, lihat [Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS](#).
- Anda harus mengaktifkan izin berikut di akun Anda untuk meluncurkan instans EC2 administrasi direktori dari konsol:
 - **ds:DescribeDirectories**

- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2>DeleteSecurityGroup
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeKeyPairs
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:RunInstances
- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam>DeleteInstanceProfile
- iam>DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam>ListAttachedRolePolicies
- iam>ListInstanceProfiles
- iam>ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ~~ssm>DeleteDocument~~
- ssm:DescribeInstanceInformation

- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:ListDocuments`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`
- `ssm:GetDocument`

Meluncurkan instans EC2 administrasi direktori di Konsol Manajemen AWS

1. Masuk ke [konsol Directory Service](#) tersebut.
2. Di bawah Active Directory, pilih Direktori.
3. Pilih ID Direktori direktori tempat Anda ingin meluncurkan instans EC2 administrasi direktori.
4. Pada halaman direktori, di pojok kanan atas, pilih Tindakan.
5. Dalam daftar dropdown Actions, pilih Launch directory administration EC2 instance.
6. Pada halaman instans EC2 administrasi direktori Launch, di bawah parameter Input, lengkapi bidangnya.
 - a. (Opsional) Anda dapat memberikan key pair untuk instance tersebut. Dari Nama Pasangan Kunci - daftar dropdown opsional, pilih key pair.
 - b. (Opsional) Pilih Lihat AWS CLI perintah untuk melihat contoh yang Anda gunakan AWS CLI untuk menjalankan otomatisasi ini.
7. Pilih Kirim.
8. Anda dibawa kembali ke halaman direktori. Flashbar hijau ditampilkan di bagian atas layar Anda untuk menunjukkan bahwa Anda berhasil memulai peluncuran.

Melihat administrasi direktori EC2 instans

Jika Anda belum meluncurkan instans EC2 apa pun untuk direktori, tanda hubung (-) ditampilkan di bawah instans EC2 administrasi direktori.

1. Di bawah Active Directory, pilih Direktori dan pilih direktori yang ingin Anda lihat.

2. Di bawah Detail direktori, di bawah Instans EC2 administrasi direktori, pilih satu atau semua instance Anda untuk dilihat.
3. Saat memilih instans, Anda diarahkan ke halaman EC2 Connect to instance untuk menghubungkan desktop jarak jauh ke instans Anda.

Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola

Anda dapat meluncurkan dan bergabung dengan Windows instans Amazon EC2 ke AWS Microsoft AD yang Dikelola. Atau, Anda dapat menggabungkan Windows instans EC2 yang ada secara manual ke Microsoft AD yang AWS Dikelola.

Seamlessly join EC2 Windows instance

Prosedur ini menggabungkan instans Amazon Windows EC2 dengan mulus ke Microsoft AD yang AWS Dikelola. Jika Anda perlu melakukan gabungan domain tanpa batas di beberapa Akun AWS, lihat [Tutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus](#). Untuk informasi selengkapnya tentang Amazon EC2, lihat [Apa itu Amazon EC2?](#).

Prasyarat

Agar domain bergabung dengan instans EC2 dengan mulus, Anda harus menyelesaikan yang berikut ini:

- Memiliki iklan Microsoft yang AWS Dikelola. Untuk mempelajari selengkapnya, lihat [Membuat Microsoft AD yang AWS Dikelola](#).
- Anda memerlukan izin IAM berikut untuk bergabung dengan instans EC2 dengan mulus: Windows
 - Profil Instans IAM dengan izin IAM berikut:
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - Domain pengguna yang bergabung dengan EC2 ke AWS Microsoft AD Terkelola memerlukan izin IAM berikut:
 - Directory Service Izin:
 - "ds:DescribeDirectories"

- "ds:CreateComputer"
- Izin VPC Amazon:
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
- Izin EC2:
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"
 - "ec2:RunInstances"
 - "ec2:CreateTags"
- AWS Systems Manager Izin:
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"

Saat iklan Microsoft AWS Terkelola dibuat, grup keamanan dibuat dengan aturan masuk dan keluar. Untuk mempelajari lebih lanjut tentang aturan dan port ini, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#). Agar domain bergabung dengan Windows instans EC2 dengan mulus, VPC tempat Anda meluncurkan instans harus mengizinkan port yang sama yang diizinkan dalam aturan masuk dan keluar grup keamanan AWS Microsoft AD Terkelola.

- Bergantung pada keamanan jaringan dan pengaturan firewall Anda, Anda mungkin diminta untuk mengizinkan lalu lintas keluar tambahan. Lalu lintas ini akan untuk HTTPS (port 443) ke titik akhir berikut:

Titik akhir	Peran
ec2messages. <i>region</i> .amazonaws.com	Membuat dan menghapus saluran sesi dengan layanan Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .
ssm. <i>region</i> .amazonaws.com	Titik akhir untuk AWS Systems Manager Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .
ssmmessages. <i>region</i> .amazonaws.com	Membuat dan menghapus saluran sesi dengan layanan Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .
ds. <i>region</i> .amazonaws.com	Titik akhir untuk Directory Service. Untuk informasi selengkapnya, lihat Ketersediaan wilayah untuk Directory Service .

- Sebaiknya gunakan server DNS yang akan menyelesaikan nama domain Microsoft AD AWS Terkelola Anda. Untuk melakukannya, Anda dapat membuat set opsi DHCP. Untuk informasi selengkapnya, lihat [Membuat atau mengubah opsi DHCP yang disetel untuk Microsoft AD yang AWS Dikelola](#).
- Jika Anda memilih untuk tidak membuat set opsi DHCP, maka server DNS Anda akan statis dan dikonfigurasi oleh AWS Microsoft AD yang Dikelola.

Untuk bergabung dengan instans Amazon Windows EC2 dengan mulus

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Di bilah navigasi, pilih yang AWS Region sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Nama dan Tag, masukkan nama yang ingin Anda gunakan untuk instans Windows EC2 Anda.

5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih Windows di panel Mulai Cepat. Anda dapat mengubah Windows Amazon Machine Image (AMI) dari daftar dropdown Amazon Machine Image (AMI).
7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada.
 - a. Untuk membuat key pair baru, pilih Create new key pair.
 - b. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format.
 - c. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk.
 - d. Pilih create key pair.
 - e. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

**Important**

Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat [Connect to the internet menggunakan gateway internet](#) di Panduan Pengguna Amazon VPC.

11. Di bawah Auto-assign IP publik, pilih Aktifkan.

Untuk informasi selengkapnya tentang pengalamatan IP publik dan pribadi, lihat pengalamatan [IP instans Amazon EC2](#) di Panduan Pengguna Amazon EC2.

12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

 Note

Setelah memilih direktori Gabung Domain, Anda mungkin melihat:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:

- Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
- Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, Anda dapat memilih profil instans IAM yang ada atau membuat yang baru. Pilih profil instans IAM yang memiliki kebijakan AWS terkelola Amazon SSMManged InstanceCore dan Amazon yang SSMDirectory ServiceAccess dilampirkan padanya dari daftar dropdown profil instans IAM. Untuk membuat yang baru, pilih Buat tautan profil IAM baru, lalu lakukan hal berikut:

1. Pilih Buat peran.
2. Di bawah Pilih entitas tepercaya, pilih AWS layanan.

3. Di bawah Kasus penggunaan, pilih EC2.
4. Di bawah Tambahkan izin, dalam daftar kebijakan, pilih SSMDirectory ServiceAccess kebijakan Amazon SSManaged InstanceCore dan Amazon. Untuk memfilter daftar, **SSM** ketik kotak pencarian. Pilih Berikutnya.

 Note

Amazon SSMDirectory ServiceAccess menyediakan izin untuk menggabungkan instance ke Active Directory yang dikelola oleh. Directory ServiceAmazon SSManaged InstanceCore memberikan izin minimum yang diperlukan untuk menggunakan AWS Systems Manager layanan ini. Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat [Buat profil instans IAM untuk Systems Manager](#) di Panduan Pengguna AWS Systems Manager .

5. Pada halaman Nama, tinjau, dan buat, masukkan nama Peran. Anda akan memerlukan nama peran ini untuk melampirkan ke instans EC2.
 6. (Opsional) Anda dapat memberikan deskripsi profil instans IAM di bidang Deskripsi.
 7. Pilih Buat peran.
 8. Kembali ke Luncurkan halaman instans dan pilih ikon penyegaran di sebelah profil instans IAM. Profil instans IAM baru Anda harus terlihat di daftar dropdown profil instans IAM. Pilih profil baru dan biarkan pengaturan lainnya dengan nilai defaultnya.
16. Pilih Luncurkan instans.

Manually join EC2 Windows instance

Untuk menggabungkan Windows instans Amazon EC2 yang ada secara manual ke Direktori Aktif AWS Microsoft AD Terkelola, instans harus diluncurkan menggunakan parameter seperti yang ditentukan dalam. [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#)

Anda akan memerlukan alamat IP dari server DNS Microsoft AD yang AWS Dikelola. Informasi ini dapat ditemukan di bawah Layanan Direktori > Direktori > tautan ID Direktori untuk direktori Anda> Detail direktori dan bagian Jaringan & Keamanan.

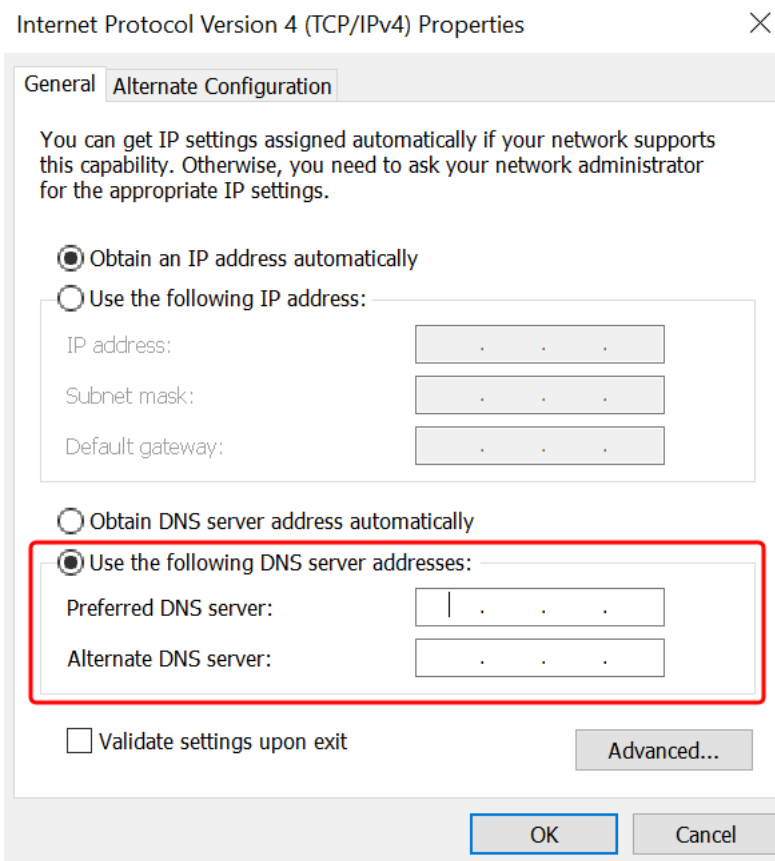
The screenshot displays the AWS Directory Service console for a specific directory instance. The left sidebar shows the navigation menu with 'Directory Service' selected. The main content area shows the directory details for 'd-1234567890'. The 'Directory details' section includes fields for Directory type (Microsoft AD), Edition (Standard), Operating system version (Windows Server 2019), Directory DNS name (corp.example.com), Directory NetBIOS name (corp), and Directory administration EC2 instance(s) (-). Below this, the 'Networking details' section shows the VPC, Availability zones (us-east-2a, us-east-2b), and Subnets. The DNS addresses for the subnets are listed as 192.0.2.1 and 198.51.100.1.

Untuk menggabungkan instans Windows ke Direktori Aktif Microsoft AD AWS Terkelola

1. Connect ke instans menggunakan klien Remote Desktop Protocol.
 2. Buka kotak dialog IPv4 TCP/properties pada instance.
 - a. Buka Koneksi Jaringan.
- Tip**

Anda dapat membuka Koneksi Jaringan langsung dengan menjalankan hal berikut dari prompt perintah pada instans.

```
%SystemRoot%\system32\control.exe ncpa.cpl
```
- b. Buka menu konteks (klik kanan) untuk koneksi jaringan yang aktif mana pun dan pilih Properti .
 - c. Dalam kotak dialog properti koneksi, buka (klik dua kali) Protokol Internet Versi 4.
3. Pilih Gunakan alamat server DNS berikut, ubah server DNS pilihan dan alamat server DNS alternatif ke alamat IP server DNS yang disediakan AWS Microsoft Ad-provided, dan pilih OK.



4. Buka kotak dialog Properti Sistem untuk instans, pilih tab Nama Komputer, dan pilih Ubah.

Tip

Anda dapat membuka kotak dialog Properti Sistem langsung dengan menjalankan hal berikut dari prompt perintah pada instans.

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. Di bidang Anggota, pilih Domain, masukkan nama yang sepenuhnya memenuhi syarat dari Direktori Aktif Microsoft AD AWS Terkelola Anda, dan pilih OK.
6. Saat diminta nama dan kata sandi untuk administrator domain, masukkan nama pengguna dan kata sandi akun yang memiliki hak istimewa bergabung domain. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

 Note

Anda dapat memasukkan nama domain yang sepenuhnya memenuhi syarat atau nama NetBIOS, diikuti dengan garis miring terbalik (\), dan kemudian nama pengguna. Nama pengguna akan menjadi Admin. Misalnya, **corp.example.com \admin** atau **corp\admin**.

7. Setelah Anda menerima pesan yang menyambut Anda ke domain, mulai ulang instans agar perubahan berlaku.

Sekarang instans Anda telah bergabung ke domain Direktori Aktif Microsoft AD AWS Terkelola, Anda dapat masuk ke instance tersebut dari jarak jauh dan menginstal utilitas untuk mengelola direktori, seperti menambahkan pengguna dan grup. Alat Administrasi Direktori Aktif dapat digunakan untuk membuat pengguna dan grup. Untuk informasi selengkapnya, lihat [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#).

 Note

Anda juga dapat menggunakan Amazon Route 53 untuk memproses kueri DNS alih-alih mengubah alamat DNS secara manual di instans Amazon EC2 Anda. Untuk informasi selengkapnya, lihat [Mengintegrasikan resolusi DNS Layanan Direktori Anda dengan Amazon Route 53 Resolver dan Meneruskan kueri DNS keluar ke jaringan](#) Anda.

Bergabung dengan instans Amazon EC2 Linux ke Direktori Aktif AWS Microsoft AD Terkelola

Anda dapat meluncurkan dan bergabung dengan instans EC2 Linux ke Microsoft AD yang AWS Dikelola di. Konsol Manajemen AWS Anda juga dapat menggabungkan instans EC2 Linux secara manual ke Microsoft AD yang AWS Dikelola. Alat seperti Winbind juga dapat digunakan sehingga Anda dapat bergabung dengan instans EC2 Linux ke AWS Microsoft AD yang Dikelola.

Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)

- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Server Perusahaan 15 SP1

 Note

Distribusi sebelum Ubuntu 14 dan Red Hat Enterprise Linux 7 dan 8 tidak mendukung fitur join domain yang mulus.

Cara domain bergabung dengan instans Linux EC2:

- [Menggabungkan instans Amazon EC2 Linux dengan mulus ke Direktori Aktif Microsoft AWS AD Terkelola](#)
- [Menggabungkan instans Amazon EC2 Linux dengan mulus ke Microsoft AD AWS Terkelola bersama](#)
- [Menggabungkan instans Amazon EC2 Linux secara manual ke Direktori Aktif AWS Microsoft AD Terkelola](#)
- [Menggabungkan instans Amazon EC2 Linux secara manual ke Direktori Aktif AWS Microsoft AD Terkelola menggunakan Winbind](#)

Menggabungkan instans Amazon EC2 Linux dengan mulus ke Direktori Aktif Microsoft AWS AD Terkelola

Prosedur ini menggabungkan instans Amazon EC2 Linux dengan mulus ke Direktori Aktif Microsoft AD AWS Terkelola Anda. Untuk menyelesaikan prosedur ini, Anda perlu membuat AWS Secrets Manager rahasia yang dapat menimbulkan biaya tambahan. Untuk informasi selengkapnya, silakan lihat [Harga AWS Secrets Manager](#).

Jika Anda perlu melakukan gabungan domain tanpa batas di beberapa AWS akun, Anda dapat memilih untuk mengaktifkan Berbagi [direktori](#).

Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0

- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Server Perusahaan 15 SP1

 Note

Distribusi sebelum Ubuntu 14 dan Red Hat Enterprise Linux 7 dan 8 tidak mendukung fitur join domain yang mulus.

Untuk demonstrasi tentang proses menggabungkan instans Linux dengan mulus ke Direktori Aktif AWS Microsoft AD Terkelola, lihat video berikut YouTube .

[Amazon EC2 untuk Linux domain AD mulus bergabung dengan demo](#)

Prasyarat

Sebelum Anda dapat mengatur gabungan domain tanpa batas ke instans Linux EC2, Anda harus menyelesaikan prosedur di bagian ini.

Prasyarat jaringan untuk bergabung dengan domain yang mulus

Agar domain bergabung dengan instans EC2 Linux dengan mulus, Anda harus menyelesaikan yang berikut ini:

- Anda akan memerlukan izin IAM berikut untuk bergabung dengan instans EC2 Linux dengan mulus:
 - Memiliki iklan Microsoft yang AWS Dikelola. Untuk mempelajari selengkapnya, lihat [Membuat Microsoft AD yang AWS Dikelola](#).
- Anda memerlukan izin IAM berikut untuk bergabung dengan instans EC2 dengan mulus: Windows
 - Profil Instans IAM dengan izin IAM berikut:
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess

- Domain pengguna yang bergabung dengan EC2 ke AWS Microsoft AD Terkelola memerlukan izin IAM berikut:
 - Directory Service Izin:
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Izin VPC Amazon:
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
 - Izin EC2:
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"
 - "ec2:RunInstances"
 - "ec2:CreateTags"
 - AWS Systems Manager Izin:
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"
- Saat iklan Microsoft AWS Terkelola dibuat, grup keamanan dibuat dengan aturan masuk dan keluar. Untuk mempelajari lebih lanjut tentang aturan dan port ini, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#). Untuk bergabung dengan instans EC2 Linux secara mulus, VPC tempat Anda meluncurkan instans harus mengizinkan port yang sama yang diizinkan dalam aturan masuk dan keluar grup keamanan AWS Microsoft AD Terkelola.
- Bergantung pada keamanan jaringan dan pengaturan firewall Anda, Anda mungkin diminta untuk mengizinkan lalu lintas keluar tambahan. Lalu lintas ini akan untuk HTTPS (port 443) ke titik akhir berikut:

Titik akhir	Peran
<code>ec2messages. <i>region</i>.amazonaws.com</code>	Membuat dan menghapus saluran sesi dengan layanan Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .
<code>ssm.<i>region</i>.amazonaws.com</code>	Titik akhir untuk AWS Systems Manager Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .
<code>ssmmessages. <i>region</i>.amazonaws.com</code>	Membuat dan menghapus saluran sesi dengan layanan Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .
<code>ds.<i>region</i>.amazonaws.com</code>	Titik akhir untuk Directory Service. Untuk informasi selengkapnya, lihat Ketersediaan wilayah untuk Directory Service .
<code>secretsmanager. <i>region</i>.amazonaws.com</code>	Titik akhir untuk AWS Secrets Manager. Untuk informasi lebih lanjut, lihat AWS Secrets Manager kuota dan titik akhir .

- Sebaiknya gunakan server DNS yang akan menyelesaikan nama domain Microsoft AD AWS Terkelola Anda. Untuk melakukannya, Anda dapat membuat set opsi DHCP. Untuk informasi selengkapnya, lihat [Membuat atau mengubah opsi DHCP yang disetel untuk Microsoft AD yang AWS Dikelola](#).
- Jika Anda memilih untuk tidak membuat set opsi DHCP, maka server DNS Anda akan statis dan dikonfigurasi oleh AWS Microsoft AD yang Dikelola.

Pilih akun layanan penggabungan domain mulus Anda

Anda dapat menggabungkan komputer Linux dengan mulus ke domain Direktori Aktif Microsoft AD yang AWS Dikelola. Untuk melakukannya, Anda harus membuat akun pengguna dengan membuat izin akun komputer untuk menggabungkan komputer ke domain. Meskipun anggota administrator

yang didelegasikan AWS atau grup lain mungkin memiliki hak istimewa yang memadai untuk menggabungkan komputer ke domain, kami tidak menyarankan untuk menggunakan ini. Sebagai praktik terbaik, kami rekomendasikan Anda menggunakan akun layanan yang memiliki hak istimewa minimum yang diperlukan untuk menggabungkan komputer ke domain.

Untuk mendelegasikan akun dengan hak istimewa minimum yang diperlukan untuk bergabung dengan komputer ke domain, Anda dapat menjalankan perintah berikut PowerShell. Anda harus menjalankan perintah ini dari komputer Windows menggabungkan domain dengan [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#) yang diinstal. Selain itu, Anda harus menggunakan akun yang memiliki izin untuk mengubah izin di OU komputer atau kontainer Anda. PowerShell Perintah menetapkan izin yang memungkinkan akun layanan untuk membuat objek komputer di wadah komputer default domain Anda.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
    'schemaNamingContext'
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
    -Filter { LDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
    $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
    in the Computers container.
$AddAccessRule = New-Object -TypeName
    'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
    'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Jika Anda lebih suka menggunakan antarmuka pengguna grafis (GUI) Anda dapat menggunakan proses manual yang dijelaskan di [Mendelegasikan hak istimewa ke akun layanan Anda](#).

Membuat rahasia untuk menyimpan akun layanan domain

Anda dapat menggunakan AWS Secrets Manager untuk menyimpan akun layanan domain. Untuk informasi selengkapnya, lihat [Membuat AWS Secrets Manager rahasia](#).

Note

Ada biaya yang terkait dengan Secrets Manager. Untuk informasi selengkapnya lihat, [Harga](#) di Panduan AWS Secrets Manager Pengguna.

Untuk Membuat rahasia dan menyimpan informasi akun layanan domain

1. Masuk ke Konsol Manajemen AWS dan buka AWS Secrets Manager konsol di <https://console.aws.amazon.com/secretsmanager/>.
2. Pilih Simpan rahasia baru.
3. Pada halaman Simpan rahasia baru, lakukan hal berikut:
 - a. Di bawah Tipe rahasia, pilih Jenis rahasia lainnya.
 - b. Di bawah pasangan kunci/nilai, lakukan hal berikut:
 - i. Dalam kotak pertama, masukkan **awsSeamlessDomainUsername**. Pada baris yang sama, di kotak berikutnya, masukkan nama pengguna untuk akun layanan Anda. Misalnya, jika Anda menggunakan PowerShell perintah sebelumnya, nama akun layanan akan menjadi **awsSeamlessDomain**.

Note

Anda harus memasukkan **awsSeamlessDomainUsername** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

The screenshot shows the AWS Secrets Manager console interface for creating a new secret. The breadcrumb trail is 'AWS Secrets Manager > Secrets > Store a new secret'. The left sidebar shows the steps: Step 1: Choose secret type, Step 2: Configure secret, Step 3 - optional: Configure rotation, and Step 4: Review. The main content area is titled 'Choose secret type'. Under 'Secret type', four options are listed: 'Credentials for Amazon RDS database', 'Credentials for Amazon DocumentDB database', 'Credentials for Amazon Redshift cluster', and 'Other type of secret' (which is selected and highlighted with a red box). Below this, the 'Key/value pairs' section has a table with two columns: 'Key/value' and 'Plaintext'. The first row has 'awsSeamlessDomainUsername' in the 'Key/value' column (highlighted with a red box) and an empty 'Plaintext' column. There is an '+ Add row' button below the table. The 'Encryption key' section shows a dropdown menu with 'aws/secretsmanager' selected and a refresh button. At the bottom right, there are 'Cancel' and 'Next' buttons.

- ii. Pilih Tambahkan baris.
- iii. Pada baris baru, di kotak pertama, masukkan **awsSeamlessDomainPassword**. Pada baris yang sama, di kotak berikutnya, masukkan kata sandi untuk akun layanan Anda.

Note

Anda harus memasukkan **awsSeamlessDomainPassword** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

- iv. Di bawah kunci Enkripsi, tinggalkan nilai default `aws/secretsmanager`. AWS Secrets Manager selalu mengenkripsi rahasia ketika Anda memilih opsi ini. Anda juga dapat memilih kunci yang Anda buat.
- v. Pilih Berikutnya.

4. Di bawah nama Rahasia, masukkan nama rahasia yang menyertakan ID direktori Anda menggunakan format berikut, ganti **d-xxxxxxxxxx** dengan ID direktori Anda:

```
aws/directory-services/d-xxxxxxxxxx/seamless-domain-join
```

Ini akan digunakan untuk mengambil rahasia dalam aplikasi.

 Note

Anda harus memasukkan **aws/directory-services/d-xxxxxxxxxx/seamless-domain-join** persis seperti itu tetapi ganti **d-xxxxxxxxxx** dengan ID direktori Anda. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

Configure secret

Secret name and description [Info](#)

Secret name
A descriptive name that helps you find your secret later.

Secret name must contain only alphanumeric characters and the characters `/_+:@-`.

Description - optional

Maximum 250 characters.

Tags - optional
No tags associated with the secret.

Resource permissions - optional [Info](#)
Add or edit a resource policy to access secrets across AWS accounts.

Replicate secret - optional
Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

5. Biarkan yang lainnya diatur ke default, dan kemudian pilih Selanjutnya.
6. Di bawah Konfigurasi rotasi otomatis, pilih Nonaktifkan rotasi otomatis, lalu pilih Selanjutnya.

Anda dapat mengaktifkan rotasi untuk rahasia ini setelah Anda menyimpannya.

7. Tinjau pengaturan, dan kemudian pilih Simpan untuk menyimpan perubahan Anda. Konsol Secrets Manager mengembalikan Anda ke daftar rahasia di akun Anda dengan rahasia baru Anda masuk di dalam daftar.
8. Pilih nama rahasia Anda yang baru dibuat dari daftar, dan perhatikan nilai ARN rahasia. Anda akan membutuhkannya di bagian selanjutnya.

Aktifkan rotasi untuk rahasia akun layanan domain

Kami menyarankan Anda memutar rahasia secara teratur untuk meningkatkan postur keamanan Anda.

Untuk mengaktifkan rotasi untuk rahasia akun layanan domain

- Ikuti petunjuk di [Mengatur rotasi otomatis untuk AWS Secrets Manager rahasia](#) di Panduan AWS Secrets Manager Pengguna.

Untuk Langkah 5, gunakan template rotasi [kredensial Microsoft Active Directory](#) di AWS Secrets Manager Panduan Pengguna.

Untuk bantuan, lihat [Memecahkan masalah AWS Secrets Manager rotasi](#) di AWS Secrets Manager Panduan Pengguna.

Untuk membuat kebijakan dan peran IAM yang diperlukan

Gunakan langkah-langkah prasyarat berikut untuk membuat kebijakan khusus yang memungkinkan akses hanya-baca ke rahasia gabungan domain tanpa batas Secrets Manager Anda (yang Anda buat sebelumnya), dan untuk membuat peran IAM Linux baru. EC2 DomainJoin

Membuat kebijakan membaca IAM Secrets Manager

Anda menggunakan konsol IAM untuk membuat kebijakan yang memberikan akses hanya-baca ke rahasia Secrets Manager Anda.

Untuk membuat kebijakan membaca IAM Secrets Manager

- Masuk ke pengguna Konsol Manajemen AWS sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Kemudian buka konsol IAM di <https://console.aws.amazon.com/iam/>.
- Di panel navigasi, Manajemen Akses, pilih Kebijakan.
- Pilih Buat kebijakan.
- Pilih tab JSON dan salin teks dari dokumen kebijakan JSON berikut. Kemudian tempelkan ke dalam kotak teks JSON.

Note

Pastikan Anda mengganti Region and Resource ARN dengan Region dan ARN sebenarnya dari rahasia yang Anda buat sebelumnya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-east-1:xxxxxxxx:secret:aws/directory-
services/d-xxxxxxxx/seamless-domain-join"
      ]
    }
  ]
}
```

5. Setelah selesai, pilih Selanjutnya. Validator kebijakan melaporkan kesalahan sintaksis. Untuk informasi selengkapnya, lihat [Memvalidasi kebijakan IAM](#).
6. Pada halaman Tinjau kebijakan, masukkan nama kebijakan, seperti **SM-Secret-Linux-DJ-d-xxxxxxxx-Read**. Tinjau bagian Ringkasan untuk melihat izin yang diberikan oleh kebijakan Anda. Lalu pilih Buat kebijakan untuk menyimpan perubahan Anda. Kebijakan baru muncul di daftar kebijakan terkelola dan siap dilampirkan pada identitas.

Note

Kami rekomendasikan Anda membuat satu kebijakan per rahasia. Melakukan hal tersebut memastikan bahwa instans hanya memiliki akses ke rahasia yang sesuai dan meminimalkan dampak jika sebuah instans dikompromikan.

Buat EC2 DomainJoin peran Linux

Anda menggunakan konsol IAM untuk membuat peran yang akan Anda gunakan untuk penggabungan domain dengan instans EC2 Linux Anda.

Untuk membuat EC2 DomainJoin peran Linux

1. Masuk ke pengguna Konsol Manajemen AWS sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Kemudian buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi, di bawah Manajemen Akses, pilih Peran.
3. Di panel konten, pilih Buat peran.
4. Di bawah Pilih jenis entitas terpercaya, pilih AWS layanan.
5. Di bawah Kasus penggunaan, pilih EC2, lalu pilih Berikutnya.

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected, which is highlighted with a red box. The 'EC2' use case description is: 'Allows EC2 instances to call AWS services on your behalf.' Below this, there is a list of other use cases, each with a description of the permissions it grants.

6. Untuk Kebijakan filter, lakukan hal berikut:

- a. Masukkan **AmazonSSMManagedInstanceCore**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.
- b. Masukkan **AmazonSSMDirectoryServiceAccess**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.
- c. Masukkan **SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read** (atau nama kebijakan yang Anda buat dalam prosedur sebelumnya). Lalu pilih kotak centang untuk item tersebut di dalam daftar.

- d. Setelah menambahkan tiga kebijakan yang tercantum di atas, pilih **Buat peran**.

 Note

Amazon SSMDirectory ServiceAccess menyediakan izin untuk menggabungkan instance ke Active Directory yang dikelola oleh Directory Service Amazon SSMManged InstanceCore memberikan izin minimum yang diperlukan untuk menggunakan AWS Systems Manager layanan ini. Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat [Buat profil instans IAM untuk Systems Manager](#) di Panduan Pengguna AWS Systems Manager .

7. Masukkan nama untuk peran baru Anda, seperti **LinuxEC2DomainJoin** atau nama lain yang Anda inginkan di bidang Nama peran.
8. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
9. (Opsional) Pilih Tambahkan tag baru di bawah Langkah 3: Tambahkan tag untuk menambahkan tag. Pasangan nilai kunci tag digunakan untuk mengatur, melacak, atau mengontrol akses untuk peran ini.
10. Pilih **Buat peran**.

Bergabunglah dengan instans Linux Anda dengan mulus

Untuk bergabung dengan instans Linux Anda dengan mulus

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Dari pemilih Region di bilah navigasi, pilih yang AWS Region sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Name and Tags, masukkan nama yang ingin Anda gunakan untuk instans Linux EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih AMI Linux yang ingin Anda luncurkan.

 Note

AMI yang digunakan harus memiliki AWS Systems Manager (Agen SSM) versi 2.3.1644.0 atau lebih tinggi. Untuk memeriksa versi SSM Agent yang diinstal di AMI Anda dengan meluncurkan sebuah instans dari AMI tersebut, lihat [Mendapatkan versi Agen SSM yang saat ini diinstal](#). Jika Anda perlu meningkatkan Agen SSM, lihat [Menginstal dan mengkonfigurasi SSM Agent pada instans EC2 untuk Linux](#).

SSM menggunakan `aws:domainJoin` plugin saat menggabungkan instance Linux ke domain Active Directory. Plugin mengubah nama host untuk instance Linux ke format EC2 AMAZ-`XXXXXXXX`. Untuk informasi selengkapnya `aws:domainJoin`, lihat [referensi plugin dokumen AWS Systems Manager perintah](#) di Panduan AWS Systems Manager Pengguna.

7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada. Untuk membuat key pair baru, pilih Create new key pair. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk. Pilih create key pair. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

 Important

Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat [Connect to the internet menggunakan gateway internet](#) di Panduan Pengguna Amazon VPC.

11. Di bawah Auto-assign IP publik, pilih Aktifkan.

Untuk informasi selengkapnya tentang pengalamatan IP publik dan pribadi, lihat pengalamatan [IP instans Amazon EC2](#) di Panduan Pengguna Amazon EC2.

12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

 Note

Setelah memilih direktori Gabung Domain, Anda mungkin melihat:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:

- Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
- Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, pilih peran IAM yang sebelumnya Anda buat di bagian prasyarat Langkah 2: Buat peran Linux. EC2 DomainJoin
16. Pilih Luncurkan instans.

 Note

Jika Anda menjalankan penggabungan domain yang mulus dengan SUSE Linux, reboot diperlukan sebelum autentikasi akan bekerja. Untuk me-reboot SUSE dari terminal Linux, ketik `sudo reboot`.

Menggabungkan instans Amazon EC2 Linux dengan mulus ke Microsoft AD AWS Terkelola bersama

Dalam prosedur ini, Anda akan dengan mulus menggabungkan instans Amazon EC2 Linux ke iklan Microsoft AWS Terkelola bersama. Untuk melakukan ini, Anda akan membuat kebijakan baca AWS Secrets Manager IAM dalam peran instans EC2 di akun tempat Anda ingin meluncurkan instans Linux EC2. Ini akan disebut seperti Account 2 dalam prosedur ini. Instans ini akan menggunakan iklan Microsoft AWS Terkelola yang sedang dibagikan dari akun lain yang disebut sebagai Account 1.

Prasyarat

Sebelum Anda dapat bergabung dengan instans Amazon EC2 Linux dengan mulus ke Microsoft AD AWS Dikelola bersama, Anda harus menyelesaikan yang berikut ini:

- Langkah 1 sampai 3 dalam tutorial, [Tutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus](#). Tutorial ini memandu Anda melalui pengaturan jaringan Anda dan berbagi iklan Microsoft AWS Terkelola Anda.
- Prosedur yang diuraikan dalam [Menggabungkan instans Amazon EC2 Linux dengan mulus ke Direktori Aktif Microsoft AWS AD Terkelola](#).

Langkah 1. Buat EC2 DomainJoin peran Linux di Akun 2

Pada langkah ini, Anda akan menggunakan konsol IAM untuk membuat peran IAM yang akan Anda gunakan untuk domain bergabung dengan instans Linux EC2 Anda saat masuk. Account 2

Buat EC2 DomainJoin peran Linux

- Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
- Di panel navigasi kiri, di bawah Manajemen Akses, pilih Peran.
- Pada halaman Peran, pilih Buat peran.

4. Di bawah Pilih jenis entitas terpercaya, pilih AWS layanan.
5. Di bawah Kasus penggunaan, pilih EC2, lalu pilih Berikutnya
6. Untuk Kebijakan filter, lakukan hal berikut:
 - a. Masukkan AmazonSSMManagedInstanceCore. Kemudian pilih kotak centang untuk item itu dalam daftar.
 - b. Masukkan AmazonSSMDirectoryServiceAccess. Kemudian pilih kotak centang untuk item itu dalam daftar.
 - c. Setelah menambahkan kebijakan ini, pilih Buat peran.

 Note

AmazonSSMDirectoryServiceAccess memberikan izin untuk menggabungkan instance ke Active Directory yang dikelola oleh. Directory ServiceAmazonSSMManagedInstanceCore memberikan izin minimum yang diperlukan untuk digunakan AWS Systems Manager. Untuk informasi selengkapnya tentang membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke peran IAM, lihat [Mengonfigurasi izin instans yang diperlukan untuk Systems Manager](#) di Panduan Pengguna.AWS Systems Manager

7. Masukkan nama untuk peran baru Anda, seperti LinuxEC2DomainJoin atau nama lain yang Anda inginkan di bidang Nama peran.
8. (Opsional) Untuk deskripsi Peran, masukkan deskripsi.
9. (Opsional) Pilih Tambahkan tag baru di bawah Langkah 3: Tambahkan tag untuk menambahkan tag. Pasangan nilai kunci tag digunakan untuk mengatur, melacak, atau mengontrol akses untuk peran ini.
10. Pilih Buat peran.

Langkah 2. Buat akses sumber daya lintas akun untuk berbagi AWS Secrets Manager rahasia

Bagian selanjutnya adalah persyaratan tambahan yang harus dipenuhi untuk bergabung dengan instans EC2 Linux dengan AWS Microsoft AD yang Dikelola bersama. Persyaratan ini termasuk membuat kebijakan sumber daya dan melampirkannya ke layanan dan sumber daya yang sesuai.

Untuk memungkinkan pengguna di akun mengakses AWS Secrets Manager rahasia di akun lain, Anda harus mengizinkan akses dalam kebijakan sumber daya dan kebijakan identitas. Jenis akses ini disebut [akses sumber daya lintas akun](#).

Jenis akses ini berbeda dengan memberikan akses ke identitas di akun yang sama dengan rahasia Secrets Manager. Anda juga harus mengizinkan kunci identitas untuk menggunakan [AWS Key Management Service](#) (KMS) yang rahasianya dienkripsi. Izin ini diperlukan karena Anda tidak dapat menggunakan kunci AWS terkelola (`aws/secretsmanager`) untuk akses lintas akun. Sebagai gantinya, Anda akan mengenkripsi rahasia Anda dengan kunci KMS yang Anda buat, dan kemudian melampirkan kebijakan kunci ke dalamnya. Untuk mengubah kunci enkripsi untuk rahasia, lihat [Memodifikasi AWS Secrets Manager rahasia](#).

 Note

Ada biaya yang terkait AWS Secrets Manager, tergantung pada rahasia yang Anda gunakan. Untuk daftar harga lengkap saat ini, lihat [AWS Secrets Manager Harga](#). Anda dapat menggunakan Secrets Manager Kunci yang dikelola AWS `aws/secretsmanager` yang dibuat untuk mengenkripsi rahasia Anda secara gratis. Jika Anda membuat kunci KMS Anda sendiri untuk mengenkripsi rahasia Anda, AWS menagih Anda dengan tarif AWS KMS saat ini. Untuk informasi selengkapnya, silakan lihat [Harga AWS Key Management Service](#).

Langkah-langkah berikut memungkinkan Anda membuat kebijakan sumber daya agar pengguna dapat menggabungkan instans Linux EC2 dengan mulus ke AWS Microsoft AD Terkelola bersama.

Lampirkan kebijakan sumber daya ke rahasia di Akun 1

1. Buka konsol Secrets Manager di <https://console.aws.amazon.com/secretsmanager/>.
2. Dari daftar rahasia, pilih Rahasia yang Anda buat selama [Prasyarat](#).
3. Pada halaman detail Rahasia di bawah tab Ikhtisar, gulir ke bawah ke Izin sumber daya.
4. Pilih Edit izin.
 - Di bidang kebijakan, masukkan kebijakan berikut. Kebijakan berikut memungkinkan Linux EC2 DomainJoin Account 2 untuk mengakses rahasia di Account 1. [Ganti nilai ARN dengan nilai ARN untuk LinuxEC2DomainJoin peran Anda yang Anda Account 2 buat di Langkah 1](#). Untuk menggunakan kebijakan ini, lihat [Melampirkan kebijakan izin ke AWS Secrets Manager rahasia](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/LinuxEC2DomainJoin"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

Tambahkan pernyataan ke kebijakan kunci untuk kunci KMS di Akun 1

1. Buka konsol Secrets Manager di <https://console.aws.amazon.com/secretsmanager/>.
2. Di panel navigasi kiri, pilih Kunci terkelola pelanggan.
3. Pada halaman Customer managed keys, pilih kunci yang Anda buat.
4. Pada halaman Detail Utama, navigasikan ke Kebijakan kunci, lalu pilih Edit.
5. Pernyataan kebijakan kunci berikut memungkinkan ApplicationRole Account 2 untuk menggunakan kunci KMS Account 1 untuk mendekripsi rahasia di Account 1. Untuk menggunakan pernyataan ini, tambahkan ke kebijakan kunci untuk kunci KMS Anda. Untuk informasi selengkapnya, lihat [Mengubah kebijakan utama](#).

```
{
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::Account2:role/ApplicationRole"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
}
```



```
"Resource": "*"
}
```

Membuat kebijakan identitas untuk identitas di Akun 2

1. Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi kiri, di bawah Manajemen akses, pilih Kebijakan.
3. Pilih Buat Kebijakan. Pilih JSON di editor Kebijakan.
4. Kebijakan berikut memungkinkan ApplicationRole masuk Account 2 untuk mengakses rahasia Account 1 dan mendekripsi nilai rahasia dengan menggunakan kunci enkripsi yang juga ada di Account 1. Anda dapat menemukan ARN untuk rahasia Anda di konsol Secrets Manager di halaman Detail Rahasia di bawah Rahasia ARN. Atau, Anda dapat memanggil [deskripsi-rahasia](#) untuk mengidentifikasi ARN rahasia. Ganti ARN Sumber Daya dengan ARN Sumber Daya untuk ARN rahasia dan Account 1. Untuk menggunakan kebijakan ini, lihat [Melampirkan kebijakan izin ke AWS Secrets Manager rahasia](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:us-east-1:111122223333:secret:secretName-AbCdEf"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Describekey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/Your_Encryption_Key"
    }
  ]
}
```

5. Pilih Berikutnya dan kemudian pilih Simpan perubahan.
6. Temukan dan pilih Peran yang Anda buat [Attach a resource policy to the secret in Account 1](#).
Account 2
7. Di bawah Tambahkan izin, pilih Lampirkan kebijakan.
8. Di bilah pencarian, temukan kebijakan yang Anda buat [Add a statement to the key policy for the KMS key in Account 1](#) dan pilih kotak untuk menambahkan kebijakan ke peran. Kemudian pilih Tambahkan izin.

Langkah 3. Bergabunglah dengan instans Linux Anda dengan mulus

Sekarang Anda dapat menggunakan prosedur berikut untuk menggabungkan instans Linux EC2 Anda dengan mulus ke AWS Microsoft AD Terkelola bersama Anda.

Untuk bergabung dengan instans Linux Anda dengan mulus

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Dari pemilih Region di bilah navigasi, pilih yang AWS Region sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Name and Tags, masukkan nama yang ingin Anda gunakan untuk instans Linux EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih AMI Linux yang ingin Anda luncurkan.

Note

AMI yang digunakan harus memiliki AWS Systems Manager (Agen SSM) versi 2.3.1644.0 atau lebih tinggi. Untuk memeriksa versi SSM Agent yang diinstal di AMI Anda dengan meluncurkan sebuah instans dari AMI tersebut, lihat [Mendapatkan versi Agen SSM yang saat ini diinstal](#). Jika Anda perlu meningkatkan Agen SSM, lihat [Menginstal dan mengkonfigurasi SSM Agent pada instans EC2 untuk Linux](#). SSM menggunakan `aws:domainJoin` plugin saat menggabungkan instance Linux ke domain Active Directory. Plugin mengubah nama host untuk instance Linux ke format EC2 AMAZ-**XXXXXXX** Untuk informasi selengkapnya `aws:domainJoin`, lihat [referensi](#)

[plugin dokumen AWS Systems Manager perintah](#) di Panduan AWS Systems Manager Pengguna.

7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada. Untuk membuat key pair baru, pilih Create new key pair. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk. Pilih create key pair. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

 Important

Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat [Connect to the internet menggunakan gateway internet](#) di Panduan Pengguna Amazon VPC.

11. Di bawah Auto-assign IP publik, pilih Aktifkan.

Untuk informasi selengkapnya tentang pengalamatan IP publik dan pribadi, lihat pengalamatan [IP instans Amazon EC2](#) di Panduan Pengguna Amazon EC2.

12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

 Note

Setelah memilih direktori Gabung Domain, Anda mungkin melihat:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:

- Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
- Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, pilih peran IAM yang sebelumnya Anda buat di bagian prasyarat Langkah 2: Buat peran Linux. EC2 DomainJoin
16. Pilih Luncurkan instans.

 Note

Jika Anda menjalankan penggabungan domain yang mulus dengan SUSE Linux, reboot diperlukan sebelum autentikasi akan bekerja. Untuk me-reboot SUSE dari terminal Linux, ketik `sudo reboot`.

Menggabungkan instans Amazon EC2 Linux secara manual ke Direktori Aktif AWS Microsoft AD Terkelola

Selain instans Amazon EC2, Anda juga dapat menggabungkan Windows instans Amazon EC2 Linux tertentu ke Direktori Aktif Microsoft AD AWS Terkelola. Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Server Perusahaan 15 SP1

 Note

Distribusi dan versi Linux lainnya mungkin bekerja namun belum diuji.

Bergabunglah dengan instans Linux ke Microsoft AD yang AWS Dikelola

Sebelum Anda dapat menggabungkan instans Amazon Linux, CentOS, Red Hat, atau Ubuntu ke direktori Anda, instans harus terlebih dahulu diluncurkan sebagaimana ditentukan dalam [Bergabunglah dengan instans Linux Anda dengan mulus](#).

 Important

Beberapa prosedur berikut, jika tidak dilakukan dengan benar, dapat membuat instans anda tidak terjangkau atau tidak dapat digunakan. Oleh karena itu, kami sangat menyarankan Anda membuat backup atau mengambil snapshot dari instans Anda sebelum melakukan prosedur ini.

Untuk menggabungkan instance Linux ke direktori Anda

Ikuti langkah-langkah untuk instans Linux tertentu Anda menggunakan salah satu tab berikut:

Amazon Linux

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasi instance Linux untuk menggunakan alamat IP server DNS dari server DNS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set

Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat](#) dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.

3. Pastikan instans Amazon Linux - 64bit Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Amazon Linux yang diperlukan pada instans Linux Anda.

Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli  
krb5-workstation
```

Note

Untuk bantuan dalam menentukan versi Amazon Linux yang Anda gunakan, lihat [Mengidentifikasi image Amazon Linux](#) dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...  
* Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

- a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

7. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan hal berikut ini ke bagian bawah file sudoers dan simpan.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "`\<space>`" untuk membuat karakter spasi Linux.)

CentOS

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasi instance Linux untuk menggunakan alamat IP server DNS dari server DNS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat](#) dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans CentOS 7 Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket CentOS 7 yang diperlukan pada instans Linux Anda.

Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.


```
...  
* Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

- a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

7. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file `sudoers` dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "`\<space>`" untuk membuat karakter spasi Linux.)

Red Hat

1. Terhubung ke instans menggunakan klien SSH apa saja.

2. Konfigurasi instance Linux untuk menggunakan alamat IP server DNS dari server DNS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat](#) dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Red Hat - 64bit adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Red Hat yang diperlukan pada instans Linux Anda.

 Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -v -U join_account example.com --install=/  
join_account
```

join_account

AMAccountName s untuk akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...  
* Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

- a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

7. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file `sudoers` dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "`\<space>`" untuk membuat karakter spasi Linux.)

SUSE

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Mengkonfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS yang disediakan Directory Service. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans.

Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 pribadi](#) di AWS Pusat Pengetahuan untuk panduan tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.

3. Pastikan instans SUSE Linux 15 Anda adalah yang terbaru.
 - a. Hubungkan repositori paket.

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

- b. Pembaruan SUSE.

```
sudo zypper update -y
```

4. Instal paket SUSE Linux 15 yang diperlukan pada instans Linux Anda.

Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account example.com --verbose
```

join_account

AMAccountNama s di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...  
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

Perhatikan bahwa kedua pengembalian berikut diharapkan.

```
! Couldn't authenticate with keytab while discovering which salt to use:  
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. Mengaktifkan SSSD di PAM secara manual.

```
sudo pam-config --add --sss
```

7. Edit nsswitch.conf untuk mengaktifkan SSSD di nsswitch.conf

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss  
group:  compat sss  
shadow: compat sss
```

8. Tambahkan baris berikut ke/etc/pam.d/common-session untuk membuat direktori home secara otomatis saat login awal

```
sudo vi /etc/pam.d/common-session
```

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

9. Reboot instans untuk menyelesaikan proses penggabungan domain.

```
sudo reboot
```

10. Hubungkan kembali ke instans menggunakan klien SSH untuk memverifikasi bergabung domain telah berhasil diselesaikan dan menyelesaikan langkah-langkah tambahan.

a. Untuk mengkonfirmasi instans telah didaftarkan pada domain

```
sudo realm list
```

```
example.com
```

```
type: kerberos
realm-name: EXAMPLE.COM
domain-name: example.com
configured: kerberos-member
server-software: active-directory
client-software: sssd
required-package: sssd-tools
required-package: sssd
required-package: adcli
required-package: samba-client
login-formats: %U@example.com
login-policy: allow-realm-logins
```

b. Untuk memverifikasi status daemon SSSD

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
  Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor
  preset: disabled)
  Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
  Main PID: 479 (sssd)
  Tasks: 4
  CGroup: /system.slice/sss.service
          ##479 /usr/sbin/sss -i --logger=files
          ##505 /usr/lib/sss/sss_be --domain example.com --uid 0 --gid 0 --
  logger=files
          ##548 /usr/lib/sss/sss_nss --uid 0 --gid 0 --logger=files
          ##549 /usr/lib/sss/sss_pam --uid 0 --gid 0 --logger=files
```

11. Untuk mengizinkan akses pengguna melalui SSH dan konsol

```
sudo realm permit join_account@example.com
```

Untuk mengizinkan akses grup domain melalui SSH dan konsol

```
sudo realm permit -g 'AWS Delegated Administrators'
```

Atau untuk mengizinkan semua pengguna mengakses

```
sudo realm permit --all
```

12. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

- a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

13. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan hal berikut ini ke bagian bawah file sudoers dan simpan.

```
## Add the "Domain Admins" group from the awsad.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasi instance Linux untuk menggunakan alamat IP server DNS dari server DNS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS](#)

[statis ke instans Amazon EC2 privat](#) dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.

3. Pastikan instans Ubuntu - 64bit Anda adalah yang terbaru.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Instal paket Ubuntu yang diperlukan pada instans Linux Anda.

Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Nonaktifkan resolusi Reverse DNS dan atur ranah default ke FQDN domain Anda. Instans Ubuntu harus dapat dipecahkan terbalik di DNS sebelum ranah akan bekerja. Jika tidak, Anda harus menonaktifkan DNS terbalik di `/etc/krb5.conf` sebagai berikut:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

AMAccountNama s untuk akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...  
* Successfully enrolled machine in realm
```

7. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

- a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

8. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file `sudoers` dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "`\<space>`" untuk membuat karakter spasi Linux.)

Membatasi akses login akun

Karena semua akun ditetapkan dalam Direktori Aktif, secara default, semua pengguna dalam direktori tersebut dapat masuk ke instans. Anda dapat mengizinkan hanya pengguna tertentu untuk masuk ke instans dengan `ad_access_filter` di `sssd.conf`. Contoh:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Menunjukkan bahwa pengguna hanya boleh diizinkan akses ke instans jika mereka adalah anggota dari grup tertentu.

cn

Nama umum grup yang harus memiliki akses. Dalam contoh ini, nama grup adalah *admins*.

ou

Ini adalah unit organisasi tempat grup di atas berada. Dalam contoh ini, OU adalah *Testou*.

dc

Ini adalah komponen domain dari domain Anda. Dalam contoh ini, *example*.

dc

Ini adalah komponen domain tambahan. Dalam contoh ini, *com*.

Anda harus menambahkan `ad_access_filter` secara manual ke `/etc/sssd/sssd.conf`.

Buka file `/etc/sssd/sssd.conf` di editor teks.

```
sudo vi /etc/sssd/sssd.conf
```

Setelah melakukan hal ini, `sssd.conf` Anda mungkin terlihat seperti ini:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam
```

```
[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Agar konfigurasi mulai berlaku, Anda perlu memulai ulang layanan sssd:

```
sudo systemctl restart sssd.service
```

Atau, Anda dapat menggunakan .

```
sudo service sssd restart
```

Karena semua akun ditetapkan dalam Direktori Aktif, secara default, semua pengguna dalam direktori tersebut dapat masuk ke instans. Anda dapat mengizinkan hanya pengguna tertentu untuk masuk ke instans dengan `ad_access_filter` di `sssd.conf`.

Contoh:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Menunjukkan bahwa pengguna hanya boleh diizinkan akses ke instans jika mereka adalah anggota dari grup tertentu.

cn

Nama umum grup yang harus memiliki akses. Dalam contoh ini, nama grup adalah *admins*.

ou

Ini adalah unit organisasi tempat grup di atas berada. Dalam contoh ini, OU adalah *Testou*.

dc

Ini adalah komponen domain dari domain Anda. Dalam contoh ini, *example*.

dc

Ini adalah komponen domain tambahan. Dalam contoh ini, *com*.

Anda harus menambahkan `ad_access_filter` secara manual ke `/etc/sss/sssd.conf`.

1. Buka file `/etc/sss/sssd.conf` di editor teks.

```
sudo vi /etc/sss/sssd.conf
```

2. Setelah melakukan hal ini, `sssd.conf` Anda mungkin terlihat seperti ini:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

3. Agar konfigurasi mulai berlaku, Anda perlu memulai ulang layanan `sssd`:

```
sudo systemctl restart sssd.service
```

Atau, Anda dapat menggunakan .

```
sudo service sssd restart
```

Pemetaan ID

Pemetaan ID dapat dilakukan dengan dua metode untuk mempertahankan pengalaman terpadu antara UNIX/Linux User Identifier (UID) dan Group Identifier (GID) dan identitas Windows dan Active Directory Security Identifier (SID). Metode-metode ini adalah:

1. Tersentralisasi
2. Didistribusikan

Note

Pemetaan identitas pengguna terpusat di Active Directory memerlukan Antarmuka Sistem Operasi Portabel atau POSIX.

Pemetaan identitas pengguna terpusat

Active Directory atau layanan Lightweight Directory Access Protocol (LDAP) lainnya menyediakan UID dan GID kepada pengguna Linux. Di Active Directory, pengidentifikasi ini disimpan dalam atribut pengguna jika ekstensi POSIX dikonfigurasi:

- UID - Nama pengguna Linux (String)
- Nomor UID - Nomor ID Pengguna Linux (Integer)
- Nomor GID - Nomor ID Grup Linux (Integer)

Untuk mengkonfigurasi instance Linux untuk menggunakan UID dan GID dari Active Directory, atur `ldap_id_mapping = False` dalam file `sssd.conf`. Sebelum menyetel nilai ini, verifikasi bahwa Anda telah menambahkan UID, nomor UID, dan nomor GID ke pengguna dan grup di Active Directory.

Pemetaan identitas pengguna terdistribusi

Jika Active Directory tidak memiliki ekstensi POSIX atau jika Anda memilih untuk tidak mengelola pemetaan identitas secara terpusat, Linux dapat menghitung nilai UID dan GID. Linux menggunakan Security Identifier (SID) unik pengguna untuk menjaga konsistensi.

Untuk mengonfigurasi pemetaan ID pengguna terdistribusi, atur `ldap_id_mapping = True` dalam file `sssd.conf`.

Masalah umum

Jika Anda mengatur `ldap_id_mapping = False`, terkadang memulai layanan SSSD akan gagal. Alasan kegagalan ini adalah karena perubahan UIDs tidak didukung. Kami menyarankan Anda menghapus cache SSSD setiap kali Anda mengubah dari pemetaan ID ke atribut POSIX atau dari atribut POSIX ke pemetaan ID. Untuk detail lebih lanjut tentang pemetaan ID dan parameter `ldap_id_mapping`, lihat halaman manual `sssd-ldap` (8) di baris perintah Linux.

Connect ke instance Linux

Ketika pengguna terhubung ke instance menggunakan klien SSH, mereka diminta untuk nama pengguna mereka. Pengguna dapat memasukkan nama pengguna dalam `EXAMPLE\username` format `username@example.com` atau. Respons akan muncul mirip dengan yang berikut ini, tergantung pada distribusi Linux yang Anda gunakan:

Amazon Linux, Red Hat Enterprise Linux, dan CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

```
As "root" (sudo or sudo -i) use the:
```

- zypper command for package management
- yast command for configuration management

```
Management and Config: https://www.suse.com/suse-in-the-cloud-basics
```

```
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation: https://help.ubuntu.com
```

```
* Management:      https://landscape.canonical.com
* Support:          https://ubuntu.com/advantage
```

```
System information as of Sat Apr 18 22:03:35 UTC 2020
```

```
System load:  0.01          Processes:            102
Usage of /:    18.6% of 7.69GB Users logged in:        2
Memory usage: 16%          IP address for eth0: 10.24.34.1
Swap usage:   0%
```

Menggabungkan instans Amazon EC2 Linux secara manual ke Direktori Aktif AWS Microsoft AD Terkelola menggunakan Winbind

Anda dapat menggunakan layanan Winbind untuk menggabungkan instans Amazon EC2 Linux secara manual ke domain Direktori Aktif Microsoft AD AWS Terkelola. Ini memungkinkan pengguna Active Directory lokal Anda yang ada untuk menggunakan kredensial Active Directory mereka saat mengakses instance Linux yang bergabung dengan Direktori Aktif AWS Microsoft AD Terkelola Anda. Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Server Perusahaan 15 SP1

Note

Distribusi dan versi Linux lainnya mungkin bekerja namun belum diuji.

Bergabunglah dengan instans Linux ke Direktori Aktif Microsoft AD AWS Terkelola

Important

Beberapa prosedur berikut, jika tidak dilakukan dengan benar, dapat membuat instans anda tidak terjangkau atau tidak dapat digunakan. Oleh karena itu, kami sangat menyarankan

Anda membuat backup atau mengambil snapshot dari instans Anda sebelum melakukan prosedur ini.

Untuk menggabungkan instance Linux ke direktori Anda

Ikuti langkah-langkah untuk instans Linux tertentu Anda menggunakan salah satu tab berikut:

Amazon Linux/CENTOS/REDHAT

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Mengkonfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS yang disediakan Directory Service. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 pribadi](#) di AWS Pusat Pengetahuan untuk panduan tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Linux Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Samba / Winbind yang diperlukan pada instans Linux Anda.

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-clients
```

5. Buat backup dari file `smb.conf` utama sehingga Anda dapat kembali ke sana jika terjadi kegagalan:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Buka file konfigurasi `[/etc/samba/smb.conf]` asli di editor teks.

```
sudo vim /etc/samba/smb.conf
```

Isi informasi lingkungan domain Active Directory Anda seperti yang ditunjukkan pada contoh di bawah ini:


```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. Buka file host [/etc/hosts] di editor teks.

```
sudo vim /etc/hosts
```

Tambahkan alamat IP privat instans Linux Anda sebagai berikut:

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

 Note

Jika Anda tidak menentukan alamat IP Anda di file /etc/hosts, Anda mungkin menerima error DNS berikut saat menggabungkan instans ke domain.:

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

Error ini berarti bahwa penggabungan berhasil tetapi perintah [net ads] tidak dapat mendaftarkan catatan DNS di DNS.

8. Menggabungkan instans Linux ke Direktori Aktif menggunakan utilitas net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan

hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Memodifikasi file konfigurasi PAM, Gunakan perintah di bawah ini untuk menambahkan entri yang diperlukan untuk autentikasi winbind:

```
sudo authconfig --enablewinbind --enablewinbindauth --enablemkhomedir --update
```

10. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi dengan mengedit file `/etc/ssh/sshd_config`.

- a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

11. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH dan tambahkan hak istimewa root untuk pengguna atau grup domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan grup atau pengguna yang diperlukan dari domain Trusting atau Trusted sebagai berikut, dan kemudian simpan.

```
## Adding Domain Users/Groups.  
%domainname\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL  
%domainname\groupname ALL=(ALL:ALL) ALL  
domainname\username ALL=(ALL:ALL) ALL  
%Trusted_DomainName\groupname ALL=(ALL:ALL) ALL  
Trusted_DomainName\username ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "<space>" untuk membuat karakter spasi Linux.)

SUSE

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Mengkonfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS yang disediakan Directory Service. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 pribadi](#) di AWS Pusat Pengetahuan untuk panduan tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans SUSE Linux 15 Anda adalah yang terbaru.
 - a. Hubungkan repositori paket.

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

- b. Pembaruan SUSE.

```
sudo zypper update -y
```

4. Instal paket Samba / Winbind yang diperlukan pada instans Linux Anda.

```
sudo zypper in -y samba samba-winbind
```

5. Buat backup dari file `smb.conf` utama sehingga Anda dapat kembali ke sana jika terjadi kegagalan:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Buka file konfigurasi [/etc/samba/smb.conf] asli di editor teks.

```
sudo vim /etc/samba/smb.conf
```

Isi informasi lingkungan domain direktori Aktif Anda seperti yang ditunjukkan pada contoh di bawah ini:

```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. Buka file host [/etc/hosts] di editor teks.

```
sudo vim /etc/hosts
```

Tambahkan alamat IP privat instans Linux Anda sebagai berikut:

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

 Note

Jika Anda tidak menentukan alamat IP Anda di file /etc/hosts, Anda mungkin menerima error DNS berikut saat menggabungkan instans ke domain.:

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

Error ini berarti bahwa penggabungan berhasil tetapi perintah [net ads] tidak dapat mendaftarkan catatan DNS di DNS.

8. Menggabungkan instans Linux ke direktori dengan perintah berikut.

```
sudo net ads join -U join_account@example.com
```

join_account

AMAccountNama s di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
Enter join_account@example.com's password:  
Using short domain name -- example  
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Memodifikasi file konfigurasi PAM, Gunakan perintah di bawah ini untuk menambahkan entri yang diperlukan untuk autentikasi Winbind:

```
sudo pam-config --add --winbind --mkhomedir
```

10Buka file konfigurasi Name Service Switch [/etc/nsswitch.conf] di editor teks.

```
vim /etc/nsswitch.conf
```

Tambahkan direktif Winbind seperti yang ditunjukkan di bawah ini.

```
passwd: files winbind  
shadow: files winbind  
group: files winbind
```

11Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi dengan mengedit file /etc/ssh/sshd_config.

a. Buka file /etc/ssh/sshd_config di editor teks.

```
sudo vim /etc/ssh/sshd_config
```

- b. Atur pengaturan PasswordAuthentication ke yes.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

12. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH dan tambahkan hak istimewa root untuk pengguna atau grup domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan grup atau pengguna yang diperlukan dari domain Trusting atau Trusted sebagai berikut, dan kemudian simpan.

```
## Adding Domain Users/Groups.  
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL  
%domainname\\groupname ALL=(ALL:ALL) ALL  
domainname\\username ALL=(ALL:ALL) ALL  
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL  
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "<space>" untuk membuat karakter spasi Linux.)

Ubuntu

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Mengkonfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS yang disediakan Directory Service. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans.

Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 pribadi](#) di AWS Pusat Pengetahuan untuk panduan tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.

3. Pastikan instans Linux Anda adalah yang terbaru.

```
sudo apt-get -y upgrade
```

4. Instal paket Samba / Winbind yang diperlukan pada instans Linux Anda.

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. Buat backup dari file `smb.conf` utama sehingga Anda dapat kembali ke sana jika terjadi kegagalan.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Buka file konfigurasi `[/etc/samba/smb.conf]` asli di editor teks.

```
sudo vim /etc/samba/smb.conf
```

Isi informasi lingkungan domain direktori Aktif Anda seperti yang ditunjukkan pada contoh di bawah ini:

```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. Buka file `host` `[/etc/hosts]` di editor teks.

```
sudo vim /etc/hosts
```

Tambahkan alamat IP privat instans Linux Anda sebagai berikut:

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

 Note

Jika Anda tidak menentukan alamat IP Anda di file `/etc/hosts`, Anda mungkin menerima error DNS berikut saat menggabungkan instans ke domain.:

```
No DNS domain configured for linux-instance. Unable to perform  
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

Error ini berarti bahwa penggabungan berhasil tetapi perintah `[net ads]` tidak dapat mendaftarkan catatan DNS di DNS.

8. Menggabungkan instans Linux ke Direktori Aktif menggunakan utilitas `net`.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
Enter join_account@example.com's password:  
Using short domain name -- example  
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Memodifikasi file konfigurasi PAM, Gunakan perintah di bawah ini untuk menambahkan entri yang diperlukan untuk autentikasi Winbind:

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. Buka file konfigurasi Name Service Switch [`/etc/nsswitch.conf`] di editor teks.


```
vim /etc/nsswitch.conf
```

Tambahkan direktif Winbind seperti yang ditunjukkan di bawah ini.

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi dengan mengedit file `/etc/ssh/sshd_config`.

a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vim /etc/ssh/sshd_config
```

b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

12. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH dan tambahkan hak istimewa root untuk pengguna atau grup domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

b. Tambahkan grup atau pengguna yang diperlukan dari domain Trusting atau Trusted sebagai berikut, dan kemudian simpan.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
```

```
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "<space>" untuk membuat karakter spasi Linux.)

Connect ke instance Linux

Ketika pengguna terhubung ke instance menggunakan klien SSH, mereka diminta untuk nama pengguna mereka. Pengguna dapat memasukkan nama pengguna dalam EXAMPLE\username format username@example.com atau. Respons akan muncul mirip dengan yang berikut ini, tergantung pada distribusi Linux yang Anda gunakan:

Amazon Linux, Red Hat Enterprise Linux, dan CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

```
As "root" (sudo or sudo -i) use the:
```

- zypper command for package management
- yast command for configuration management

```
Management and Config: https://www.suse.com/suse-in-the-cloud-basics
```

```
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)
```

```
* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage
```

```
System information as of Sat Apr 18 22:03:35 UTC 2020
```

```
System load: 0.01          Processes:            102
Usage of /:  18.6% of 7.69GB Users logged in:       2
Memory usage: 16%          IP address for eth0: 10.24.34.1
Swap usage:  0%
```

Bergabung dengan instans Amazon EC2 Mac ke Direktori Aktif AWS Microsoft AD Terkelola

Prosedur ini secara manual menggabungkan instans Amazon EC2 Mac ke Direktori Aktif Microsoft AD AWS Terkelola Anda.

Prasyarat

- Instans Amazon EC2 Mac memerlukan Host Khusus [Amazon](#) EC2. Anda harus mengalokasikan host khusus dan meluncurkan instance ke host. Untuk informasi selengkapnya, lihat [Meluncurkan instance Mac](#) di Panduan Pengguna Amazon EC2.
- Sebaiknya buat pilihan DHCP yang ditetapkan untuk Direktori Aktif Microsoft AD AWS Terkelola Anda. Ini akan memungkinkan instance apa pun di VPC Amazon Anda mengarah ke domain dan server DNS yang ditentukan untuk menyelesaikan nama domain mereka. Untuk informasi selengkapnya, lihat [Membuat atau mengubah opsi DHCP yang disetel untuk Microsoft AD yang AWS Dikelola](#).

Note

Harga Dedicated Host bervariasi menurut opsi pembayaran yang Anda pilih. Untuk informasi selengkapnya, lihat [Harga dan Penagihan](#) di Panduan Pengguna Amazon EC2.

Menggabungkan instance Mac secara manual

1. Gunakan perintah SSH berikut untuk terhubung ke instance Mac Anda. Untuk informasi selengkapnya tentang menghubungkan ke instans Mac, lihat [Connect ke instance Mac Anda](#).

```
ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
```

- Setelah Anda terhubung ke instance Mac Anda, buat kata sandi untuk *ec2-user* akun menggunakan perintah berikut:

```
sudo passwd ec2-user
```

- Saat diminta di baris perintah, berikan kata sandi untuk *ec2-user* akun tersebut. Anda dapat memperbarui sistem operasi dan perangkat lunak Anda dengan mengikuti prosedur di [Perbarui sistem operasi dan perangkat lunak](#) di Panduan Pengguna Amazon EC2.
- Gunakan *dsconfigad* perintah berikut untuk menggabungkan instance Mac Anda ke domain Direktori Aktif Microsoft AD AWS Terkelola. Pastikan untuk mengganti nama domain, nama komputer, dan unit organisasi dengan informasi domain Microsoft AD Active Directory AWS Terkelola. Untuk informasi selengkapnya, lihat [Mengonfigurasi akses domain di Utilitas Direktori di Mac](#) di situs web Apple.

Warning

Nama komputer seharusnya tidak mengandung tanda hubung. Tanda hubung dapat mencegah pengikatan ke Direktori Aktif AWS Microsoft AD yang Dikelola.

```
sudo dsconfigad -add domainName -computer computerName -username Username -  
ou "Your-AWS-Delegated-Organizational-Unit"
```

Contoh berikut adalah seperti apa perintah itu ketika bergabung dengan pengguna administratif pada instance Mac bernama **myec2mac01 example.com** domain:

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -  
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

- Gunakan perintah berikut untuk menambahkan Administrator AWS Delegasi ke pengguna administratif pada instance Mac Anda:

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators"
```

- Gunakan perintah berikut untuk mengonfirmasi bahwa gabungan domain Microsoft AD Active Directory AWS Terkelola berhasil:

```
dsconfigad -show
```

Anda telah berhasil menggabungkan instance Mac ke Direktori Aktif Microsoft AD AWS Terkelola. Sekarang Anda dapat masuk ke instans Mac menggunakan kredensial Direktori Aktif Microsoft AD AWS Terkelola.

Ketika Anda pertama kali masuk ke instance Mac Anda, Anda harus diberikan opsi untuk masuk sebagai pengguna “Lainnya”. Pada titik ini, Anda dapat menggunakan kredensi domain Active Directory untuk masuk ke instance Mac. Jika Anda tidak diberikan “Lainnya” di layar masuk setelah menyelesaikan langkah-langkah ini, masuk sebagai pengguna ec2 dan kemudian keluar.

Untuk masuk menggunakan antarmuka pengguna grafis dengan pengguna domain, ikuti langkah-langkah di [Connect to graphical user interface \(GUI\) instans Anda](#) di Panduan Pengguna Amazon EC2.

Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola

Untuk bergabung dengan komputer ke Microsoft AD yang AWS Dikelola, Anda memerlukan akun yang memiliki hak istimewa untuk bergabung dengan komputer ke direktori.

Dengan AWS Directory Service untuk Microsoft Active Directory, anggota grup Admin dan Administrator Server AWS Delegasi memiliki hak istimewa ini.

Namun, sebagai praktik terbaik, Anda harus menggunakan akun yang hanya memiliki hak istimewa minimum yang diperlukan. Prosedur berikut menunjukkan cara membuat grup baru yang disebut *Joiners* dan mendelegasikan hak istimewa untuk grup ini yang diperlukan untuk menggabungkan komputer ke direktori.

Anda harus melakukan prosedur ini pada komputer yang telah tergabung ke direktori Anda dan memiliki MMC snap-in Pengguna dan Komputer Direktori Aktif terinstal. Anda juga harus masuk sebagai administrator domain.

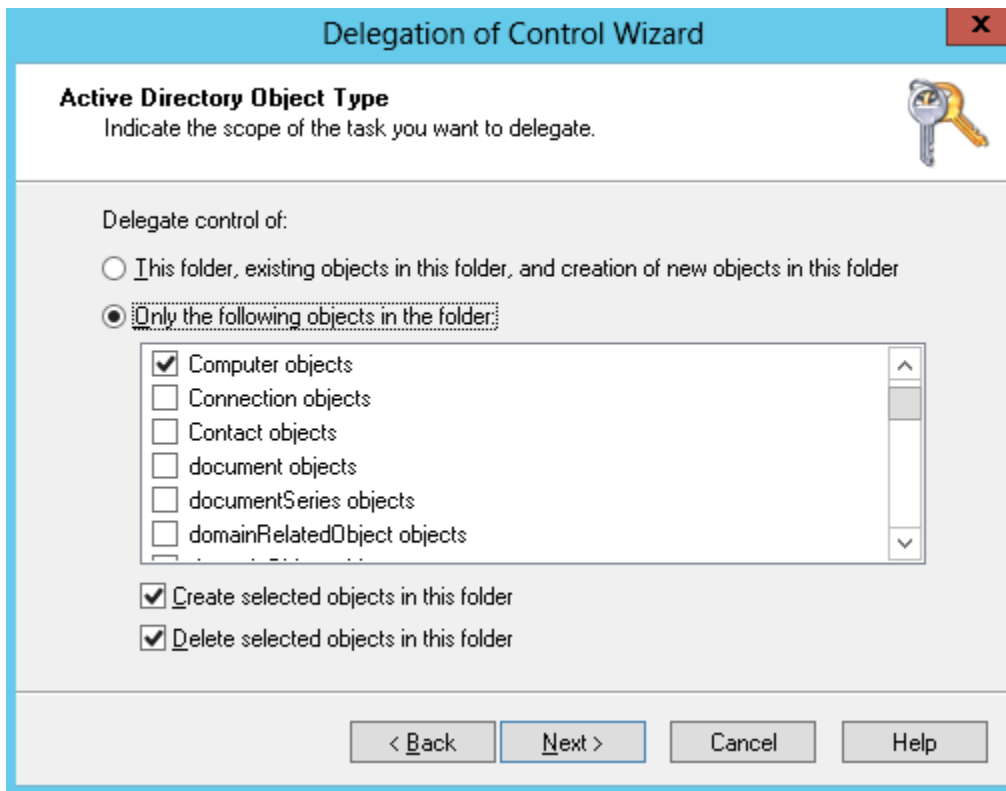
Untuk mendelegasikan hak istimewa bergabung untuk AWS Microsoft AD yang Dikelola

1. Buka Pengguna dan komputer Direktori Aktif dan pilih organizational unit (OU) yang memiliki nama NetBIOS Anda di pohon navigasi, kemudian pilih Pengguna OU.

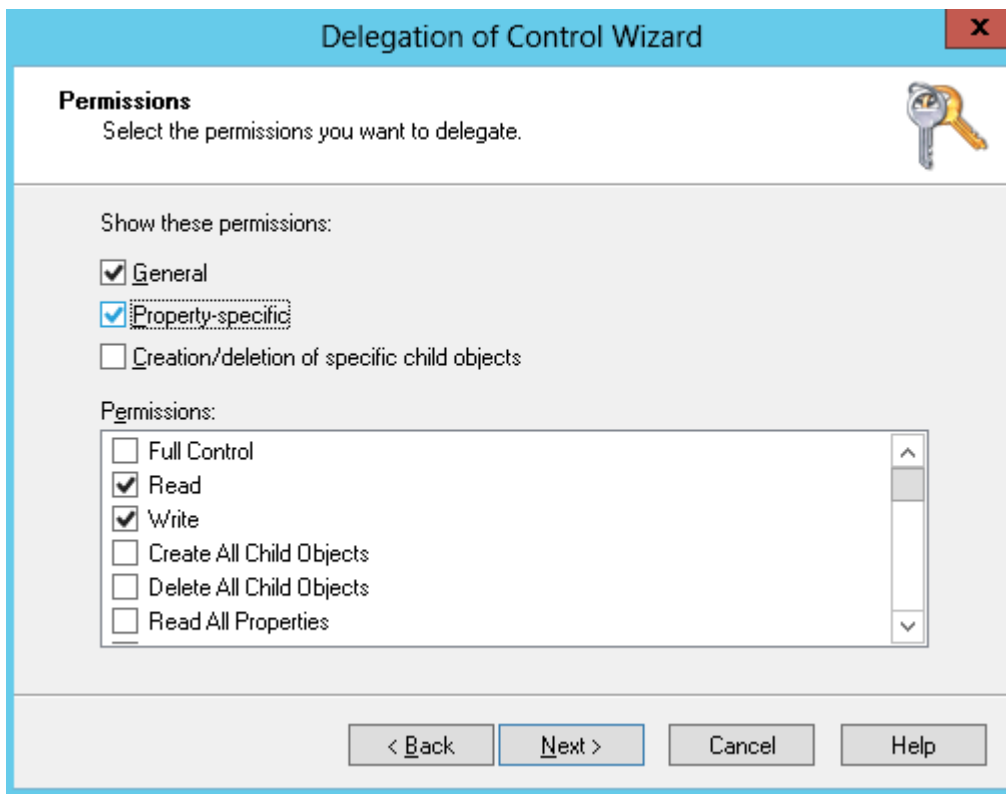
Important

Saat Anda meluncurkan AWS Directory Service untuk Microsoft Active Directory, AWS buat unit organisasi (OU) yang berisi semua objek direktori Anda. OU ini, yang memiliki nama NetBIOS yang Anda ketik saat membuat direktori Anda, terletak di root domain. Root domain dimiliki dan dikelola oleh AWS. Anda tidak dapat membuat perubahan ke root domain itu sendiri, oleh karena itu, Anda harus membuat grup **Joiners** dalam OU yang memiliki nama NetBIOS Anda.

2. Buka menu konteks (klik kanan) untuk Pengguna, pilih Baru, lalu pilih Grup.
3. Di kotak Objek Baru - Grup, ketik hal berikut dan pilih OK.
 - Untuk Nama grup, ketik **Joiners**.
 - Untuk Cakupan grup, pilih Global.
 - Untuk Jenis grup, pilih Keamanan.
4. Pada pohon navigasi, pilih kontainer Komputer di bawah nama NetBIOS Anda. Dari menu Tindakan, pilih Kendali Delegasi.
5. Pada halaman Delegasi Control Wizard, pilih Selanjutnya, lalu pilih Tambahkan.
6. Di kotak Pilih Pengguna, Komputer, atau Grup, ketik Joiners dan pilih OK. Jika ditemukan lebih dari satu objek, pilih grup Joiners yang dibuat di atas. Pilih Berikutnya.
7. Pada halaman Tugas untuk Didelegasikan, pilih Buat tugas kustom untuk didelegasikan, lalu pilih Selanjutnya.
8. Pilih Hanya objek berikut dalam folder, lalu pilih Objek komputer.
9. Pilih Buat objek yang dipilih dalam folder ini dan Hapus objek yang dipilih dalam folder ini. Lalu pilih Selanjutnya.



10. Pilih Baca dan Tulis, lalu pilih Selanjutnya.



11. Verifikasi informasi pada halaman Menyelesaikan Delegasi Control Wizard, dan klik Selesai.

12. Buat pengguna dengan kata sandi yang kuat dan tambahkan pengguna tersebut ke grup `Joiners`. Pengguna ini harus berada di kontainer Pengguna yang berada di bawah nama `NetBIOS` Anda. Pengguna tersebut kemudian akan memiliki hak istimewa yang memadai untuk menghubungkan instans ke direktori.

Membuat atau mengubah opsi DHCP yang disetel untuk Microsoft AD yang AWS Dikelola

AWS merekomendasikan agar Anda membuat set opsi DHCP untuk Directory Service direktori Anda dan menetapkan opsi DHCP yang disetel ke VPC tempat direktori Anda berada. Ini memungkinkan setiap instans di VPC tersebut mengarah ke domain tertentu, dan server DNS untuk menyelesaikan nama domain mereka.

Untuk informasi selengkapnya tentang set opsi DHCP, lihat [Set opsi DHCP](#) di Panduan Pengguna Amazon VPC.

Untuk membuat set opsi DHCP untuk direktori Anda

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Set Opsi DHCP, lalu pilih Buat set opsi DHCP.
3. Pada halaman Buat set opsi DHCP, masukkan nilai berikut untuk direktori Anda:

Nama

Tanda opsional untuk set opsi.

Nama domain

Nama yang memenuhi syarat untuk direktori, seperti `corp.example.com`.

Server nama domain

Alamat IP server DNS direktori AWS-provided Anda.

Note

Anda dapat menemukan alamat ini dengan membuka panel navigasi [Konsol AWS Directory Service](#), memilih direktori dan kemudian memilih ID direktori yang benar.

Server NTP

Biarkan bidang ini kosong.

Server nama NetBIOS

Biarkan bidang ini kosong.

Jenis simpul NetBIOS

Biarkan bidang ini kosong.

4. Pilih Buat set opsi DHCP. Set opsi DHCP baru muncul dalam daftar opsi DHCP Anda.
5. Catat ID set baru opsi DHCP (dopt-~~xxxxxxxxxx~~). Anda menggunakannya untuk mengasosiasikan set opsi yang baru dengan VPC Anda.

Untuk mengubah set opsi DHCP yang terkait dengan VPC

Setelah Anda membuat set opsi DHCP, Anda tidak dapat mengubahnya. Jika Anda ingin VPC Anda untuk menggunakan set opsi DHCP yang berbeda, Anda harus membuat satu set baru dan mengasosiasikannya dengan VPC Anda. Anda juga dapat mengatur VPC Anda untuk tidak menggunakan opsi DHCP sama sekali.

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Your VPCs.
3. Pilih VPC, lalu pilih Tindakan, Edit pengaturan VPC.
4. Untuk Set opsi DHCP, pilih satu set opsi atau pilih Tidak ada set opsi DHCP, lalu pilih Simpan.

Untuk mengubah set opsi DHCP yang terkait dengan VPC menggunakan baris perintah lihat berikut ini:

- AWS CLI: [associate-dhcp-options](#)
- AWS Tools for Windows PowerShell: [Register-EC2DhcpOption](#)

Manajemen pengguna dan grup di Microsoft AD yang AWS Dikelola

Anda dapat mengelola pengguna dan grup di Microsoft AD yang AWS Dikelola. Anda membuat pengguna untuk mewakili orang atau entitas yang dapat mengakses direktori Anda. Anda juga dapat membuat grup untuk memberikan dan menolak izin ke lebih dari satu pengguna sekaligus. Anda dapat menambahkan tidak hanya pengguna ke grup, tetapi juga grup ke grup. Saat Anda menambahkan pengguna ke grup, pengguna mewarisi peran dan izin yang ditetapkan ke grup. Saat Anda menambahkan grup ke grup, grup akan berbagi hubungan orang tua-anak, tempat grup anak mewarisi peran dan izin yang ditetapkan ke grup induk. Anda juga dapat menyalin keanggotaan grup pengguna ke pengguna lain.

Anda dapat mengelola pengguna dan grup dengan [the section called “Directory Service Data”](#) menggunakan metode berikut:

- [Konsol Manajemen AWS](#)
- [AWS CLI](#)
- [AWS Directory Service Data API](#)
- [AWS Tools for Windows PowerShell](#)

Untuk demonstrasi dari AWS Directory Service Data CLI, lihat video berikut. YouTube

[Mengelola pengguna dan grup di Microsoft AD yang AWS Dikelola menggunakan CRUD APIs](#)

Atau, Anda dapat menggunakan instance yang [bergabung dengan domain](#).

Kelola pengguna dan grup dengan Konsol Manajemen AWS

Anda dapat mengelola pengguna dan grup Konsol Manajemen AWS dengan AWS Directory Service Data with. Directory Service Data adalah ekstensi Directory Service yang memberi Anda kemampuan untuk melakukan tugas manajemen objek bawaan. Beberapa tugas ini termasuk membuat pengguna dan grup dan menambahkan pengguna ke grup serta grup ke grup.

Untuk informasi selengkapnya, lihat [AWS Mengelola pengguna dan grup Microsoft AD yang Dikelola dengan Konsol Manajemen AWS](#).

 Note

Untuk menggunakan fitur ini, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup](#).

Anda hanya dapat mengelola pengguna dan grup dengan Konsol Manajemen AWS from the Primary AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).

Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

Kelola pengguna dan grup dengan AWS CLI

Anda dapat mengelola pengguna dan grup dengan AWS CLI melalui [AWS Directory Service Data API](#). Directory Service Data adalah ekstensi Directory Service yang memberi Anda kemampuan untuk melakukan tugas manajemen objek bawaan menggunakan ds-data namespace. Beberapa tugas ini termasuk membuat pengguna dan grup dan menambahkan pengguna ke grup serta grup ke grup.

Buat pengguna dengan AWS Directory Service Data CLI

Berikut ini adalah contoh AWS CLI perintah yang menggunakan ds-data namespace untuk membuat pengguna.

```
aws ds-data create-user --directory-id d-1234567890 --sam-account-name "jane.doe" --  
region your-Primary-Region-name
```

 Note

Untuk menggunakan ini AWS CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan atau menonaktifkan manajemen pengguna dan grup atau Directory Service Data AWS](#).

Anda hanya dapat mengelola pengguna dan grup dengan AWS Directory Service Data CLI dari primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).

Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) atau [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#). Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan di IAM](#)

Untuk informasi selengkapnya, lihat [AWS Mengelola pengguna dan grup Microsoft AD yang Dikelola dengan AWS CLI](#).

Kelola pengguna dan grup dengan AWS Tools for PowerShell

[AWS Tools for PowerShell](#) Ini menyediakan dua modul terpisah untuk mengelola AWS Directory Service: `AWS.Tools.DirectoryService (DS)` dan `AWS.Tools.DirectoryServiceData (DSD)`. Saat bekerja dengan AWS Directory Service, pastikan Anda menggunakan modul yang sesuai untuk operasi yang Anda inginkan.

- `DirectoryServiceModul` ini berisi cmdlet untuk mengelola konfigurasi dan administrasi layanan direktori, termasuk cmdlet seperti `Enable-DSDirectoryDataAccess`, dan `Disable-DSDirectoryDataAccess` `Reset-DSUserPassword`
- `DirectoryServiceDataModul` ini berisi cmdlet untuk melakukan operasi dalam direktori, yang secara khusus difokuskan pada manajemen pengguna dan grup. Cmdlet DSD ini mencakup operasi manajemen pengguna (`New-DSDUser`, `Get-DSDUser`, dan `Remove-DSDUser`) `Update-DSDUser`, operasi manajemen grup (`Get-DSDGroup`, `New-DSDGroup`, `Remove-DSDGroup`) `Update-DSDGroup`, manajemen keanggotaan grup (`Add-DSDGroupMember`, dan `Remove-DSDGroupMember`) dan fungsionalitas pencarian (`Search-DSDUser` dan `Search-DSDGroup`)

Mengelola pengguna dan grup dengan instans lokal atau instans Amazon EC2

Jika AWS Directory Service Data tidak mendukung kasus penggunaan Anda, sebaiknya mengelola pengguna dan grup dengan instans lokal atau EC2.

Untuk membuat pengguna dan grup di Microsoft AD yang AWS Dikelola, Anda dapat menggunakan instans apa pun (baik dari lokal maupun EC2) yang telah digabungkan ke AWS Microsoft AD yang Dikelola. Anda harus masuk sebagai pengguna yang memiliki hak istimewa untuk membuat pengguna dan grup. Anda juga perlu menginstal Alat Direktori Aktif pada instans Anda sehingga Anda dapat menambahkan pengguna dan grup Anda dengan alat Pengguna dan Komputer Direktori Aktif.

- Anda dapat menerapkan instans EC2 yang telah dikonfigurasi sebelumnya dengan alat administratif Active Directory yang sudah diinstal sebelumnya dari konsol manajemen. Directory Service Untuk informasi selengkapnya, lihat [Meluncurkan instans administrasi direktori di Direktori Aktif Microsoft AD AWS Terkelola](#).
- Jika Anda perlu menerapkan instans EC2 yang dikelola sendiri dengan alat administratif dan menginstal alat yang diperlukan, lihat. [Langkah 3: Menerapkan instans Amazon EC2 untuk mengelola Direktori Aktif Microsoft AD yang AWS Dikelola](#)

Topik

- [AWS Mengelola pengguna dan grup Microsoft AD yang Dikelola dengan Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell](#)
- [Mengelola pengguna dan grup dengan EC2 instans Amazon](#)

AWS Mengelola pengguna dan grup Microsoft AD yang Dikelola dengan Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell

Anda dapat menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell untuk AWS mengelola pengguna dan grup Microsoft AD yang Dikelola [AWS Directory Service Data](#). AWS Directory Service Data CLI menggunakan namespace. ds-data Untuk informasi lebih lanjut tentang AWS CLI, lihat [Memulai dengan AWS CLI](#). Untuk informasi selengkapnya AWS Tools for PowerShell, lihat [Panduan AWS Tools for PowerShell Pengguna](#).

Lihat prosedur berikut untuk informasi selengkapnya tentang membuat, melihat, memperbarui, dan menghapus pengguna dan grup Microsoft AD yang AWS Dikelola.

Prosedur manajemen pengguna dan grup

- [Mengaktifkan atau menonaktifkan manajemen pengguna dan grup atau Directory Service Data AWS](#)
- [Membuat pengguna Microsoft AD yang AWS Dikelola](#)
- [Melihat dan memperbarui pengguna Microsoft AD yang AWS Dikelola](#)
- [Menghapus pengguna Microsoft AD yang AWS Dikelola](#)
- [Menonaktifkan pengguna AWS Microsoft AD yang Dikelola](#)
- [Menyetel ulang dan mengaktifkan kata sandi pengguna AWS Microsoft AD yang Dikelola](#)
- [Membuat grup iklan Microsoft yang AWS Dikelola](#)
- [Melihat dan memperbarui detail grup Microsoft AD yang AWS Dikelola](#)
- [Menghapus grup iklan Microsoft yang AWS Dikelola](#)
- [Menambahkan dan menghapus anggota Microsoft AD yang AWS Dikelola ke grup dan grup ke grup](#)
- [Menyalin keanggotaan grup Microsoft AD AWS Terkelola di Konsol Manajemen AWS](#)

Mengaktifkan atau menonaktifkan manajemen pengguna dan grup atau Directory Service Data AWS

Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data, itu harus diaktifkan. Setelah diaktifkan, Anda dapat mengelola pengguna dan grup dari Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Important

- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Untuk daftar wilayah yang mendukung AWS Directory Service Data, lihat [Didukung Wilayah AWS untuk Directory Service Data](#).

- Kontrol akses untuk AWS Directory Service Data berbeda dari kontrol akses untuk Layanan AWS seperti Amazon WorkSpaces, Amazon Quick, dan Amazon WorkMail. Untuk informasi selengkapnya, lihat [AWS otorisasi aplikasi dengan Directory Service Data](#).

Mengaktifkan AWS Directory Service Data

Gunakan prosedur berikut untuk mengaktifkan manajemen pengguna dan grup atau AWS Directory Service Data untuk iklan Microsoft AWS Terkelola yang ada dengan Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Konsol Manajemen AWS

Anda dapat mengaktifkan manajemen pengguna dan grup dengan Konsol Manajemen AWS.

Untuk mengaktifkan manajemen pengguna dan grup

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Pada halaman Detail direktori, untuk mengaktifkan manajemen pengguna dan grup, pilih Aktifkan.
3. Dalam kotak dialog Aktifkan manajemen pengguna dan grup, pilih Aktifkan.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang mengaktifkan AWS Directory Service Data CLI. Anda harus menyertakan nomor ID Direktori Anda dalam permintaan Anda.

Note

Perintah enable AWS Directory Service Data CLI digunakan. `aws ds`

Untuk mengaktifkan AWS Directory Service Data CLI

- Buka AWS CLI, dan jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola Anda:

```
aws ds enable-directory-data-access --directory-id d-1234567890
```

AWS Tools for PowerShell

Untuk mengaktifkan Directory Service Data dengan Tools for PowerShell

- Buka PowerShell, dan jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola Anda:

```
Enable-DSDirectoryDataAccess -DirectoryId d-1234567890
```

Menonaktifkan AWS Directory Service Data

Gunakan prosedur berikut untuk menonaktifkan manajemen pengguna dan grup atau AWS Directory Service Data untuk iklan Microsoft AWS Terkelola yang ada dengan Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Konsol Manajemen AWS

Anda dapat menonaktifkan manajemen pengguna dan grup dengan file Konsol Manajemen AWS.

Untuk menonaktifkan manajemen pengguna dan grup

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Pada halaman Detail direktori, untuk menonaktifkan manajemen pengguna dan grup, pilih Nonaktifkan.
3. Dalam kotak dialog Nonaktifkan manajemen pengguna dan grup, pilih Nonaktifkan.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang menonaktifkan AWS Directory Service Data CLI. Anda harus menyertakan nomor ID Direktori Anda dalam permintaan Anda.

Note

Menonaktifkan perintah AWS Directory Service Data CLI digunakan. `aws ds`

Untuk menonaktifkan AWS Directory Service Data CLI

- Buka AWS CLI, dan jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola Anda:

```
aws ds disable-directory-data-access --directory-id d-1234567890
```

AWS Tools for PowerShell

Untuk menonaktifkan Directory Service Data dengan Tools for PowerShell

- Buka PowerShell, dan jalankan perintah berikut, ganti ID Direktori dengan ID Direktori Microsoft AD AWS Terkelola Anda:

```
Disable-DSDirectoryDataAccess -DirectoryId d-123456789
```

Membuat pengguna Microsoft AD yang AWS Dikelola

Gunakan prosedur berikut untuk membuat pengguna Microsoft AD AWS Terkelola baru dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

Konsol Manajemen AWS

Anda dapat membuat akun pengguna Microsoft AD AWS Terkelola baru di file Konsol Manajemen AWS. Saat membuat akun pengguna baru, Anda menentukan detail pengguna baru dan menentukan apakah akan menambahkan pengguna baru ke grup atau menyalin keanggotaan grup pengguna lain ke pengguna baru.

Untuk informasi selengkapnya, lihat [AWS Atribut Directory Service Data](#) dan [Jenis grup dan ruang lingkup grup](#).

Untuk membuat pengguna Microsoft AD yang AWS Dikelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pada halaman Detail direktori, di bawah bagian Pengguna, pilih Buat akun pengguna.
5. Halaman Tentukan detail pengguna terbuka. Di bawah bagian Informasi yang diperlukan, masukkan nama login pengguna dan kata sandi. Nama logon pengguna harus memenuhi ketentuan berikut:
 - Harus nama logon yang unik
 - Panjangnya bisa sampai 20 karakter
 - Hanya dapat berisi karakter alfanumerik
 - ~!@#\$%^&* _+=`|\\(){}[]:;'"<>,.?/
 - Kata sandi harus mematuhi persyaratan kebijakan kata sandi Anda. Periksa dengan AWS administrator Anda untuk informasi lebih lanjut.

Warning

Nama logon pengguna tidak dapat diubah setelah pengguna dibuat.

- a. (Opsional) Di bawah bagian Informasi utama, Anda dapat memasukkan nama depan dan belakang untuk pengguna. Anda juga dapat memasukkan nama tampilan dan deskripsi untuk pengguna.

- b. (Opsional) Di bawah bagian Metode kontak, Anda dapat memasukkan alamat email dan nomor telepon untuk pengguna.
- c. (Opsional) Di bawah bagian Informasi terkait Pekerjaan, Anda dapat memasuki departemen, manajer, kantor, dan perusahaan untuk pengguna.
- d. (Opsional) Di bawah bagian Alamat, Anda dapat memasukkan alamat untuk pengguna.
- e. (Opsional) Di bawah bagian Pengaturan akun, Anda dapat memasukkan catatan, bahasa pilihan, dan nama utama layanan untuk pengguna.

Untuk informasi selengkapnya tentang atribut pengguna, lihat [AWS Atribut Directory Service Data](#) dan [Microsoft dokumentasi](#).

- 6. Pilih Berikutnya setelah Anda memberikan detail akun pengguna.
- 7. Pada halaman Tambahkan pengguna ke grup - opsional, Anda dapat menambahkan pengguna ke grup baru atau ke grup yang ada. Anda juga dapat menyalin keanggotaan grup pengguna yang ada ke pengguna baru. Jika Anda tidak ingin menambahkan pengguna ke grup, pilih Berikutnya. Pindah ke Langkah 12 untuk melanjutkan prosedur ini.
- 8. (Opsional) Untuk membuat grup baru, lihat [Membuat grup iklan Microsoft yang AWS Dikelola](#).
- 9. (Opsional) Untuk menambahkan pengguna baru ke grup yang ada:
 - Pilih grup yang ingin Anda tambahkan pengguna baru di bagian Grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian.
- 10. (Opsional) Untuk menyalin keanggotaan grup pengguna yang sudah ada ke pengguna baru:
 - a. Pilih Salin keanggotaan grup dari tab pengguna. Untuk menemukan pengguna dengan keanggotaan grup yang ingin Anda salin, masukkan nama log masuk pengguna di kotak pencarian di bawah bagian Pengguna.
 - b. Di bagian Grup yang dipilih, pilih grup yang harus menjadi anggota pengguna baru.
- 11. Pilih Berikutnya saat Anda siap membuat akun pengguna baru.
- 12. Pada halaman Tinjau dan buat pengguna, tinjau semua pilihan yang Anda buat. Pilih Create user (Buat pengguna).
- 13. Setelah pengguna dikonfigurasi, Anda telah dibawa ke halaman detail pengguna baru. Sebuah spanduk muncul yang menyatakan pengguna telah berhasil dibuat.

⚠ Important

Jika Anda menerima pesan galat yang memberi tahu Anda bahwa Anda tidak memiliki izin untuk membuat pengguna, ikuti petunjuk dalam pesan galat untuk meminta administrator Anda memberi Anda akses.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang membuat akun pengguna Microsoft AD AWS Terkelola baru dengan AWS Directory Service Data CLI. Anda harus menyertakan nomor ID direktori Anda dan nama login pengguna dalam permintaan Anda. Anda juga dapat menyertakan atribut lain, seperti nama tampilan pengguna dengan `DisplayName` atribut. Untuk informasi selengkapnya, lihat [AWS Atribut Directory Service Data](#) dan [Jenis grup dan ruang lingkup grup](#).

Untuk membuat pengguna Microsoft AD yang AWS Dikelola dengan AWS CLI

- Buka AWS CLI, dan jalankan perintah berikut, ganti ID Direktori, nama pengguna, dan nama tampilan dengan ID Direktori Microsoft AD AWS Terkelola dan kredensial yang diinginkan:

```
aws ds-data create-user \  
  --directory-id d-1234567890 \  
  --sam-account-name "jane.doe" \  
  --other-attributes '{  
    "DisplayName" : { "S": "jane.doe" },  
    "Department":{ "S": "Legal" }  
  }'
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang membuat akun pengguna Microsoft AD AWS Terkelola baru dengan AWS Tools for PowerShell. Anda harus menyertakan nomor ID direktori Anda dan nama login pengguna dalam permintaan Anda. Anda juga dapat menyertakan atribut lain, seperti nama tampilan pengguna dengan `DisplayName` atribut. Untuk informasi selengkapnya, lihat [AWS Atribut Directory Service Data](#) dan [Jenis grup dan ruang lingkup grup](#).

Untuk membuat pengguna Microsoft AD AWS Terkelola dengan Tools for PowerShell

- Buka PowerShell, dan jalankan perintah berikut, ganti ID Direktori, nama pengguna, dan nama tampilan dengan ID Direktori Microsoft AD AWS Terkelola dan kredensial yang diinginkan:

```
New-DSDUser `
  -DirectoryId d-1234567890 `
  -SAMAccountName "jane.doe" `
  -OtherAttribute @{
    DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'jane.doe' }
    Department = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'Legal' }
  }
```

Melihat dan memperbarui pengguna Microsoft AD yang AWS Dikelola

Gunakan prosedur berikut untuk melihat atau memperbarui detail pengguna Microsoft AD AWS Terkelola dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Melihat detail pengguna Microsoft AD yang AWS Dikelola

Anda dapat melihat detail pengguna di Konsol Manajemen AWS atau AWS CLI. Detail pengguna mencakup informasi profil dan akun serta keanggotaan grup.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS](#)

[kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

- [Membuat pengguna Microsoft AD yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat melihat detail pengguna Microsoft AD yang AWS Dikelola di Konsol Manajemen AWS.

Untuk melihat detail dan detail akun pengguna Microsoft AD AWS Terkelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Pengguna. Tab menampilkan daftar pengguna di direktori Anda.
5. Pilih pengguna. Anda diarahkan ke layar Detail Pengguna. Layar Detail pengguna menampilkan informasi berikut:
 - Grup pengguna adalah anggota (keanggotaan grup)
 - Detail profil (seperti informasi utama seperti nama login pengguna, nama depan, nama belakang, dll.)
 - Pengaturan akun (seperti informasi akun seperti nama utama pengguna, nama utama layanan, nama terhormat, dll.)
 - Status akun

Untuk informasi selengkapnya tentang atribut pengguna, lihat [AWS Atribut Directory Service Data](#) dan [Microsoft dokumentasi](#).

AWS CLI

Dengan ini AWS CLI, Anda dapat melihat detail pengguna, yang mencakup informasi profil dan akun serta keanggotaan grup.

Untuk melihat profil pengguna Microsoft AD AWS Terkelola dan detail akun dengan AWS CLI

Berikut ini menjelaskan cara melihat detail pengguna Microsoft AD AWS Terkelola dengan AWS Directory Service Data CLI.

- Untuk melihat detail pengguna, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori dan nama pengguna dengan ID Direktori Microsoft AD AWS Terkelola dan nama pengguna Anda:

```
aws ds-data describe-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

Untuk melihat keanggotaan grup pengguna

Berikut ini menjelaskan cara melihat keanggotaan grup pengguna Microsoft AD AWS Terkelola dengan AWS Directory Service Data CLI.

- Untuk melihat keanggotaan grup pengguna, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori dan nama pengguna dengan ID Direktori Microsoft AD AWS Terkelola dan nama pengguna Anda:

```
aws ds-data list-groups-for-member --directory-id d-1234567890 --sam-account-name "jane.doe"
```

Untuk informasi selengkapnya tentang atribut pengguna, lihat [AWS Atribut Directory Service Data](#) dan [Microsoft dokumentasi](#).

AWS Tools for PowerShell

Dengan Tools for PowerShell, Anda dapat melihat detail pengguna, yang mencakup informasi profil dan akun serta keanggotaan grup.

Untuk melihat profil pengguna Microsoft AD AWS Terkelola dan detail akun dengan Tools for PowerShell

Berikut ini menjelaskan cara melihat detail pengguna Microsoft AD AWS Terkelola dengan Alat untuk PowerShell.

- Untuk melihat detail pengguna, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori dan nama pengguna dengan ID Direktori Microsoft AD AWS Terkelola dan nama pengguna Anda:

```
Get-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

Untuk melihat keanggotaan grup pengguna

Berikut ini menjelaskan cara melihat keanggotaan grup pengguna Microsoft AD AWS Terkelola dengan Alat untuk PowerShell.

- Untuk melihat keanggotaan grup pengguna, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori dan nama pengguna dengan ID Direktori Microsoft AD AWS Terkelola dan nama pengguna Anda:

```
(Get-DSDGroupsForMemberList -DirectoryId d-1234567890 -SAMAccountName "jane.doe").Groups
```

Untuk informasi selengkapnya tentang atribut pengguna, lihat [AWS Atribut Directory Service Data](#) dan [Microsoft dokumentasi](#).

Memperbarui detail pengguna Microsoft AD yang AWS Dikelola

Gunakan prosedur berikut untuk memperbarui pengguna Microsoft AD AWS Terkelola dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, AWS Tools for PowerShell.

 Note

Panjang atribut minimum adalah 1.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).

- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).
- [Membuat pengguna Microsoft AD yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat memperbarui detail pengguna Microsoft AD yang AWS Dikelola di Konsol Manajemen AWS.

Untuk memperbarui detail pengguna Microsoft AD AWS Terkelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Pengguna. Tab menampilkan daftar pengguna di direktori Anda.
5. Pilih pengguna. Untuk menemukan pengguna, masukkan nama logon pengguna di kotak pencarian di bawah bagian Pengguna. Anda diarahkan ke layar Detail Pengguna.
6. Untuk mengedit grup yang menjadi anggota pengguna, pilih Grup. Dari tab ini, Anda dapat menambah dan menghapus pengguna dari grup. Untuk informasi selengkapnya, lihat [Menambahkan anggota Microsoft AD yang AWS Dikelola ke grup](#).
7. Untuk mengedit detail profil pengguna, pilih Profil, lalu pilih Edit. Atau pilih Tindakan, lalu pilih Edit pengguna. Buat dan tinjau pembaruan Anda, lalu pilih Simpan.

Warning

Nama logon pengguna tidak dapat diubah setelah pengguna dibuat.

8. Untuk mengedit pengaturan akun pengguna, pilih Pengaturan akun pengguna. Atau pilih Tindakan, lalu pilih Edit pengguna. Buat dan tinjau pembaruan Anda, lalu pilih Simpan.

Untuk informasi selengkapnya tentang atribut pengguna, lihat [AWS Atribut Directory Service Data](#) dan [Microsoft dokumentasi](#).

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang memperbarui detail pengguna Microsoft AD AWS Terkelola dengan AWS Directory Service Data CLI.

Saat memperbarui akun pengguna, Anda harus menyertakan nomor ID direktori dan nama log masuk pengguna. Anda juga harus menyertakan jenis dan atribut pembaruan yang ingin Anda perbarui dalam permintaan Anda, seperti nama belakang pengguna dengan Surname parameter. Untuk informasi selengkapnya, lihat [atribut AWS Directory Service Data](#).

- Untuk memperbarui detail pengguna, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori, nama pengguna, jenis pengguna, dan nilai atribut dengan ID Direktori Microsoft AD AWS Terkelola, nama pengguna, dan jenis pengguna serta nilai atribut yang diinginkan:

```
aws ds-data update-user --directory-id d-1234567890 --sam-account-name "jane.doe" --  
update-type "REPLACE" --surname "Doe"
```

Note

Saat menghapus atribut pengguna dengan perintah CLI [update-user](#), Anda harus menentukan atribut dan nilai yang tepat untuk dihapus. Untuk menentukan atribut pengguna, gunakan [perintah deskripsi-pengguna](#).

Untuk informasi selengkapnya tentang atribut pengguna, lihat [AWS Atribut Directory Service Data](#) dan [Microsoft dokumentasi](#).

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang memperbarui detail pengguna Microsoft AD yang AWS Dikelola AWS Tools for PowerShell.

Saat memperbarui akun pengguna, Anda harus menyertakan nomor ID direktori dan nama log masuk pengguna. Anda juga harus menyertakan jenis dan atribut pembaruan yang ingin Anda perbarui dalam permintaan Anda, seperti nama belakang pengguna dengan Surname parameter. Untuk informasi selengkapnya, lihat [atribut AWS Directory Service Data](#).

- Untuk memperbarui detail pengguna, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori, nama pengguna, jenis pengguna, dan nilai atribut dengan ID Direktori Microsoft AD AWS Terkelola, nama pengguna, dan jenis pengguna serta nilai atribut yang diinginkan:

```
Update-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe" -UpdateType  
"REPLACE" -Surname "Doe"
```

Untuk informasi selengkapnya tentang atribut pengguna, lihat [AWS Atribut Directory Service Data](#) dan [Microsoft dokumentasi](#).

Menghapus pengguna Microsoft AD yang AWS Dikelola

Gunakan prosedur berikut untuk menghapus pengguna Microsoft AD AWS Terkelola dengan manajemen pengguna dan grup atau AWS Directory Service Data di Konsol Manajemen AWS, AWS CLI, AWS Tools for PowerShell.

Important

Saat Anda menghapus akun pengguna dari direktori, semua informasi tentang pengguna dihapus, termasuk izin apa pun yang dimiliki pengguna untuk mengakses akun dan aplikasi mereka.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola:](#)

[AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

- [Membuat pengguna Microsoft AD yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat menghapus akun pengguna Microsoft AD yang AWS Dikelola di Konsol Manajemen AWS.

Untuk menghapus akun pengguna Microsoft AD yang AWS Dikelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Pengguna. Tab menampilkan daftar pengguna di direktori Anda.
5. Pilih pengguna yang akunnya ingin Anda hapus. Untuk menemukan pengguna, masukkan nama logon pengguna di kotak pencarian di bawah bagian Pengguna. Anda diarahkan ke layar Detail Pengguna.
6. Pilih Tindakan. Kemudian pilih Hapus akun pengguna dan Hapus akun pengguna lagi.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang menghapus akun pengguna Microsoft AD AWS Terkelola dengan AWS Directory Service Data CLI.

Untuk menghapus akun pengguna Microsoft AD yang AWS Dikelola dengan AWS CLI

- Buka AWS CLI, dan jalankan perintah berikut, ganti ID Direktori dan nama pengguna dengan ID Direktori Microsoft AD AWS Terkelola dan nama pengguna Anda:

```
aws ds-data delete-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang menghapus akun pengguna Microsoft AD yang AWS Dikelola. AWS Tools for PowerShell

Untuk menghapus akun pengguna Microsoft AD yang AWS Dikelola dengan AWS Tools for PowerShell

- Buka PowerShell, dan jalankan perintah berikut, ganti ID Direktori dan nama pengguna dengan ID Direktori Microsoft AD AWS Terkelola dan nama pengguna Anda:

```
Remove-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

Menonaktifkan pengguna AWS Microsoft AD yang Dikelola

Gunakan prosedur berikut untuk menonaktifkan pengguna Microsoft AD AWS Terkelola dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Important

Ketika Anda menonaktifkan akun pengguna, pengguna kehilangan izin untuk mengakses akun dan aplikasi mereka.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna

dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

- [Membuat pengguna Microsoft AD yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat menonaktifkan akun pengguna Microsoft AD yang AWS Dikelola di file Konsol Manajemen AWS.

Untuk menonaktifkan akun pengguna Microsoft AD AWS Terkelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Pengguna. Tab menampilkan daftar pengguna di direktori Anda.
5. Pilih pengguna yang akunnya ingin Anda nonaktifkan. Anda diarahkan ke layar Detail Pengguna.
6. Pilih Tindakan. Kemudian pilih Nonaktifkan akun pengguna dan Nonaktifkan akun pengguna lagi.

Note

Untuk mengaktifkan kembali akun pengguna Anda, Anda harus mengatur ulang kata sandi pengguna. Untuk informasi selengkapnya, lihat [Menyetel ulang dan mengaktifkan kata sandi pengguna AWS Microsoft AD yang Dikelola](#).

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang menonaktifkan akun pengguna Microsoft AD AWS Terkelola dengan AWS Directory Service Data CLI.

Untuk menonaktifkan akun pengguna Microsoft AD AWS Terkelola dengan AWS CLI

- Buka AWS CLI, dan jalankan perintah berikut, ganti ID Direktori dan nama pengguna dengan ID Direktori Microsoft AD AWS Terkelola dan nama pengguna Anda:

```
aws ds-data disable-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

 Note

Untuk mengaktifkan kembali akun pengguna Anda, Anda harus mengatur ulang kata sandi pengguna. Untuk informasi selengkapnya, lihat [Menyetel ulang dan mengaktifkan kata sandi pengguna AWS Microsoft AD yang Dikelola](#).

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang menonaktifkan akun pengguna Microsoft AD AWS Terkelola. AWS Tools for PowerShell

Untuk menonaktifkan akun pengguna Microsoft AD AWS Terkelola dengan AWS Tools for PowerShell

- Buka PowerShell, dan jalankan perintah berikut, ganti ID Direktori dan nama pengguna dengan ID Direktori Microsoft AD AWS Terkelola dan nama pengguna Anda:

```
Disable-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

 Note

Untuk mengaktifkan kembali akun pengguna Anda, Anda harus mengatur ulang kata sandi pengguna. Untuk informasi selengkapnya, lihat [Menyetel ulang dan mengaktifkan kata sandi pengguna AWS Microsoft AD yang Dikelola](#).

Menyetel ulang dan mengaktifkan kata sandi pengguna AWS Microsoft AD yang Dikelola

Gunakan prosedur berikut untuk mengatur ulang kata sandi pengguna Microsoft AD yang AWS Dikelola untuk mengaktifkan akun mereka dengan manajemen pengguna dan grup atau AWS Directory Service Data di Konsol Manajemen AWS, AWS CLI, AWS Tools for PowerShell.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).
- [Membuat pengguna Microsoft AD yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat mengatur ulang kata sandi pengguna Microsoft AD yang AWS Dikelola untuk mengaktifkan akun mereka di Konsol Manajemen AWS. Anda dapat melakukan tugas ini baik dari layar Direktori atau layar Detail direktori.

Direktori

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih Tindakan, lalu pilih Setel ulang kata sandi pengguna dan aktifkan akun.

- a. Di bawah Nama logon pengguna, masukkan nama logon pengguna untuk pengguna yang kata sandinya ingin Anda atur ulang.
 - b. Di bawah Kata sandi baru, masukkan kata sandi baru pengguna.
 - c. Di bawah Konfirmasi kata sandi, masukkan kata sandi baru pengguna lagi.
4. Setelah Anda mengonfirmasi kata sandi baru pengguna, pilih Atur ulang kata sandi dan aktifkan akun.

Detail direktori

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di AWS Region.
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Pengguna. Tab menampilkan daftar pengguna di direktori Anda.
5. Pilih pengguna yang kata sandinya ingin Anda atur ulang.
6. Pilih Tindakan, lalu pilih Setel ulang kata sandi pengguna dan aktifkan akun.
 - a. Di bawah Kata sandi baru, masukkan kata sandi baru pengguna.
 - b. Di bawah Konfirmasi kata sandi, masukkan kata sandi baru pengguna lagi.
7. Setelah Anda mengonfirmasi kata sandi baru pengguna, pilih Atur ulang kata sandi dan aktifkan akun.

AWS CLI

Anda dapat mengatur ulang kata sandi penggunaan Microsoft AD yang AWS Dikelola untuk mengaktifkan akun mereka dengan AWS Directory Service Data CLI.

Note

Perintah reset kata sandi pengguna menggunakan `aws ds`.

Untuk mengatur ulang kata sandi pengguna Microsoft AD yang AWS Dikelola dengan AWS CLI

- Untuk mengatur ulang kata sandi pengguna, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori, nama pengguna, dan kata sandi dengan ID Direktori Microsoft AD AWS Terkelola, nama pengguna, dan kredensial yang diinginkan:

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "your-password"
```

AWS Tools for PowerShell

Anda dapat mengatur ulang kata sandi penggunaan Microsoft AD yang AWS Dikelola untuk mengaktifkan akun mereka AWS Tools for PowerShell.

Untuk mengatur ulang kata sandi pengguna Microsoft AD yang AWS Dikelola dengan AWS Tools for PowerShell

- Untuk mengatur ulang kata sandi pengguna, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori, nama pengguna, dan kata sandi dengan ID Direktori Microsoft AD AWS Terkelola, nama pengguna, dan kredensial yang diinginkan:

```
Reset-DSUserPassword -DirectoryId d-1234567890 -UserName "jane.doe" -NewPassword "your-password"
```

Membuat grup iklan Microsoft yang AWS Dikelola

Gunakan prosedur berikut untuk membuat grup Microsoft AD AWS Terkelola dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).

- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

Konsol Manajemen AWS

Anda dapat membuat grup AD Microsoft AWS Terkelola baru di Konsol Manajemen AWS. Saat membuat grup baru, Anda menentukan detail grup dan menentukan [jenis dan cakupan grup](#). Anda juga memiliki opsi untuk menambahkan pengguna dan grup anak ke grup baru Anda atau menambahkan grup baru Anda ke grup induk.

Untuk membuat grup AD Microsoft AWS Terkelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih Buat grup. Anda diarahkan ke prosedur di mana Anda selesai membuat grup baru Anda.
6. Halaman Tentukan detail grup terbuka. Masukkan nama Grup. Nama grup harus memenuhi ketentuan berikut:
 - Harus nama grup yang unik
 - Panjangnya bisa sampai 64 karakter
 - Hanya dapat berisi karakter alfanumerik
 - ~!@#\$%^&* _+=`|()\{}[]:;'"<>,.?/

 Warning

Nama grup tidak dapat diubah setelah grup dibuat.

7. Pilih tipe Grup dari salah satu dari berikut ini:
 - Keamanan
 - Distribusi
 - Untuk mempelajari selengkapnya, lihat [the section called “Jenis grup”](#).
8. Pilih lingkup Grup dari salah satu dari berikut ini:
 - Domain lokal
 - Universal
 - Global
 - Anda dapat mengaktifkan Bandingkan cakupan untuk menampilkan bagan persamaan dan perbedaan antara cakupan grup. Untuk mempelajari selengkapnya, lihat [the section called “Lingkup grup”](#).
9. Setelah memberikan informasi utama dan metode kontak, pilih Berikutnya.
10. Halaman Tambahkan pengguna ke grup - Opsional terbuka dan Anda dapat menambahkan pengguna ke grup baru. Untuk menemukan pengguna yang akan ditambahkan ke grup, masukkan nama log masuk pengguna di kotak pencarian di bawah bagian Pengguna. Pilih pengguna yang ingin Anda tambahkan ke grup dan pilih Berikutnya.
11. Halaman Tambahkan grup anak - Opsional terbuka dan Anda dapat menambahkan grup yang ada ke grup baru. Grup yang ada menjadi grup anak dari grup yang baru dibuat. Saat Anda menambahkan grup anak ke grup Anda, grup Anda menjadi grup induk, dan grup anak mewarisi semua peran dan izin grup Anda. Untuk menemukan grup yang akan ditambahkan, masukkan nama grup di kotak pencarian di bawah bagian Tambahkan grup anak. Pilih grup anak yang ingin Anda tambahkan ke grup baru dan pilih Berikutnya.
12. Halaman Tambahkan grup induk - Opsional terbuka dan Anda dapat menambahkan grup baru ke grup yang ada. Grup baru menjadi kelompok induk dari grup yang ada. Saat Anda menambahkan grup ke grup induk, grup Anda menjadi grup anak dan mewarisi semua peran dan izin grup induk. Untuk menemukan grup yang akan ditambahkan, masukkan nama grup di kotak pencarian di bawah bagian Tambahkan grup induk. Pilih grup induk yang ingin Anda tambahkan ke grup baru dan pilih Berikutnya.

13. Pada halaman Tinjau dan buat grup, tinjau pilihan Anda, lalu pilih Buat grup.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang membuat grup AD Microsoft AWS Terkelola dengan AWS Directory Service Data CLI. Saat membuat grup baru, Anda harus menyertakan nomor ID Direktori dan nama grup. Anda juga dapat menambahkan atribut lain, seperti nama tampilan grup dengan `DisplayName` atribut. Untuk informasi selengkapnya, lihat [AWS Atribut Directory Service Data](#) dan [Jenis grup dan ruang lingkup grup](#).

Untuk membuat grup AD Microsoft AWS Terkelola dengan AWS CLI

- Buka AWS CLI, dan jalankan perintah berikut, ganti ID Direktori, nama pengguna, dan nama tampilan grup dengan ID Direktori Microsoft AD AWS Terkelola, nama pengguna, dan nama tampilan grup yang diinginkan:

```
aws ds-data create-group \
  --directory-id d-1234567890 \
  --sam-account-name "your-group-name" \
  --other-attributes '{
    "DisplayName": { "S": "myGroupDisplayName" }
    "Description": { "S": "myGroupDescription" }
  }'
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang membuat grup AD Microsoft AWS Terkelola dengan AWS Tools for PowerShell. Saat membuat grup baru, Anda harus menyertakan nomor ID Direktori dan nama grup. Anda juga dapat menambahkan atribut lain, seperti nama tampilan grup dengan `DisplayName` atribut. Untuk informasi selengkapnya, lihat [AWS Atribut Directory Service Data](#) dan [Jenis grup dan ruang lingkup grup](#).

Untuk membuat grup AD Microsoft AWS Terkelola dengan AWS Tools for PowerShell

- Buka PowerShell, dan jalankan perintah berikut, ganti ID Direktori, nama pengguna, dan nama tampilan grup dengan ID Direktori Microsoft AD AWS Terkelola, nama pengguna, dan nama tampilan grup yang diinginkan:

```
New-DSDGroup `
-DirectoryId d-1234567890 `
-SAMAccountName "your-group-name" `
-OtherAttribute @{
    DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'myGroupDisplayName' }
    Description = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'myGroupDescription' }
}
```

Melihat dan memperbarui detail grup Microsoft AD yang AWS Dikelola

Gunakan prosedur berikut untuk melihat atau memperbarui detail grup Microsoft AD AWS Terkelola dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Melihat detail grup iklan Microsoft yang AWS Dikelola

Anda dapat melihat atau memperbarui detail grup di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).
- [Membuat grup iklan Microsoft yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat melihat detail grup Microsoft AD yang AWS Dikelola di Konsol Manajemen AWS.

Untuk melihat detail grup Microsoft AD AWS Terkelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup. Anda diarahkan ke layar Detail grup. Layar Detail grup menampilkan informasi berikut:
 - Tab anggota mencantumkan pengguna dan grup anak yang merupakan anggota grup Anda.
 - Tab grup induk mencantumkan grup induk tempat grup Anda menjadi anggota.
 - Tab properti mencantumkan properti grup (seperti informasi utama seperti nama grup, nama tampilan grup, dll.).

AWS CLI

Anda dapat melihat detail grup Microsoft AD AWS Terkelola dengan AWS Directory Service Data CLI.

Untuk melihat detail grup Microsoft AD AWS Terkelola dengan AWS CLI

Berikut ini menjelaskan cara melihat detail grup Microsoft AD AWS Terkelola dengan AWS CLI.

- Untuk melihat detail grup, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori dan nama grup dengan ID Direktori Microsoft AD AWS Terkelola dan nama grup Anda:

```
aws ds-data describe-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

Untuk melihat anggota grup Microsoft AD yang AWS Dikelola dengan AWS CLI

Berikut ini menjelaskan cara melihat anggota grup Microsoft AD yang AWS Dikelola dengan AWS CLI.

- Untuk melihat detail grup, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori dan nama grup dengan ID Direktori Microsoft AD AWS Terkelola dan nama grup Anda:

```
aws ds-data list-group-members --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS Tools for PowerShell

Anda dapat melihat detail grup Microsoft AD yang AWS Dikelola dengan AWS Tools for PowerShell.

Untuk melihat detail grup Microsoft AD AWS Terkelola dengan AWS Tools for PowerShell

Berikut ini menjelaskan cara melihat detail grup Microsoft AD AWS Terkelola dengan Alat untuk PowerShell.

- Untuk melihat detail grup, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori dan nama grup dengan ID Direktori Microsoft AD AWS Terkelola dan nama grup Anda:

```
Get-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

Untuk melihat anggota grup Microsoft AD yang AWS Dikelola dengan AWS Tools for PowerShell

Berikut ini menjelaskan cara melihat anggota grup Microsoft AD AWS Terkelola dengan Alat untuk PowerShell.

- Untuk melihat detail grup, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori dan nama grup dengan ID Direktori Microsoft AD AWS Terkelola dan nama grup Anda:

```
(Get-DSDGroupMemberList -DirectoryId d-1234567890 -SAMAccountName "your-group-name").Members
```


Memperbarui detail grup Microsoft AD yang AWS Dikelola

Gunakan prosedur berikut untuk memperbarui detail grup Microsoft AD AWS Terkelola dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).
- [Membuat grup iklan Microsoft yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat memperbarui detail grup dengan Konsol Manajemen AWS. Untuk informasi selengkapnya, lihat [AWS Atribut Directory Service Data](#) dan [Jenis grup dan ruang lingkup grup](#)

Untuk memperbarui detail grup Microsoft AD AWS Terkelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup. Anda diarahkan ke layar Detail grup.

6. Untuk mengedit pengguna dan grup anak yang merupakan anggota grup Anda, pilih Anggota. Dari tab ini, Anda dapat menambahkan dan menghapus pengguna dan grup anak dari grup Anda. Untuk informasi selengkapnya, lihat [Menambahkan dan menghapus anggota ke grup dan grup ke grup](#).
7. Untuk mengedit grup induk yang menjadi anggota grup Anda, pilih Grup induk. Dari tab ini, Anda dapat menambahkan dan menghapus grup Anda dari grup induk. Untuk informasi selengkapnya, lihat [Menambahkan dan menghapus anggota ke grup dan grup ke grup](#).
8. Untuk mengedit properti grup Anda, pilih Properti, lalu pilih Edit. Atau pilih Tindakan, lalu pilih Edit grup. Buat dan tinjau pembaruan Anda, lalu pilih Simpan.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang memperbarui detail grup Microsoft AD AWS Terkelola dengan AWS Directory Service Data CLI.

Saat memperbarui grup, Anda harus menyertakan nomor ID direktori dan nama grup Anda. Anda juga harus menyertakan jenis dan atribut pembaruan yang ingin Anda perbarui dalam permintaan Anda, seperti alamat email grup dengan `EmailAddress` parameter. Untuk informasi selengkapnya, lihat [AWS Atribut Directory Service Data](#) dan [Jenis grup dan ruang lingkup grup](#).

- Untuk memperbarui detail grup Microsoft AD AWS Terkelola dengan AWS CLI

Untuk memperbarui detail grup, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori, nama grup, jenis pembaruan, dan atribut dengan ID Direktori Microsoft AD AWS Terkelola, nama grup, dan jenis serta atribut pembaruan yang diinginkan:

```
aws ds-data update-group --directory-id d-1234567890 --sam-account-name "your-group-name" --update-type "REPLACE" --group-scope "global"
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang memperbarui detail grup Microsoft AD AWS Terkelola AWS Tools for PowerShell.

Saat memperbarui grup, Anda harus menyertakan nomor ID direktori dan nama grup Anda. Anda juga harus menyertakan jenis dan atribut pembaruan yang ingin Anda perbarui dalam permintaan Anda, seperti alamat email grup dengan `EmailAddress` parameter. Untuk informasi selengkapnya, lihat [AWS Atribut Directory Service Data](#) dan [Jenis grup dan ruang lingkup grup](#).

- Untuk memperbarui detail grup Microsoft AD AWS Terkelola dengan AWS Tools for PowerShell

Untuk memperbarui detail grup, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori, nama grup, jenis pembaruan, dan atribut dengan ID Direktori Microsoft AD AWS Terkelola, nama grup, dan jenis serta atribut pembaruan yang diinginkan:

```
Update-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name" -  
UpdateType "REPLACE" -GroupScope "global"
```

Menghapus grup iklan Microsoft yang AWS Dikelola

Gunakan prosedur berikut untuk menghapus grup Microsoft AD AWS Terkelola dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Important

Saat Anda menghapus grup, semua informasi tentang grup akan dihapus, termasuk izin apa pun yang diwarisi anggota grup.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola:](#)

[AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

- [Buat grup iklan Microsoft yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat menghapus grup iklan Microsoft yang AWS Dikelola di Konsol Manajemen AWS.

Untuk menghapus grup iklan Microsoft yang AWS Dikelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih grup yang ingin Anda hapus. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup. Anda diarahkan ke layar Detail grup.
6. Pilih Hapus grup. Kotak dialog muncul di mana Anda dapat memilih Konfirmasi untuk menghapus grup.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang menghapus grup AD Microsoft AWS Terkelola dengan AWS Directory Service Data CLI.

Untuk menghapus grup iklan Microsoft yang AWS Dikelola dengan AWS CLI

- Buka AWS CLI, dan jalankan perintah berikut, ganti ID Direktori dan nama grup dengan ID Direktori Microsoft AD AWS Terkelola dan nama grup Anda:

```
aws ds-data delete-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang menghapus grup Microsoft AD AWS Terkelola dengan AWS Tools for PowerShell

Untuk menghapus grup iklan Microsoft yang AWS Dikelola dengan AWS Tools for PowerShell

- Buka PowerShell, dan jalankan perintah berikut, ganti ID Direktori dan nama grup dengan ID Direktori Microsoft AD AWS Terkelola dan nama grup Anda:

```
Remove-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

Menambahkan dan menghapus anggota Microsoft AD yang AWS Dikelola ke grup dan grup ke grup

Dengan [AWS Directory Service Data API](#), anggota dapat menjadi pengguna, grup, atau komputer. Pengguna mewakili orang atau entitas yang dapat mengakses direktori Anda. Grup memungkinkan Anda untuk memberikan dan menolak izin untuk lebih dari satu pengguna pada satu waktu.

Gunakan prosedur berikut untuk menambah atau menghapus pengguna Microsoft AD yang AWS Dikelola ke grup atau grup ke grup lain dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Menambahkan pengguna ke grup

Gunakan prosedur berikut untuk menambahkan pengguna Microsoft AD yang AWS Dikelola ke grup dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

Important

Saat Anda menambahkan pengguna Microsoft AD AWS Terkelola ke grup, pengguna mewarisi peran dan izin yang ditetapkan ke grup. Peran dan izin ini merupakan bagian dari keanggotaan grup pengguna.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).

- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).
- [Buat pengguna Microsoft AD yang AWS Dikelola](#).
- [Buat grup iklan Microsoft yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat menambahkan anggota Microsoft AD yang AWS Dikelola ke grup dengan Konsol Manajemen AWS.

Untuk menambahkan pengguna Microsoft AD yang AWS Dikelola ke grup dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup. Tab menampilkan daftar grup di AWS Region.
5. Pilih grup. Anda diarahkan ke layar Detail grup.
6. Pilih Anggota. Tab menampilkan daftar pengguna dan grup anak menurut jenis anggota di grup Anda.
7. Di bawah tab Anggota, Pilih Tambah anggota.
8. Di bawah Anggota, pilih pengguna yang ingin ditambahkan ke grup, lalu pilih Tambahkan anggota ke grup. Untuk menemukan anggota, masukkan nama log masuk pengguna untuk pengguna dan nama grup untuk grup di kotak pencarian di bawah bagian Anggota.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang menambahkan anggota AD Microsoft AWS Terkelola ke grup dengan AWS Directory Service Data CLI.

Untuk menambahkan pengguna Microsoft AD yang AWS Dikelola ke grup dengan AWS CLI

- Untuk menambahkan pengguna ke grup, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori, grup, dan nama anggota dengan ID Direktori Microsoft AD AWS Terkelola serta nama grup serta anggota:

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang menambahkan anggota Microsoft AD AWS Terkelola ke grup dengan AWS Tools for PowerShell.

Untuk menambahkan pengguna Microsoft AD yang AWS Dikelola ke grup dengan AWS Tools for PowerShell

- Untuk menambahkan pengguna ke grup, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori, grup, dan nama anggota dengan ID Direktori Microsoft AD AWS Terkelola serta nama grup serta anggota:

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -MemberName "jane.doe"
```

Menghapus pengguna dari grup

Dengan [AWS Directory Service Data API](#), anggota dapat menjadi pengguna, grup, atau komputer. Pengguna mewakili orang atau entitas yang dapat mengakses direktori Anda. Grup memungkinkan Anda untuk memberikan dan menolak izin untuk lebih dari satu pengguna pada satu waktu.

Gunakan prosedur berikut untuk menghapus pengguna Microsoft AD yang AWS Dikelola ke grup dengan manajemen pengguna dan grup atau AWS Directory Service Data baik di Konsol Manajemen AWS, AWS CLI, atau AWS Tools for PowerShell.

⚠ Important

Saat Anda menghapus pengguna Microsoft AD AWS Terkelola dari grup, pengguna kehilangan akses ke peran dan izin yang ditetapkan ke grup. Peran dan izin ini adalah bagian dari keanggotaan grup.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).
- [Buat pengguna Microsoft AD yang AWS Dikelola](#).
- [Buat grup iklan Microsoft yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat menghapus anggota Microsoft AD yang AWS Dikelola dari grup dengan Konsol Manajemen AWS.

Untuk menghapus pengguna Microsoft AD yang AWS Dikelola dari grup dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region

3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup. Anda diarahkan ke layar Detail grup.
6. Pilih Anggota. Tab menampilkan daftar pengguna dan grup anak menurut jenis anggota di grup Anda.
7. Pilih pengguna yang ingin Anda hapus dari grup Anda, lalu pilih Hapus. Untuk menemukan pengguna, masukkan nama logon pengguna di kotak pencarian di bawah bagian Anggota.
8. Konfirmasikan bahwa Anda ingin menghapus pengguna dari grup Anda, lalu pilih Hapus lagi.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang menghapus anggota Microsoft AD AWS Terkelola dari grup dengan AWS Directory Service Data CLI.

Untuk menghapus pengguna Microsoft AD yang AWS Dikelola dari grup dengan AWS CLI

- Untuk menghapus pengguna ke grup, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori, grup, dan nama anggota dengan ID Direktori Microsoft AD AWS Terkelola, grup, dan nama anggota:

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang menghapus anggota Microsoft AD AWS Terkelola dari grup dengan AWS Tools for PowerShell.

Untuk menghapus pengguna Microsoft AD yang AWS Dikelola dari grup dengan AWS Tools for PowerShell

- Untuk menghapus pengguna ke grup, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori, grup, dan nama anggota dengan ID Direktori Microsoft AD AWS Terkelola, grup, dan nama anggota:

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -  
MemberName "jane.doe"
```

Menambahkan grup ke grup

Saat Anda menambahkan grup AD Microsoft AWS Terkelola ke grup lain, grup tersebut akan membagikan hubungan orang tua-anak. Grup anak mendapatkan akses ke peran dan izin yang ditetapkan ke grup induk. Anda dapat menambahkan grup anak ke grup dan grup Anda ke grup induk.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).
- [Buat grup iklan Microsoft yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat menambahkan grup AD Microsoft yang AWS Dikelola ke grup dengan Konsol Manajemen AWS.

Untuk menambahkan grup anak ke grup Anda dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region

3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup. Anda diarahkan ke layar Detail grup.
6. Pilih Anggota. Tab menampilkan daftar pengguna dan grup anak menurut jenis anggota di grup Anda.
7. Pilih Tambah anggota.
8. Di bawah Anggota, pilih grup anak yang ingin ditambahkan ke grup, lalu pilih Tambahkan anggota ke grup.

Untuk menambahkan grup induk ke grup dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup. Anda diarahkan ke layar Detail grup.
6. Pilih grup Induk. Tab menampilkan daftar grup yang menjadi anggota grup Anda.
7. Pilih Tambahkan grup induk.
8. Di bawah Grup, pilih grup yang ingin Anda tambahkan grup, lalu pilih Tambah grup induk lagi.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang menambahkan grup AD Microsoft AWS Terkelola ke grup dengan AWS Directory Service Data CLI.

Untuk menambahkan grup anak ke grup Anda dengan AWS CLI

- Untuk menambahkan grup anak ke grup induk, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori, grup, dan nama anggota dengan ID Direktori Microsoft AD AWS Terkelola, grup, dan nama anggota:

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang menambahkan grup AD Microsoft AWS Terkelola ke grup dengan AWS Tools for PowerShell.

Untuk menambahkan grup anak ke grup Anda dengan AWS Tools for PowerShell

- Untuk menambahkan grup anak ke grup induk, buka, dan jalankan perintah berikutPowerShell, ganti ID Direktori, grup, dan nama anggota dengan ID Direktori Microsoft AD AWS Terkelola, grup, dan nama anggota:

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

Menghapus grup dari grup

Saat Anda menghapus grup iklan Microsoft AWS Terkelola dari grup lain, grup tersebut tidak lagi membagikan hubungan orang tua-anak. Grup anak kehilangan akses ke peran dan izin yang ditetapkan ke grup induk. Anda dapat menghapus grup anak dari grup dan grup Anda dari grup induk.

Sebelum Anda memulai salah satu prosedur, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola:](#)

[AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

- [Buat grup iklan Microsoft yang AWS Dikelola](#).

Konsol Manajemen AWS

Anda dapat menghapus grup AD Microsoft yang AWS Dikelola ke grup dengan Konsol Manajemen AWS.

Untuk menghapus grup anak dari grup Anda dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih grup. Anda diarahkan ke layar Detail grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup.
6. Pilih Anggota. Tab menampilkan daftar pengguna dan grup anak menurut jenis anggota di grup Anda.
7. Pilih grup anak yang ingin Anda hapus dari grup, lalu pilih Hapus.
8. Konfirmasikan grup anak yang ingin Anda hapus dari grup, lalu pilih Hapus lagi.

Untuk menghapus grup Anda dari grup induk dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih grup. Anda diarahkan ke layar Detail grup. Untuk menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup.
6. Pilih grup Induk. Tab menampilkan daftar grup yang menjadi anggota grup Anda.
7. Pilih grup induk tempat Anda ingin menghapus grup, lalu pilih Hapus grup induk.

8. Konfirmasikan grup induk tempat Anda ingin menghapus grup, lalu pilih Hapus grup induk lagi.

AWS CLI

Berikut ini menjelaskan cara memformat permintaan yang menghapus grup AD Microsoft AWS Terkelola ke grup dengan AWS Directory Service Data CLI.

- Untuk menghapus grup anak dari grup induk dengan AWS CLI

Untuk menambahkan hapus grup anak dari grup induk, buka, dan jalankan perintah berikut AWS CLI, ganti ID Direktori, grup, dan nama anggota dengan ID Direktori Microsoft AD AWS Terkelola, grup, dan nama anggota:

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS Tools for PowerShell

Berikut ini menjelaskan cara memformat permintaan yang menghapus grup AD Microsoft AWS Terkelola ke grup dengan AWS Tools for PowerShell.

- Untuk menghapus grup anak dari grup induk dengan AWS Tools for PowerShell

Untuk menambahkan hapus grup anak dari grup induk, buka, dan jalankan perintah berikut PowerShell, ganti ID Direktori, grup, dan nama anggota dengan ID Direktori Microsoft AD AWS Terkelola, grup, dan nama anggota:

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

Menyalin keanggotaan grup Microsoft AD AWS Terkelola di Konsol Manajemen AWS

Anda dapat menyalin keanggotaan grup dari satu pengguna Microsoft AD AWS Terkelola ke pengguna lain di. Konsol Manajemen AWS Keanggotaan grup adalah peran dan izin yang diwarisi pengguna saat Anda menambahkannya ke grup.

Sebelum Anda memulai prosedur ini, Anda harus menyelesaikan yang berikut:

- [Membuat Microsoft AD yang AWS Dikelola](#).
- Untuk menggunakan manajemen pengguna dan grup atau AWS Directory Service Data CLI, itu harus diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan manajemen pengguna dan grup atau Directory Service Data](#).
- Anda hanya dapat mengaktifkan fitur ini dari Primer AWS Region untuk direktori Anda. Untuk informasi selengkapnya, lihat [Wilayah Utama vs tambahan](#).
- Anda memerlukan izin IAM yang diperlukan untuk menggunakan AWS Directory Service Data. Untuk informasi selengkapnya, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#). Untuk mulai memberikan izin kepada pengguna dan beban kerja, Anda dapat menggunakan kebijakan AWS terkelola seperti atau. [AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess](#) [AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess](#) Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).
- [Buat grup iklan Microsoft yang AWS Dikelola](#).

Untuk menyalin keanggotaan grup Microsoft AD AWS Terkelola dengan Konsol Manajemen AWS

1. Buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Dari panel navigasi, pilih Active Directory, lalu pilih Direktori. Anda diarahkan ke layar Direktori di mana Anda dapat melihat daftar direktori di. AWS Region
3. Pilih direktori. Anda diarahkan ke layar Detail direktori.
4. Pilih Grup. Tab menampilkan daftar grup di Anda AWS Region.
5. Pilih pengguna yang akunnya ingin Anda salin keanggotaan grup mereka. Untuk menemukan pengguna, masukkan nama login pengguna di kotak pencarian di bawah bagian Pengguna. Anda diarahkan ke layar Detail Pengguna.
6. Pilih Salin semua keanggotaan grup. Anda diarahkan ke prosedur di mana Anda dapat menentukan grup mana yang ingin Anda salin.
 - a. Untuk Verifikasi grup yang akan disalin, di bawah Grup yang akan disalin, pilih grup dengan peran dan izin yang ingin Anda salin, lalu pilih Berikutnya.
 - b. Untuk Pilih akun tujuan, di bawah Jenis akun, pilih Akun pengguna yang ada untuk menyalin keanggotaan grup ke akun pengguna yang ada. Atau, pilih Akun pengguna baru untuk membuat pengguna baru dan menyalin keanggotaan grup ke akun pengguna baru. Untuk

menemukan grup, masukkan nama grup di kotak pencarian di bawah bagian Grup yang dipilih.

- i. (Opsional) Jika Anda memilih Akun pengguna yang ada, pilih akun tujuan tempat Anda ingin menyalin peran dan izin, lalu pilih Berikutnya.
- ii. (Opsional) Jika Anda memilih Akun pengguna baru, selesaikan prosedur, lalu pilih Berikutnya. Untuk informasi tentang membuat pengguna, lihat [Membuat pengguna](#).
- c. Untuk Meninjau dan menyalin keanggotaan grup, tinjau pilihan Anda, lalu pilih Salin keanggotaan grup.

Mengelola pengguna dan grup dengan EC2 instans Amazon

Bagian ini mencakup prosedur untuk mengelola pengguna dan grup dengan EC2 instans Amazon yang bergabung dengan iklan Microsoft AWS Terkelola Anda.

Sebaiknya mengelola pengguna dan grup dengan EC2 instance Amazon jika Directory Service Data API tidak mendukung kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Referensi API AWS Directory Service Data](#).

Note

Sebelum Anda menyelesaikan salah satu prosedur dalam topik berikut, Anda harus menginstal alat administrasi Direktori Aktif. Untuk informasi selengkapnya, lihat [Menginstal alat administrasi Direktori Aktif](#).

Topik

- [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#)
- [Membuat pengguna Microsoft AD yang AWS Dikelola](#)
- [Menghapus akun pengguna dengan EC2 instans Amazon](#)
- [Menyetel ulang kata sandi pengguna Microsoft AD yang AWS Dikelola](#)
- [Membuat grup iklan Microsoft yang AWS Dikelola](#)
- [Menambahkan pengguna Microsoft AD yang AWS Dikelola ke grup](#)

Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola

Anda dapat mengelola Direktori Aktif Microsoft AD AWS Terkelola menggunakan Active Directory Domain Services and Active Directory Lightweight Directory Services Tools. Untuk menggunakannya Active Directory Domain Services and Active Directory Lightweight Directory Services Tools, Anda harus menginstalnya. Prosedur berikut memandu Anda melalui cara menginstal alat ini pada instans Amazon EC2 Windows Server atau dengan PowerShell perintah. Atau, Anda dapat meluncurkan instans EC2 administrasi direktori yang sudah memiliki alat-alat ini diinstal.

EC2 Windows Server instance

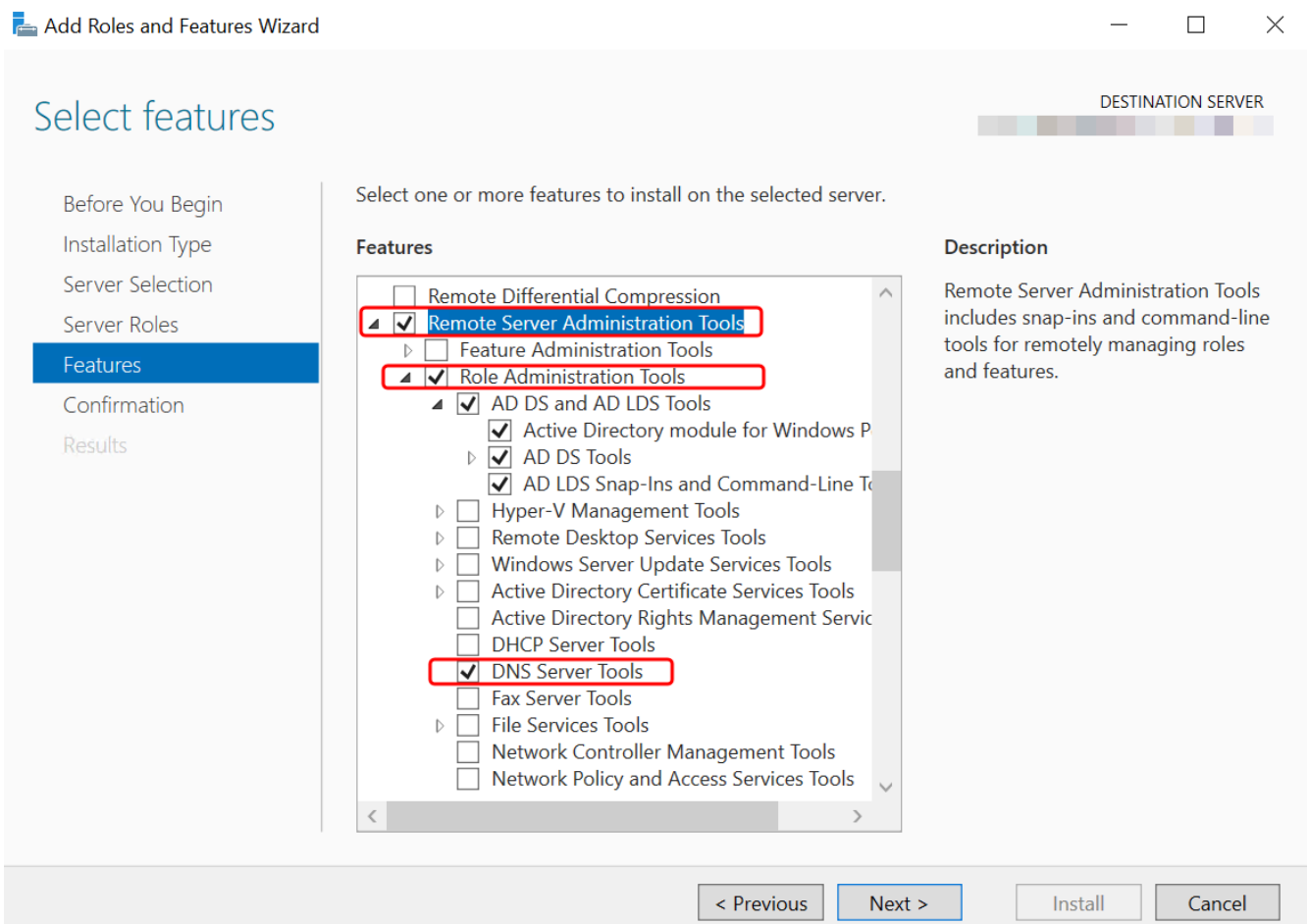
Sebelum Anda dapat memulai prosedur ini, selesaikan yang berikut ini:

1. Buat Direktori Aktif Microsoft AD yang AWS Dikelola. Untuk informasi selengkapnya, lihat [Membuat Microsoft AD yang AWS Dikelola](#).
2. Luncurkan dan gabungkan instans Windows Server EC2 ke Direktori Aktif Microsoft AD AWS Terkelola Anda. Instans EC2 memerlukan kebijakan berikut untuk membuat pengguna dan grup: **AmazonSSManagedInstanceCore** dan **AmazonSSMDirectoryServiceAccess**. Untuk informasi selengkapnya, lihat [Meluncurkan instans administrasi direktori di Direktori Aktif Microsoft AD AWS Terkelola](#) dan [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#).
3. Anda akan memerlukan kredensi untuk Administrator domain Direktori Aktif Anda. Kredensi ini dibuat ketika AD AWS Microsoft yang Dikelola dibuat. Jika Anda mengikuti prosedur di [Membuat Microsoft AD yang AWS Dikelola](#), nama pengguna Administrator Anda menyertakan nama NetBIOS Anda, **corp\admin**

Menginstal alat administrasi Direktori Aktif pada instans Windows Server EC2

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Di konsol Amazon EC2, pilih Instans, pilih instance Windows Server, lalu pilih Connect.
3. Di halaman Connect to instance, pilih klien RDP.
4. Di tab klien RDP, pilih Unduh File Desktop Jarak Jauh, lalu pilih Dapatkan Kata Sandi untuk mengambil kata sandi Anda.
5. Dalam kata sandi Dapatkan Windows, pilih Unggah file kunci pribadi. Pilih file kunci pribadi.pem yang terkait dengan instance Windows Server. Setelah mengunggah file kunci pribadi, pilih Dekripsi kata sandi.

6. Di kotak dialog Keamanan Windows, salin kredensi administrator lokal Anda untuk komputer Windows Server untuk masuk. Nama pengguna dapat dalam format berikut: **NetBIOS-Name\admin** atau **DNS-Name\admin**. Misalnya, **corp\admin** akan menjadi nama pengguna jika Anda mengikuti prosedur di [Membuat Microsoft AD yang AWS Dikelola](#).
7. Setelah masuk ke instance Windows Server, buka Server Manager dari menu Start dengan memilih Server Manager.
8. Di Dasbor Manajer Server, pilih Tambahkan peran dan fitur.
9. Di Tambahkan peran dan fitur Wizard pilih Jenis Instalasi, pilih Instalasi berbasis peran atau berbasis fitur, dan pilih Selanjutnya.
10. Di bawah Pilihan Server, pastikan server lokal dipilih, dan pilih Fitur di panel navigasi sebelah kiri.
11. Di pohon Fitur, pilih dan buka Alat Administrasi Server Jarak Jauh, Alat Administrasi Peran, dan Alat AD DS dan AD LDS. Dengan AD DS dan AD LDS Tools dipilih, modul Active Directory untuk PowerShell, AD DS Tools, dan AD LDS Snap-in dan Command-Line Tools dipilih. Gulir ke bawah dan pilih DNS Server Tools, lalu pilih Berikutnya.



12. Tinjau informasi dan pilih Instal. Ketika instalasi fitur selesai, Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools tersedia dari menu Start di folder Administrative Tools.

PowerShell

Anda dapat menginstal Alat Administrasi Direktori Aktif menggunakan PowerShell. Misalnya, Anda dapat menginstal alat administrasi jarak jauh Active Directory dari PowerShell prompt menggunakan `Install-WindowsFeature RSAT-ADDS`. Untuk informasi selengkapnya, lihat [Menginstal- WindowsFeature](#) di situs web Microsoft.

Directory administration instance

Anda dapat meluncurkan instans EC2 administrasi direktori Konsol Manajemen AWS yang sudah memiliki Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools diinstal dengan mengikuti prosedur di [Meluncurkan instans administrasi direktori di Direktori Aktif Microsoft AD AWS Terkelola](#).

Membuat pengguna Microsoft AD yang AWS Dikelola

Anda dapat membuat pengguna Microsoft AD yang AWS Dikelola dengan Alat Administrasi Direktori Aktif dan PowerShell. Sebelum Anda dapat membuat pengguna dengan Alat Administrasi Direktori Aktif, Anda harus menyelesaikan prosedur di [Menginstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola](#).

Active Directory Administration Tools

Gunakan prosedur berikut untuk membuat pengguna Microsoft AD yang AWS Dikelola dengan Alat Administrasi Direktori Aktif.

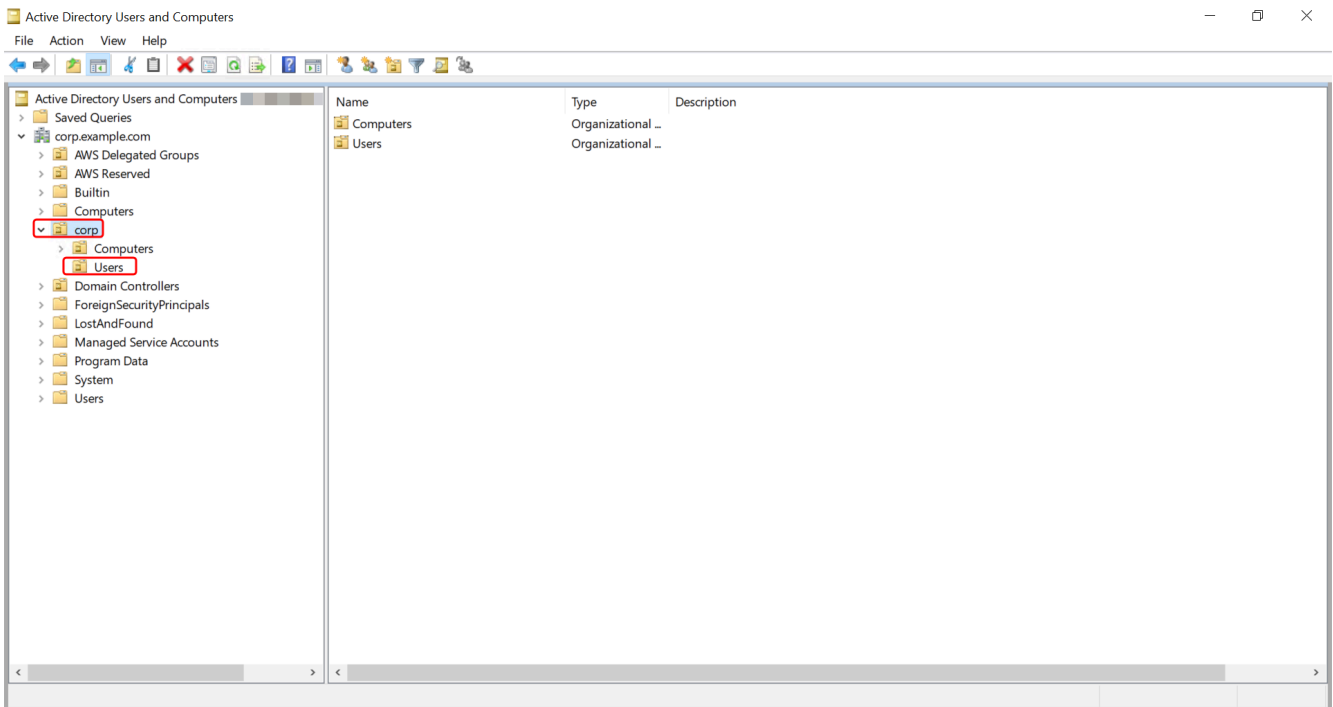
1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif dari menu Start Windows. Ada pintasan ke alat ini yang ditemukan di folder Alat Administratif Windows.

Tip

Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.

```
%SystemRoot%\system32\dsa.msc
```

- Di pohon direktori, pilih OU di bawah nama NetBIOS direktori Anda OU di mana Anda ingin menyimpan pengguna Anda (misalnya, **corp\Users**). Untuk informasi lebih lanjut tentang struktur OU yang digunakan oleh direktori di AWS, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).



- Pada menu Tindakan, pilih Baru, lalu pilih Pengguna untuk membuka wizard pengguna baru.
- Pada halaman pertama wizard, masukkan nilai untuk bidang berikut, lalu pilih Berikutnya.
 - Nama depan
 - Nama belakang
 - Nama logon pengguna
- Pada halaman kedua wizard, masukkan kata sandi sementara di Kata Sandi dan Konfirmasi Kata Sandi. Pastikan pilihan Pengguna harus mengubah kata sandi pada proses masuk berikutnya dipilih. Tidak satu pun dari pilihan lain harus dipilih. Pilih Berikutnya.
- Pada halaman ketiga wizard, verifikasi bahwa informasi pengguna baru sudah benar dan pilih Selesai. Pengguna baru akan muncul di folder Pengguna.

PowerShell

Gunakan prosedur berikut untuk membuat pengguna Microsoft AD yang AWS Dikelola dengan PowerShell.

1. Connect ke instance yang bergabung dengan domain Active Directory Anda sebagai administrator Active Directory.
2. Buka PowerShell.
3. Ketik perintah berikut mengganti nama pengguna **jane.doe** dengan nama pengguna pengguna yang ingin Anda buat. Anda akan diminta PowerShell untuk memberikan kata sandi untuk pengguna baru. Untuk informasi selengkapnya tentang persyaratan kompleksitas kata sandi Direktori Aktif, lihat [Microsoft dokumentasi](#). Untuk informasi selengkapnya tentang ADUser perintah New-, lihat [Microsoft dokumentasi](#).

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -  
AsSecureString 'Password')
```

Menghapus akun pengguna dengan EC2 instans Amazon

Anda dapat menggunakan prosedur berikut untuk menghapus pengguna dengan EC2 instans Amazon yang bergabung dengan iklan Microsoft AWS Terkelola Anda.

Note

Sebelum Anda menyelesaikan prosedur ini, Anda harus menginstal alat administrasi Direktori Aktif. Untuk informasi selengkapnya, lihat [Menginstal alat administrasi Direktori Aktif](#).

Untuk menghapus kluster

1. Buka alat Pengguna dan Komputer Direktori Aktif. Ada pintasan ke alat ini di folder Alat Administratif Windows.

Tip

Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.

```
%SystemRoot%\system32\dsa.msc
```

2. Di pohon direktori, pilih OU yang berisi pengguna yang ingin Anda hapus (misalnya, Corp\Users).
3. Pilih pengguna yang ingin Anda hapus. Pada menu Tindakan, pilih Hapus.
4. Kotak dialog akan muncul meminta Anda untuk mengonfirmasi bahwa Anda ingin menghapus pengguna. Pilih Ya untuk menghapus pengguna.

Pengguna yang dihapus disimpan sementara di Tempat Sampah AD. Untuk informasi selengkapnya tentang Tempat Sampah Daur [Ulang AD, lihat Tempat Sampah AD: Memahami, Menerapkan, Praktik Terbaik, dan Pemecahan Masalah di blog Tim](#) Layanan Ask the Directory Microsoft.

Menyetel ulang kata sandi pengguna Microsoft AD yang AWS Dikelola

Pengguna harus mematuhi kebijakan kata sandi sebagaimana didefinisikan dalam Direktori Aktif. Terkadang ini bisa mendapatkan yang terbaik dari pengguna, termasuk administrator Direktori Aktif, dan mereka lupa kata sandi mereka. Ketika ini terjadi, Anda dapat dengan cepat mengatur ulang kata sandi pengguna menggunakan Directory Service jika pengguna berada di Microsoft AD yang AWS Dikelola.

Anda harus masuk sebagai pengguna dengan izin yang diperlukan untuk mengatur ulang kata sandi. Untuk informasi selengkapnya tentang izin, lihat [Ikhtisar mengelola izin akses ke sumber daya Anda Directory Service](#).

Anda dapat mengatur ulang kata sandi untuk setiap pengguna di Direktori Aktif Anda dengan pengecualian berikut:

- Anda dapat mengatur ulang kata sandi untuk setiap pengguna dalam Unit Organisasi (OU) yang didasarkan dari nama NetBIOS yang Anda gunakan saat Anda membuat Direktori Aktif Anda. Misalnya, jika Anda mengikuti prosedur dalam nama NetBIOS [Membuat Microsoft AD yang AWS Dikelola](#) Anda akan menjadi CORP dan kata sandi pengguna yang dapat Anda atur ulang akan menjadi anggota OU. Corp/Users
- Anda tidak dapat mengatur ulang kata sandi pengguna mana pun di luar OU yang didasarkan pada nama NetBIOS yang Anda gunakan saat membuat Direktori Aktif Anda. Misalnya, Anda tidak dapat mengatur ulang kata sandi untuk pengguna di OU AWS Cadangan. Untuk informasi selengkapnya

tentang struktur OU untuk Microsoft AD yang AWS Dikelola, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).

Untuk informasi selengkapnya tentang cara kebijakan kata sandi diterapkan saat kata sandi disetel ulang di Microsoft AD yang AWS Dikelola, lihat [Bagaimana kebijakan kata sandi diterapkan](#).

Anda dapat menggunakan salah satu alat berikut untuk mengatur ulang kata sandi pengguna Microsoft AD yang AWS Dikelola:

- Konsol Manajemen AWS
- AWS CLI
- PowerShell

Konsol Manajemen AWS

Gunakan prosedur berikut untuk mengatur ulang kata sandi pengguna Microsoft AD yang AWS Dikelola dengan Konsol Manajemen AWS.

1. Di panel navigasi [Directory Service konsol](#), di bawah Direktori Aktif, pilih Direktori, lalu pilih Direktori Aktif dalam daftar tempat Anda ingin mengatur ulang kata sandi pengguna.
2. Pada halaman Detail direktori, pilih Tindakan, lalu pilih Setel ulang kata sandi pengguna.
3. Dalam dialog Reset kata sandi pengguna, di Nama pengguna ketikkan nama pengguna pengguna yang kata sandinya perlu diubah.
4. Ketik kata sandi di Kata sandi baru dan Konfirmasi kata sandi, lalu pilih Atur ulang sandi.

AWS CLI

Gunakan prosedur berikut untuk mengatur ulang kata sandi pengguna Microsoft AD yang AWS Dikelola dengan AWS CLI.

1. Untuk menginstal AWS CLI, lihat [Menginstal atau memperbarui versi terbaru AWS CLI](#).
2. Buka AWS CLI.
3. Ketik perintah berikut dan ganti ID Direktori, nama pengguna **jane.doe**, dan kata sandi **Pa\$\$w0rd** dengan ID Direktori Direktori Aktif dan kredensial yang diinginkan. Lihat [reset-user-password](#) di Referensi AWS CLI Perintah untuk informasi lebih lanjut.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

PowerShell

Gunakan prosedur berikut untuk mengatur ulang kata sandi pengguna Microsoft AD yang AWS Dikelola dengan PowerShell.

1. Connect ke instance yang bergabung dengan domain Active Directory Anda sebagai administrator Active Directory.
2. Buka PowerShell.
3. Ketik perintah berikut mengganti nama pengguna **jane.doe**, ID Direktori, dan kata sandi **P@ssw0rd** dengan ID Direktori Direktori Aktif dan kredensial yang diinginkan. Lihat [Reset-Cmdlet DSUser Kata Sandi untuk informasi](#) selengkapnya.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword "P@ssw0rd"
```

Membuat grup iklan Microsoft yang AWS Dikelola

Anda dapat membuat grup di Microsoft AD yang AWS Dikelola. Gunakan prosedur berikut untuk membuat grup keamanan dengan EC2 instans Amazon yang digabungkan ke direktori AD Microsoft AWS Terkelola Anda. Sebelum Anda dapat membuat grup keamanan, Anda harus menyelesaikan prosedur di [Menginstal Alat Administrasi Direktori Aktif](#).

Active Directory Administration Tools

Gunakan prosedur berikut untuk membuat grup AD Microsoft AWS Terkelola dengan Alat Administrasi Direktori Aktif.

Untuk membuat grup

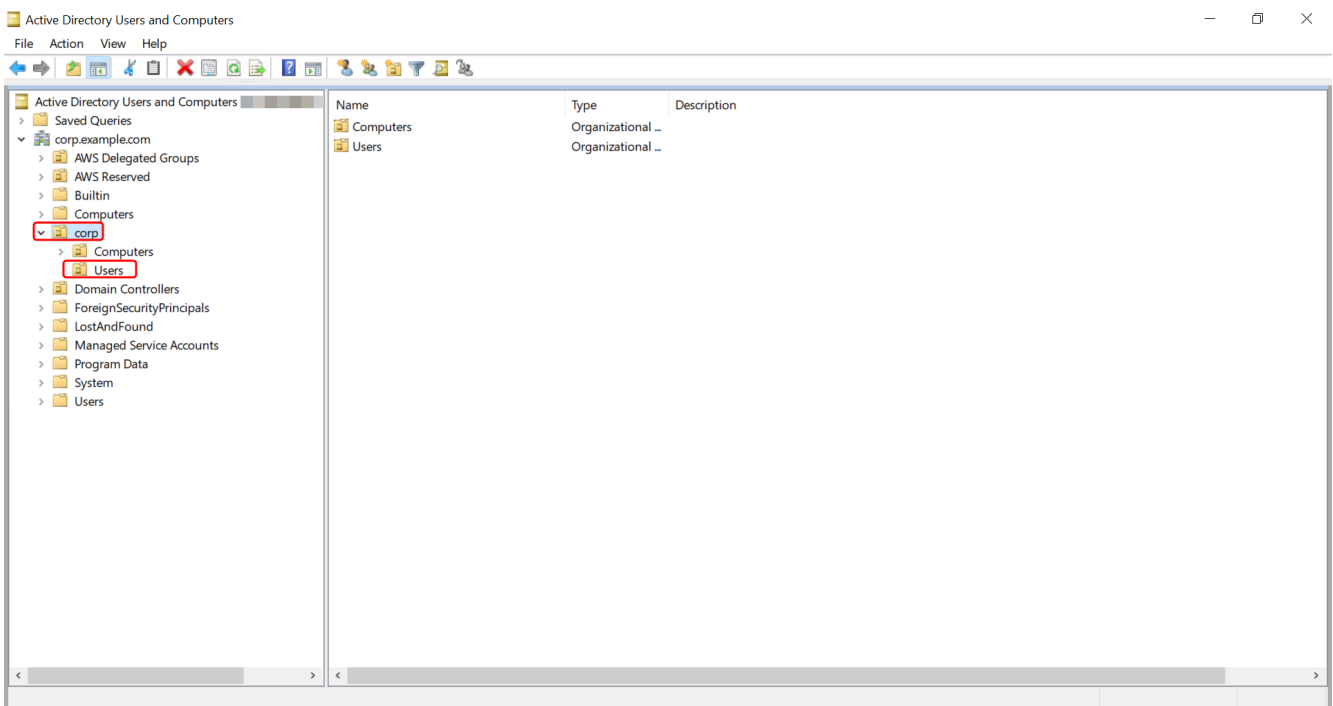
1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif. Ada jalan pintas untuk alat ini di folder Alat Administratif.

Tip

Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.

```
%SystemRoot%\system32\dsa.msc
```

3. Pada pohon direktori, pilih OU di bawah direktori OU nama NetBIOS Anda di mana Anda ingin menyimpan grup Anda (misalnya, Corp\Users). Untuk informasi lebih lanjut tentang struktur OU yang digunakan oleh direktori di AWS, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).



4. Pada menu Tindakan, klik Baru, dan kemudian klik Grup untuk membuka wizard grup baru.
5. Ketik nama untuk grup di Nama grup, pilih lingkup Grup yang memenuhi kebutuhan Anda, dan pilih Keamanan untuk jenis Grup. Untuk informasi selengkapnya tentang lingkup grup Active Directory dan grup keamanan, lihat [Grup keamanan Active Directory](#) di dokumentasi Microsoft Windows Server.
6. Klik OK. Grup keamanan baru akan muncul di folder Pengguna.

PowerShell

Anda dapat menggunakan PowerShell perintah untuk membuat grup. Untuk informasi selengkapnya, lihat [New- ADGroup](#) di PowerShell dokumentasi Windows Server 2022.

Menambahkan pengguna Microsoft AD yang AWS Dikelola ke grup

Anda dapat menambahkan pengguna Microsoft AD yang AWS Dikelola ke grup. Gunakan prosedur berikut untuk menambahkan pengguna ke grup keamanan dengan EC2 instans Amazon yang digabungkan ke direktori AD Microsoft AWS Terkelola Anda.

Active Directory Administration Tools

Untuk menambahkan pengguna ke grup

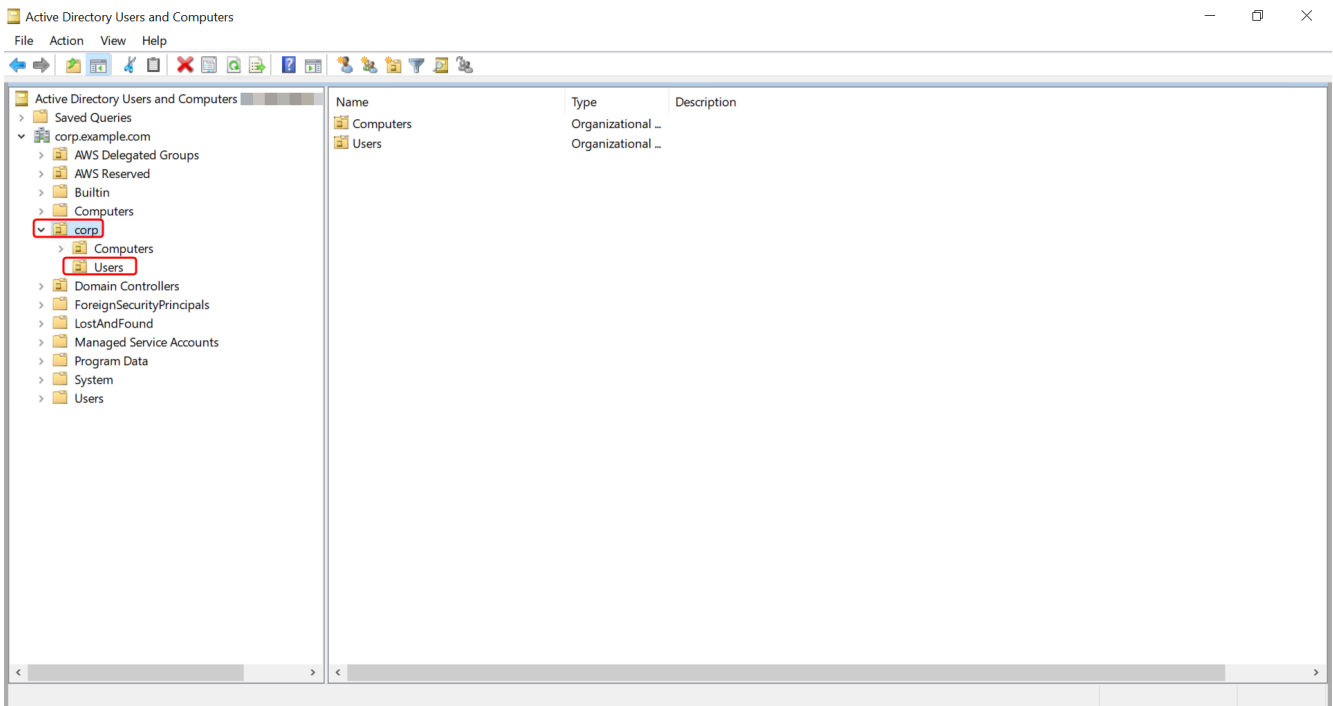
1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif. Ada jalan pintas untuk alat ini di folder Alat Administratif.

Tip

Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.

```
%SystemRoot%\system32\dsa.msc
```

3. Pada pohon direktori, pilih OU di bawah direktori Anda NetBIOS nama OU di mana Anda disimpan grup Anda, dan pilih grup yang Anda ingin tambahkan pengguna sebagai anggota.



4. Pada menu Tindakan, klik Properti untuk membuka kotak dialog properti untuk grup.
5. Pilih tab Anggota dan klik Tambahkan.
6. Untuk Masukkan nama objek yang akan dipilih, ketik nama pengguna yang ingin Anda tambahkan dan klik OK. Nama akan ditampilkan dalam daftar Anggota. Klik OK lagi untuk memperbarui keanggotaan grup.
7. Verifikasikan bahwa pengguna tersebut sekarang adalah anggota grup dengan memilih pengguna di folder Pengguna dan klik Properti di menu Tindakan untuk membuka kotak dialog properti. Pilih tab Anggota dari. Anda harus melihat nama grup dalam daftar grup yang dimiliki pengguna.

AWS Directory Service Data

AWS Directory Service Data adalah perpanjangan dari AWS Directory Service. Anda dapat membuat, membaca, memperbarui, dan pengguna, grup, dan keanggotaan Active Directory (AD) dari AWS Directory Service untuk Microsoft Active Directory tanpa menerapkan instans manajemen AD khusus pada instans Amazon. EC2 Anda juga dapat melakukan tugas manajemen objek bawaan di seluruh direktori tanpa konektivitas jaringan langsung. Ini menyederhanakan penyediaan dan manajemen akses untuk mencapai penerapan yang sepenuhnya otomatis. Untuk informasi selengkapnya, lihat [Referensi API AWS Directory Service Data](#).

Directory Service Data mendukung operasi penulisan pengguna dan grup, seperti `CreateUser` dan `CreateGroup`, dalam Microsoft AD AWS Terkelola yang ada di unit organisasi (OU) Anda. Directory Service Data mendukung operasi baca, suka `ListUsers` dan `ListGroups`, pada semua pengguna, grup, dan keanggotaan grup dalam AD Microsoft AWS Terkelola dan di seluruh dunia tepercaya. Directory Service Data mendukung penambahan dan penghapusan anggota grup dari grup di OU dan OU Grup AWS Delegasi, sehingga Anda dapat mendelegasikan izin dengan menambahkan pengguna ke objek grup tertentu yang didelegasikan. Untuk informasi selengkapnya, lihat [Manajemen pengguna dan grup di Microsoft AD yang AWS Dikelola](#).

Note

Directory Service Data hanya tersedia di Wilayah Utama Anda. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).

Topik

- [Replikasi dan konsistensi](#)
- [AWS Atribut Directory Service Data](#)
- [Jenis grup dan ruang lingkup grup](#)

Replikasi dan konsistensi

Directory Service Data API terhubung ke pengontrol domain Microsoft AD AWS Terkelola untuk melakukan operasi pada objek direktori yang mendasarinya. Active Directory adalah platform yang akhirnya konsisten, dan replikasi terus terjadi antara pengontrol domain Directory Service direktori. Secara default, setiap Directory Service direktori dibuat dengan dua pengontrol domain.

Directory Service Data mencoba mempertahankan pengalaman yang konsisten dengan memanfaatkan pengontrol domain yang sama di seluruh permintaan. Jika kontroler domain tidak tersedia, Directory Service Data beralih ke pengontrol domain alternatif. Selama peristiwa ini, Anda mungkin melihat konsistensi pada akhirnya di seluruh pengontrol domain saat objek direplikasi di seluruh pengontrol domain.

Batas direktori bervariasi menurut edisi Microsoft AD yang AWS Dikelola:

- Edisi standar — Mendukung 8 transaksi per detik untuk operasi baca dan 4 TPS untuk operasi tulis per direktori.

- Edisi perusahaan — Mendukung 16 transaksi per detik untuk operasi baca dan 8 TPS untuk operasi tulis per direktori.

 Note

Ada batas konkurensi 10 permintaan bersamaan untuk edisi Standard dan Enterprise.

- Akun AWS— Mendukung total 100 transaksi per detik untuk operasi Directory Service Data di semua direktori.

AWS Atribut Directory Service Data

Topik ini menjelaskan cara bekerja dengan atribut di [Referensi API AWS Directory Service Data](#).

Minta Atribut

Atribut berikut harus didefinisikan dalam parameter badan permintaan. Untuk contoh cara mendefinisikan atribut ini, lihat [CreateGroup](#) di Referensi API AWS Directory Service Data.

Nama atribut Directory Service Data	Nama tampilan LDAP	Konsol Manajemer AWS	PowerShell alias	Jenis akses	Jenis objek	Nilai atribut	Dapat dicari
DistinguishedName	distingui shedName	Nama terhormat	Tidak ada	ReadOnly	Pengguna, Grup	String	Tidak
EmailAddress	pos	Alamat Email	EmailAddress	Dapat dibuat	Pengguna	Tali	Ya
Diaktifkan	Tidak ada	Diaktifkan	Diaktifkan	bisa berubah	Pengguna	Boolean	Tidak
GivenName	givenName	Nama Depan	GivenName	Dapat dibuat	Pengguna	Tali	Ya

Nama atribut Directory Service Data	Nama tampilan LDAP	Konsol Manajemer AWS	PowerShell alias	Jenis akses	Jenis objek	Nilai atribut	Dapat dicari
GroupScope	GroupScope	Lingkup grup	Tidak ada	Dapat dibuat	Kelompok	Enum	Tidak
GroupType	GroupType	Jenis grup	Tidak ada	Dapat dibuat	Kelompok	Enum	Tidak
SamAccountName	sAMAccountName	Nama masuk pengguna	sAMAccountName	Dapat dibuat	Pengguna, Grup	Tali	Ya
SID	ObjectSID	Pengidentifikasi keamanan pengguna/grup (SID)	SID	ReadOnly	Pengguna, Grup	String	Tidak
Nama keluarga	sn	Nama belakang	Nama keluarga	Dapat dibuat	Pengguna	Tali	Ya
UserPrincipalName	userPrincipalName	Nama utama pengguna	UserPrincipalName	ReadOnly	Pengguna	String	Tidak

Atribut Lainnya

Atribut berikut harus didefinisikan `OtherAttributes` dan tidak dipetakan ke parameter badan permintaan apa pun. Ketika Anda menentukan atribut lain dalam permintaan Anda, Anda harus menentukan nama atribut, tipe data, dan nilai untuk setiap atribut. Untuk contoh cara mendefinisikan atribut ini, lihat [CreateUser](#) di Referensi API AWS Directory Service Data.

Note

Nama-nama atribut ini tidak peka huruf besar/kecil bila diberikan sebagai input dan setara dengan nama tampilan LDAP.

Nama atribut Directory Service Data	Nama tampilan LDAP	Konsol Manajemer AWS	PowerShell alias	Jenis akses	Jenis objek	Nilai atribut	Dapat dicari
Asisten	asisten	Asisten	Tidak ada	ReadOnly	Pengguna	String	Tidak
Cn	cn	Nama Umum	Tidak ada	ReadOnly	Pengguna, Grup	String	Tidak
Co	co	Negara/wilayah	Negara	bisa berubah	Pengguna	String	Tidak
Perusahaan	perusahaan	Perusahaan	Perusahaan	Dapat dibuat	Pengguna	String	Tidak
Departemen	departemen	Departemen	Departemen	Dapat dibuat	Pengguna	String	Tidak
Deskripsi	deskripsi	Deskripsi	Deskripsi	Dapat dibuat	Pengguna, Grup	String	Tidak
DirectReports	DirectReports	Laporan langsung	Tidak ada	ReadOnly	Pengguna	Set string	Tidak
DisplayName	displayName	Nama tampilan	DisplayName	Dapat dibuat	Pengguna, Grup	Tali	Ya

Nama atribut Directory Service Data	Nama tampilan LDAP	Konsol Manajemer AWS	PowerShell alias	Jenis akses	Jenis objek	Nilai atribut	Dapat dicari
Facsimile Telephone Number	facsimile Telephone Number	Faks	Faks	Dapat dibuat	Pengguna, Grup	String	Tidak
HomePhone	HomeTelephon	Nomor telepon rumah	HomePhon	Dapat dibuat	Pengguna	String	Tidak
Info	info	Catatan	Tidak ada	bisa berubah	Pengguna, Grup	String	Tidak
Inisial	inisial	Inisial	Inisial	bisa berubah	Pengguna	String	Tidak
IpPhone	IPPhone	Telepon IP	Tidak ada	bisa berubah	Pengguna	String	Tidak
L	I	Kota	Kota	Dapat dibuat	Pengguna	Tali	Ya
Manajer	manajer	pengelola	pengelola	bisa berubah	Pengguna	String	Tidak
Surat	pos	Alamat Email	EmailAddress	bisa berubah	Kelompok	Tali	Ya
Ponsel	seluler	Nomor ponsel	MobilePhone	bisa berubah	Pengguna	String	Tidak
ObjectClasses	ObjectClasses	Pengguna/Grup	Tidak ada	ReadOnly	Kelompok	String	Tidak

Nama atribut Directory Service Data	Nama tampilan LDAP	Konsol Manajemer AWS	PowerShell alias	Jenis akses	Jenis objek	Nilai atribut	Dapat dicari
ObjectGUID	ObjectGUID	Pengidentifikasi unik global (GUID)	Tidak ada	ReadOnly	Pengguna, Grup	String	Tidak
Pager	pager	Pager	Tidak ada	bisa berubah	Pengguna	String	Tidak
PhysicalDeliveryOfficeName	physicalDeliveryOfficeName	Kantor	Tidak ada	Dapat dibuat	Pengguna	Tali	Ya
PostalCode	Kode Pos	Zip/Kode Pos	PostalCode	Dapat dibuat	Pengguna	String	Tidak
PreferredLanguage	DiutamakanBahasa	Bahasa pilihan	Tidak ada	bisa berubah	Pengguna	String	Tidak
ProxyAddresses	ProxyAddress	Alamat proxy	Tidak ada	ReadOnly	Pengguna, Grup	String multi-nilai	Ya
ServicePrincipalName	servicePrincipalName	Nama utama layanan	ServicePrincipalName	bisa berubah	Pengguna	String multi-nilai	Tidak
State	st	Negara Bagian/Provinsi	Status	Dapat dibuat	Pengguna	String	Tidak
StreetAddress	Alamat Jalan	Alamat jalan	StreetAddress	Dapat dibuat	Pengguna	String	Tidak

Nama atribut Directory Service Data	Nama tampilan LDAP	Konsol Manajemer AWS	PowerShell alias	Jenis akses	Jenis objek	Nilai atribut	Dapat dicari
Telephone Number	Telephone number	Nomor telepon	OfficePhone	Dapat dibuat	Pengguna	String	Tidak
Judul	title	Judul pekerjaan	judul	bisa berubah	Pengguna	String	Tidak
WhenChanged	Ketika Berubah	Terakhir diperbarui	Tidak ada	ReadOnly	Pengguna, Grup	String	Tidak
WWWHome	WWWHome	URL halaman rumah	WWWHome	bisa berubah	Pengguna, Grup	String	Tidak

Jenis grup dan ruang lingkup grup

Grup di Microsoft AD yang AWS Dikelola memiliki jenis grup dan cakupan grup. Lihat bagian berikut untuk informasi lebih lanjut tentang masing-masing.

Topik

- [Jenis grup](#)
- [Lingkup grup](#)

Jenis grup

Jenis grup menentukan sumber daya bersama dalam Direktori Aktif yang dapat diakses anggota grup. Ada dua jenis kelompok:

- Keamanan - Anda dapat menetapkan izin ke grup ini sehingga anggota grup dapat mengakses sumber daya Direktori Aktif bersama.

- Distribusi - Anda dapat menggunakan jenis ini untuk membuat daftar distribusi email. Anggota grup ini tidak dapat mengakses sumber daya bersama Direktori Aktif.

Tidak ada batasan saat mengubah antar tipe grup.

Untuk informasi selengkapnya tentang jenis grup, lihat [dokumentasi Microsoft](#).

Lingkup grup

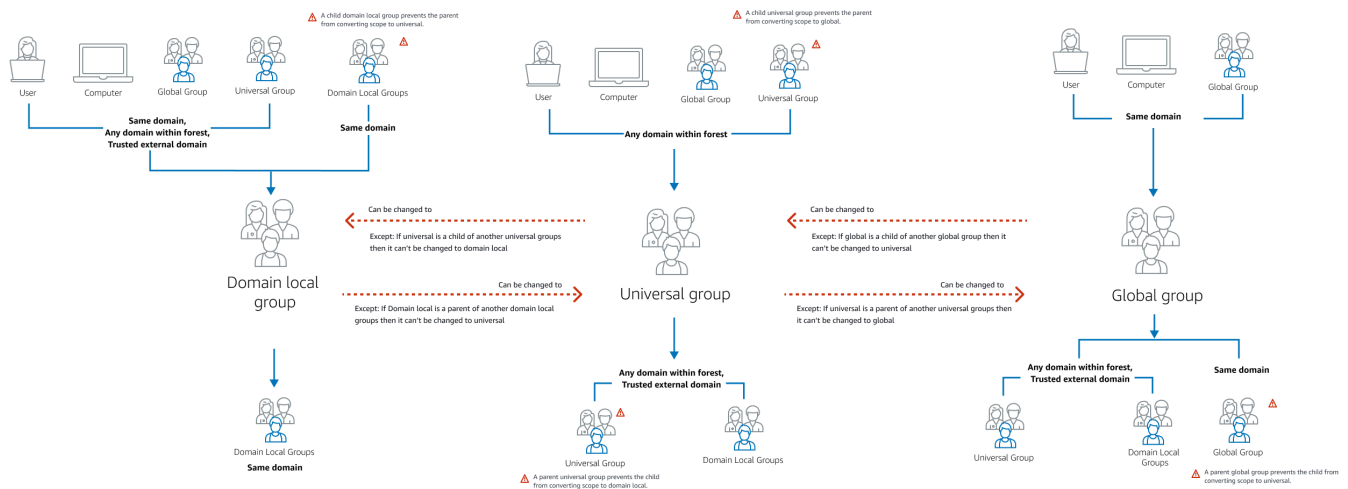
Lingkup grup menentukan bagaimana anggota grup didefinisikan dengan pohon domain atau hutan. Ada tiga lingkup kelompok:

- Domain lokal - untuk menetapkan izin kepada anggota grup yang terletak di domain yang sama.
- Universal - untuk menetapkan izin kepada anggota grup yang berada dalam domain apa pun.
- Global - untuk menetapkan izin kepada anggota grup yang berada dalam domain atau hutan apa pun.

Ada batasan saat mengubah ruang lingkup grup. Daftar dan diagram berikut menguraikan keterbatasan ini.

- Mengubah cakupan grup dari Domain Lokal ke Universal - Ya
 - Kecuali jika grup lokal domain adalah induk dari grup lokal domain lain.
- Mengubah cakupan grup dari Universal ke Domain Lokal - Ya
 - Kecuali jika kelompok universal adalah kelompok anak dari kelompok universal lain.
- Mengubah cakupan grup dari Universal ke Global - Ya
 - Kecuali jika kelompok universal adalah induk dari kelompok universal lainnya.
- Mengubah cakupan grup dari Global ke Universal - Ya
 - Kecuali jika kelompok global adalah anak dari kelompok global lain.

Untuk informasi selengkapnya tentang cakupan grup, lihat [Microsoft dokumentasi](#).



Menghubungkan Microsoft AD yang AWS Dikelola ke Microsoft Entra Connect Sync

Tutorial ini memandu Anda melalui langkah-langkah yang diperlukan untuk menginstal [Microsoft Entra Connect Sync](#) untuk menyinkronkan Anda [Microsoft Entra ID](#) ke Microsoft AD yang AWS Dikelola.

Dalam tutorial ini, Anda akan melakukan hal-hal berikut:

1. Buat pengguna domain Microsoft AD yang AWS Dikelola.
2. Unduh Entra Connect Sync.
3. Gunakan PowerShell untuk menjalankan skrip untuk memberikan izin yang sesuai untuk pengguna yang baru dibuat.
4. Instal Entra Connect Sync.

Prasyarat

Anda akan memerlukan yang berikut untuk menyelesaikan tutorial ini:

- Iklan Microsoft yang AWS Dikelola. Untuk informasi selengkapnya, lihat [the section called "Membuat Microsoft AD yang AWS Dikelola"](#).
- Instans Windows Server Amazon EC2 bergabung dengan iklan AWS Microsoft Terkelola Anda. Untuk informasi selengkapnya, lihat [Bergabung dengan instance Windows](#).

- WindowsServer EC2 dengan Direktori Aktif Administration Tools diinstal untuk mengelola iklan Microsoft AWS Terkelola Anda. Untuk informasi selengkapnya, lihat [the section called “Menginstal Alat Administrasi AD”](#).

Buat pengguna domain Active Directory

Tutorial ini mengasumsikan Anda sudah memiliki AWS Managed Microsoft AD serta instance EC2 Windows Server dengan Active Directory Administration Tools diinstal. Untuk informasi selengkapnya, lihat [the section called “Menginstal Alat Administrasi AD”](#).

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buat pengguna domain Microsoft AD yang AWS Dikelola. Pengguna ini akan menjadi Active Directory Directory Service (AD DS) Connector account untuk Entra Connect Sync. Untuk langkah-langkah rinci tentang proses ini, lihat [the section called “Membuat pengguna”](#).

Unduh Entra Connect Sync

- Unduh Entra Connect Sync dari [Microsoft situs web](#) ke instans EC2 yang merupakan admin Microsoft AD yang AWS Dikelola.

Warning

Jangan buka atau jalankan Entra Connect Sync pada saat ini. Langkah selanjutnya akan memberikan izin yang diperlukan untuk pengguna domain Anda yang dibuat di Langkah 1.

Jalankan PowerShell Script

- [Buka PowerShell sebagai Administrator](#) dan jalankan skrip berikut.

Saat skrip sedang berjalan, Anda akan diminta untuk memasukkan [AMAccountName s](#) untuk pengguna domain yang baru dibuat dari Langkah 1.

Note

Lihat berikut ini untuk informasi selengkapnya tentang menjalankan skrip:

- Anda dapat menyimpan skrip dengan ps1 ekstensi ke folder seperti **temp**. Kemudian, Anda dapat menggunakan PowerShell perintah berikut untuk memuat skrip:

```
import-module "c:\temp\entra.ps1"
```

- Setelah memuat skrip, Anda dapat menggunakan perintah berikut untuk mengatur izin yang diperlukan untuk menjalankan skrip, mengganti *Entra_Service_Account_Name* dengan nama akun Entra layanan Anda:

```
Set-EntraConnectSvcPerms -ServiceAccountName Entra_Service_Account_Name
```

```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig\AdSyncConfig.psm1"
```

```
try {  
    # Attempt to import the module  
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."  
    Import-Module $modulePath -ErrorAction Stop  
    Write-Host -ForegroundColor Green "Success!"  
}  
catch {  
    # Display the exception message  
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"  
}
```

```
Function Set-EntraConnectSvcPerms {  
    [CmdletBinding()]  
    Param (  
        [String]$ServiceAccountName  
    )  
  
    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator  
  
    Try {  
        $Domain = Get-ADDomain -ErrorAction Stop  
    } Catch [System.Exception] {  
        Write-Output "Failed to get AD domain information $_"  
    }  
}
```

```

$BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
$Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'

Try {
    $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
'DistinguishedName'
} Catch [System.Exception] {
    Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
}

Try {
    $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
Stop | Select-Object -ExpandProperty 'DistinguishedName'
} Catch [System.Exception] {
    Write-Output "Failed to get service account DN $_"
}

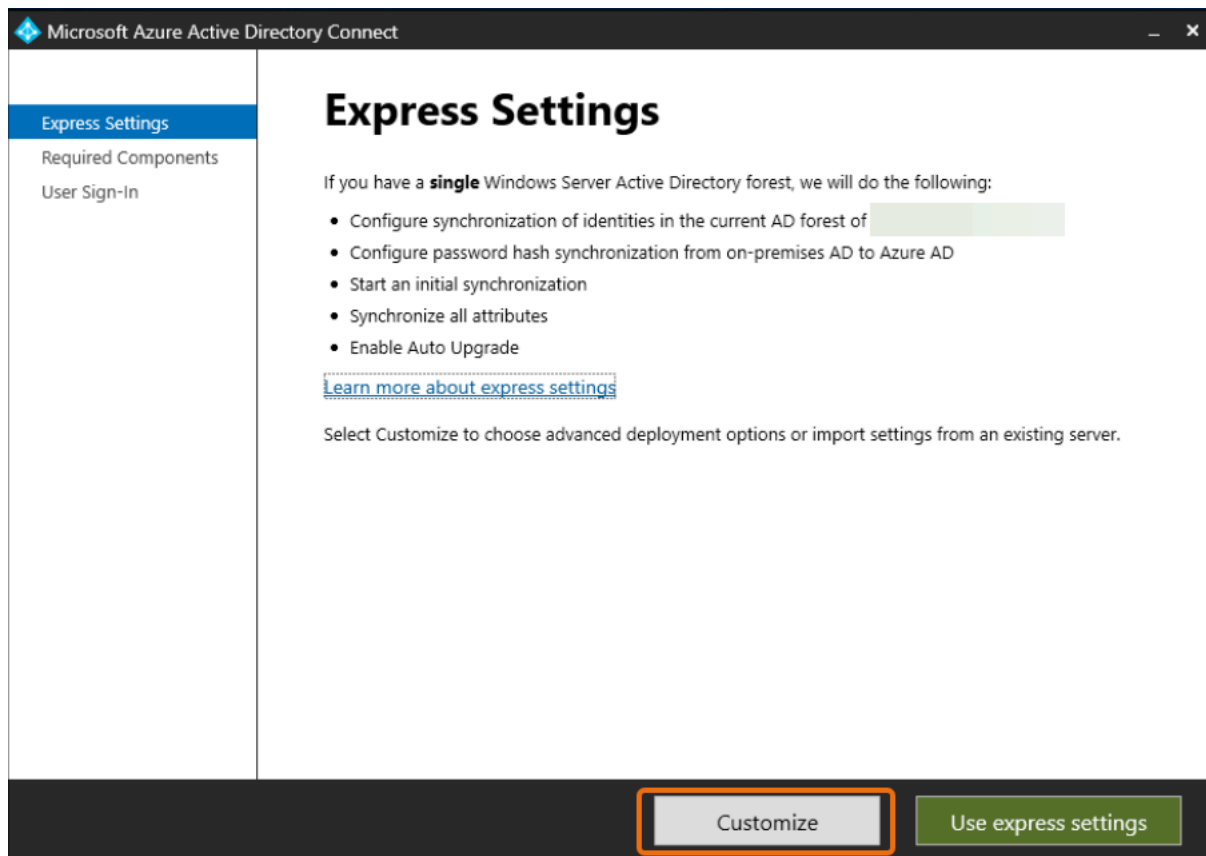
Foreach ($OU in $OUs) {
    try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
$ADConnectorAccountDN -ADObjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

        Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADObjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
on OU $OU"
    }
    catch {
        Write-Host "An error occurred while setting permissions for
$ADConnectorAccountDN on OU $OU : $_"
    }
}
}

```

Instal Entra Connect Sync

1. Setelah skrip selesai, Anda dapat menjalankan file konfigurasi yang diunduh Microsoft Entra Connect (sebelumnya dikenal sebagai Azure Active Directory Connect).
2. Sebuah Microsoft Azure Active Directory Connect jendela terbuka setelah menjalankan file konfigurasi dari langkah sebelumnya. Pada jendela Pengaturan Ekspres, pilih Sesuaikan.



3. Pada jendela Instal komponen yang diperlukan, pilih kotak centang Gunakan akun layanan yang ada. Di NAMA AKUN LAYANAN dan KATA SANDI AKUN LAYANAN, masukkan AD DS Connector account nama dan kata sandi untuk pengguna yang Anda buat di Langkah 1. Misalnya, jika AD DS Connector account nama Anda `entra`, nama akun akan menjadi `corp\entra`. Kemudian pilih Instal.

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In

Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. ?

☐ Specify a custom installation location

☐ Use an existing SQL Server

☒ Use an existing service account

☐ Managed Service Account

☒ Domain Account

SERVICE ACCOUNT NAME

corp\entra

SERVICE ACCOUNT PASSWORD

.....

☐ Specify custom sync groups

☐ Import synchronization settings ?

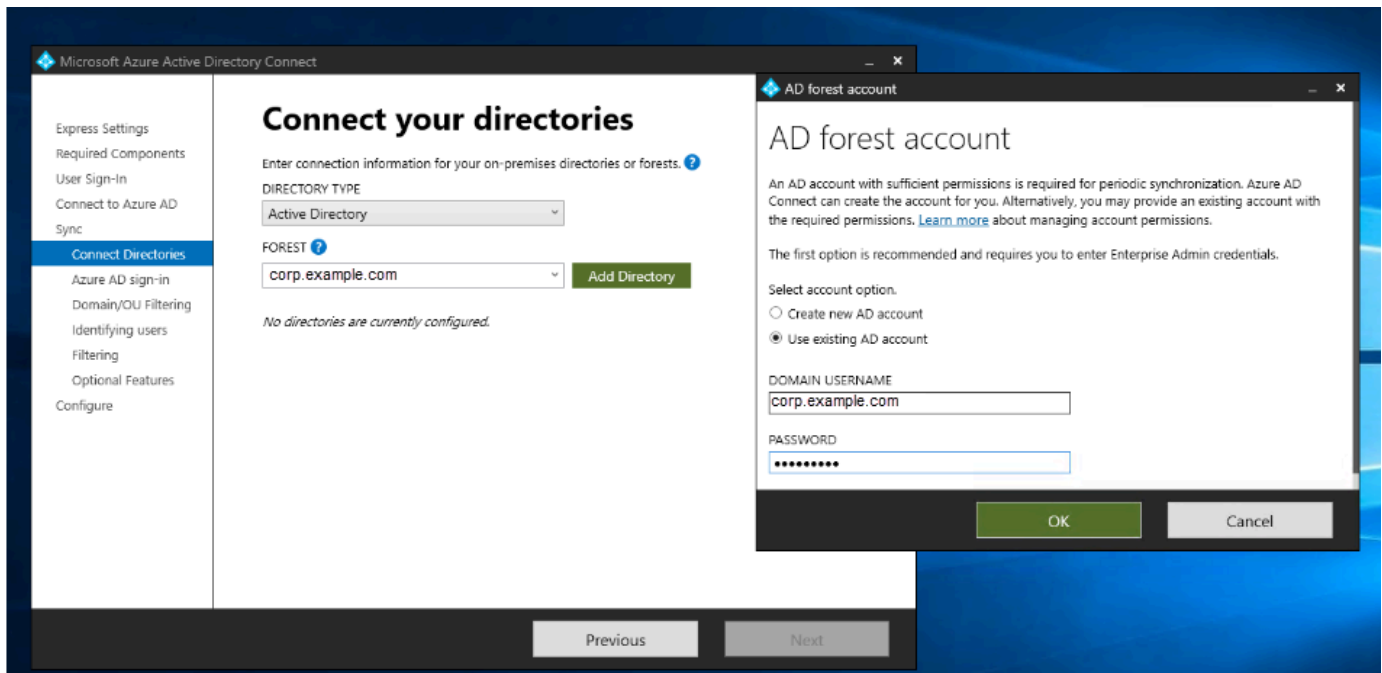
Previous Install

4. Pada jendela User Sign-in, pilih salah satu opsi berikut:
 - a. [Pass-through Authentication](#) - Opsi ini memungkinkan Anda untuk masuk ke Active Directory Anda dengan nama pengguna dan kata sandi Anda.
 - b. Jangan mengkonfigurasi - Ini memungkinkan Anda untuk menggunakan masuk federasi dengan Microsoft Entra (sebelumnya dikenal sebagai Azure Active Directory (AzureAD)) atau. Office 365

Kemudian pilih Berikutnya.

5. Pada Azure jendela Connect to, masukkan nama pengguna dan kata sandi [Administrator Global](#) Anda Entra ID dan pilih Berikutnya.
6. Pada jendela Connect your directories, pilih Active Directory for DIRECTORY TYPE. Pilih hutan untuk Microsoft AD for FOREST yang AWS Dikelola. Kemudian pilih Tambahkan Direktori.

7. Kotak pop-up muncul meminta opsi akun Anda. Pilih Gunakan akun AD yang ada. Masukkan nama AD DS Connector account pengguna dan kata sandi yang dibuat pada Langkah 1 dan kemudian pilih OK. Kemudian pilih Berikutnya.



8. Pada jendela Azure AD Masuk, pilih Lanjutkan tanpa mencocokkan semua sufiks UPN dengan domain terverifikasi, hanya jika Anda tidak memiliki domain vanity terverifikasi yang ditambahkan. Entra ID Kemudian pilih Berikutnya.
9. Pada jendela pemfilteran domain/OU, pilih opsi yang sesuai dengan kebutuhan Anda. Untuk informasi selengkapnya, lihat [Entra Connect Sync: Mengkonfigurasi pemfilteran](#) dalam Microsoft dokumentasi. Kemudian pilih Berikutnya.
10. Pada jendela Mengidentifikasi Pengguna, Pemfilteran, dan Fitur Opsional, pertahankan nilai default dan pilih Berikutnya.
11. Pada jendela Konfigurasi, tinjau pengaturan konfigurasi dan pilih Konfigurasi. Instalasi untuk Entra Connect Sync akan selesai dan pengguna akan mulai melakukan sinkronisasi dengan Microsoft Entra ID

AWS Tutorial lab uji Microsoft AD yang dikelola

Bagian ini menyediakan serangkaian tutorial terpandu untuk membantu Anda membangun lingkungan lab pengujian AWS tempat Anda dapat bereksperimen dengan Microsoft AD yang AWS Dikelola.

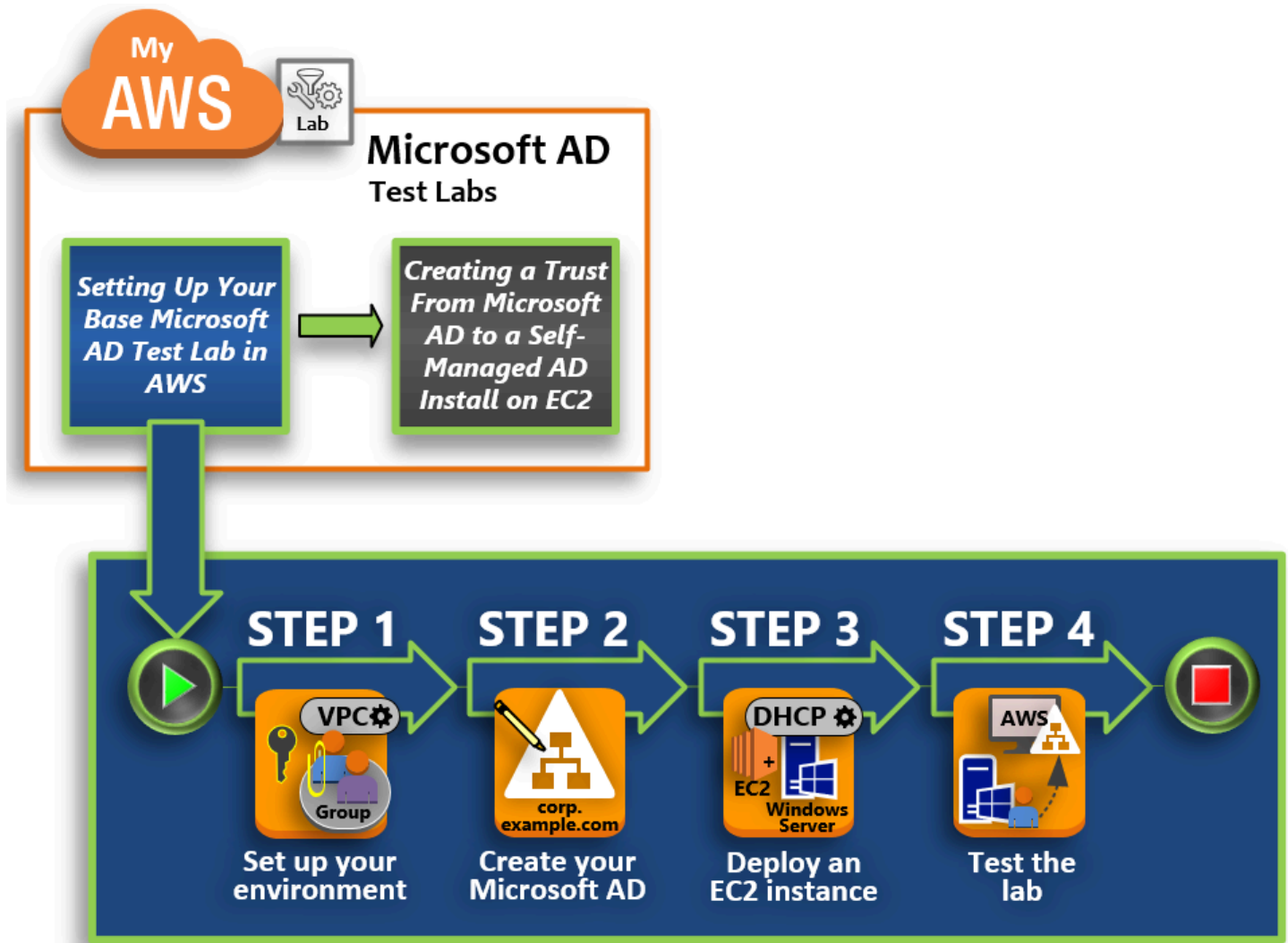
Topik

- [Tutorial: Menyiapkan lab uji Microsoft AD AWS Terkelola basis Anda di AWS](#)
- [Tutorial: Membuat kepercayaan dari Microsoft AD yang AWS Dikelola ke instalasi Direktori Aktif yang dikelola sendiri di Amazon EC2](#)

Tutorial: Menyiapkan lab uji Microsoft AD AWS Terkelola basis Anda di AWS

Tutorial ini mengajarkan Anda cara mengatur AWS lingkungan Anda untuk mempersiapkan instalasi Microsoft AD AWS Terkelola baru yang menggunakan instans Amazon EC2 baru yang menjalankan Windows Server 2019. Ini kemudian mengajarkan Anda untuk menggunakan alat administrasi Direktori Aktif khas untuk mengelola lingkungan Microsoft AD yang AWS Dikelola dari instans EC2 Windows Anda. Pada saat Anda menyelesaikan tutorial, Anda akan mengatur prasyarat jaringan dan telah mengkonfigurasi hutan AD AWS Microsoft yang Dikelola baru.

Seperti yang ditunjukkan dalam ilustrasi berikut, lab yang Anda buat dari tutorial ini adalah komponen dasar untuk pembelajaran langsung tentang Managed AWS Microsoft AD. Anda dapat menambahkan tutorial opsional nanti untuk pengalaman langsung yang lebih banyak. Seri tutorial ini sangat ideal untuk siapa saja yang baru akan Microsoft AD yang Dikelola AWS dan menginginkan laboratorium pengujian untuk tujuan evaluasi. Tutorial ini memakan waktu sekitar 1 jam untuk menyelesaikannya.



Langkah 1: Siapkan AWS lingkungan Anda untuk Direktori Aktif Microsoft AD yang AWS Dikelola

Setelah menyelesaikan tugas prasyarat, Anda membuat dan mengonfigurasi VPC Amazon di instans EC2 Anda.

Langkah 2: Buat Direktori Aktif Microsoft AD AWS Terkelola

Pada langkah ini, Anda mengatur iklan Microsoft yang AWS Dikelola AWS untuk pertama kalinya.

Langkah 3: Menerapkan instans Amazon EC2 untuk mengelola Direktori Aktif Microsoft AD yang AWS Dikelola

Di sini, Anda menelusuri berbagai tugas pasca deployment yang diperlukan untuk komputer klien untuk terhubung ke domain baru Anda dan mengatur sistem Windows Server baru di EC2.

Langkah 4: Verifikasi bahwa laboratorium pengujian dasar beroperasi

Akhirnya, sebagai administrator, Anda memverifikasi bahwa Anda dapat masuk dan terhubung ke Microsoft AD yang Dikelola AWS dari sistem Windows Server di EC2. Setelah Anda berhasil menguji bahwa laboratorium beroperasi, Anda dapat terus menambahkan modul panduan laboratorium pengujian lainnya.

Prasyarat

Jika Anda berencana untuk menggunakan hanya langkah-langkah UI dalam tutorial ini untuk membuat laboratorium pengujian Anda, Anda dapat melewati bagian prasyarat ini dan melanjutkan ke Langkah 1. Namun, jika Anda berencana untuk menggunakan AWS CLI perintah atau AWS Tools for Windows PowerShell modul untuk membuat lingkungan lab pengujian Anda, Anda harus terlebih dahulu mengonfigurasi berikut ini:

- Pengguna IAM dengan akses dan kunci akses rahasia — Pengguna IAM dengan kunci akses diperlukan jika Anda ingin menggunakan AWS CLI atau AWS Tools for Windows PowerShell modul. Jika Anda tidak memiliki access key, lihat [Membuat, memodifikasi, dan melihat access key \(Konsol Manajemen AWS\)](#).
- AWS Command Line Interface (opsional) - Unduh dan [Instal AWS CLI pada Windows](#). Setelah diinstal, buka prompt perintah atau PowerShell jendela, lalu ketik `aws configure`. Perhatikan bahwa Anda memerlukan access key dan kunci rahasia untuk menyelesaikan pengaturan. Lihat prasyarat pertama untuk langkah-langkah tentang cara melakukannya. Anda akan diminta hal berikut:
 - AWS ID kunci akses [Tidak ada]: AKIAIOSFODNN7EXAMPLE
 - AWS kunci akses rahasia [Tidak ada]: wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
 - Nama Region default [Tidak ada]: us-west-2
 - Format keluar default [Tidak ada]: json
- AWS Tools for Windows PowerShell(opsional) - Unduh dan instal versi terbaru AWS Tools for Windows PowerShell dari <https://aws.amazon.com/powershell/>, lalu jalankan perintah berikut. Perhatikan bahwa Anda memerlukan access key dan kunci rahasia Anda untuk menyelesaikan pengaturan. Lihat prasyarat pertama untuk langkah-langkah tentang cara melakukannya.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey  
{wJalrXUtnFEMI/K7MDENG/ bPxrFiCYEXAMPLEKEY} -StoreAs {default}
```

Langkah 1: Siapkan AWS lingkungan Anda untuk Direktori Aktif Microsoft AD yang AWS Dikelola

Sebelum dapat membuat Microsoft AD AWS Terkelola di lab AWS pengujian, Anda harus terlebih dahulu menyiapkan key pair Amazon EC2 agar semua data login dienkripsi.

Membuat key pair

Jika Anda sudah memiliki key pair, Anda dapat melewati langkah ini. Untuk informasi selengkapnya tentang pasangan kunci Amazon EC2, lihat [Membuat pasangan kunci](#).

Untuk membuat pasangan kunci

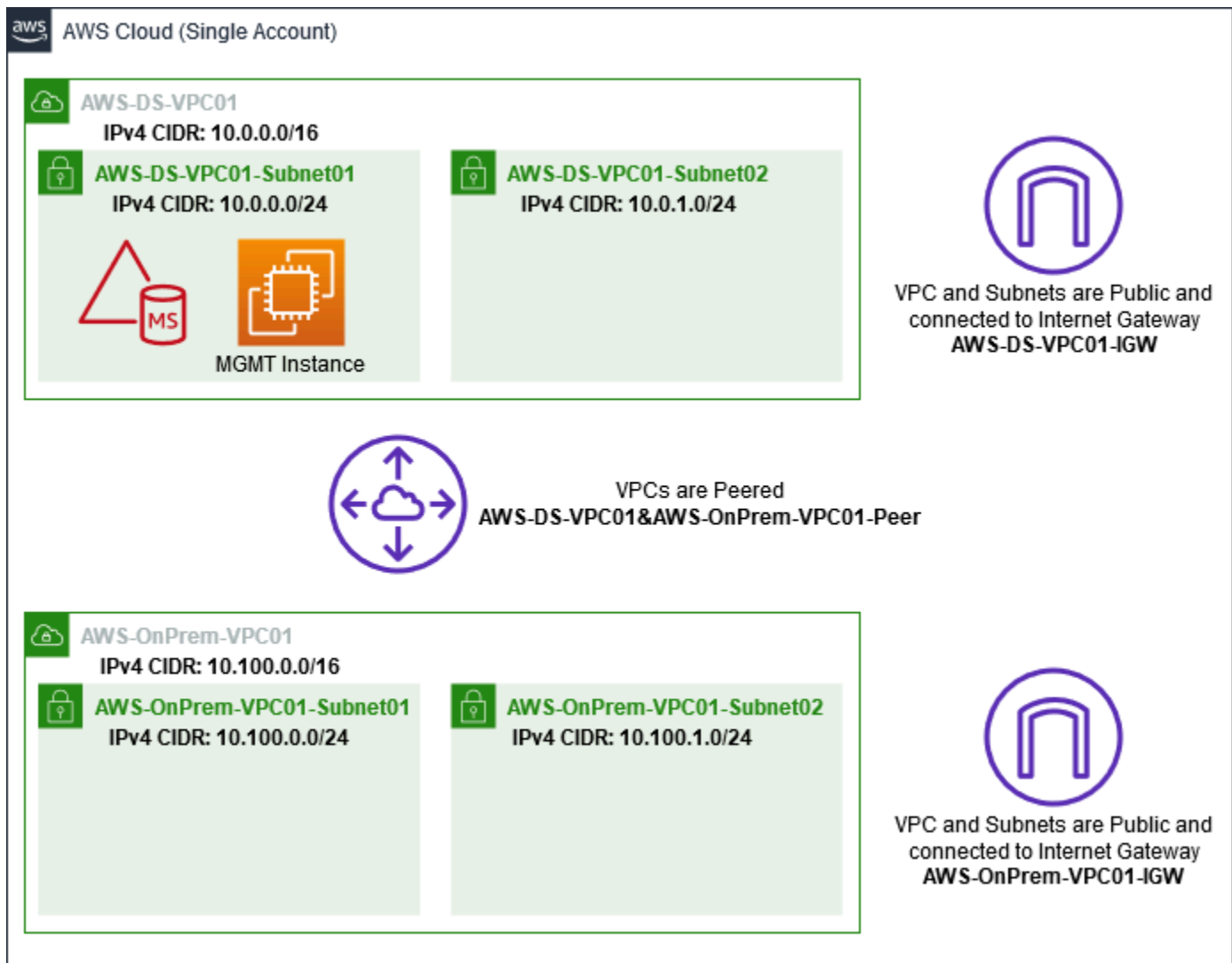
1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di. <https://console.aws.amazon.com/ec2/>
2. Pada panel navigasi, di bawah Jaringan & Keamanan, pilih Key Pair, dan kemudian pilih Buat Key Pair.
3. Untuk Nama key pair, ketik **AWS-DS-KP**. Untuk Format file key pair, pilih pem, lalu pilih Buat.
4. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Nama file adalah nama yang Anda tentukan ketika Anda membuat key pair Anda dengan ekstensi .pem. Simpan file kunci privat di suatu tempat yang aman.

Important

Ini adalah satu-satunya kesempatan bagi Anda untuk menyimpan file kunci pribadi. Anda harus menyediakan nama key pair Anda saat meluncurkan sebuah instans dan kunci pribadi yang terkait setiap kali Anda mendekripsi kata sandi untuk instans tersebut.

Buat, konfigurasi, dan peer dua Amazon VPCs

Seperti yang ditunjukkan dalam ilustrasi berikut, pada saat Anda menyelesaikan proses multi-langkah ini, Anda akan membuat dan mengonfigurasi dua publik VPCs, dua subnet publik per VPC, satu Internet Gateway per VPC, dan satu koneksi VPC Peering antara. VPCs Kami memilih untuk menggunakan publik VPCs dan subnet untuk tujuan kesederhanaan dan biaya. Untuk beban kerja produksi, kami sarankan Anda menggunakan pribadi VPCs. Untuk informasi selengkapnya tentang meningkatkan keamanan VPC, lihat [Keamanan dalam Amazon Virtual Private Cloud](#).



Semua AWS CLI dan PowerShell contoh menggunakan informasi VPC dari bawah dan dibangun di us-west-2. Anda dapat memilih [Region yang didukung](#) mana pun untuk membangun lingkungan Anda. Untuk informasi umum, lihat [Apa yang Dimaksud dengan Amazon VPC?](#).

Langkah 1: Buat dua VPCs

Pada langkah ini, Anda perlu membuat dua VPCs di akun yang sama menggunakan parameter yang ditentukan dalam tabel berikut. AWS Microsoft AD yang dikelola mendukung penggunaan akun terpisah dengan [Bagikan iklan Microsoft yang AWS Dikelola](#) fitur tersebut. VPC pertama akan digunakan untuk AWS Microsoft AD yang Dikelola. VPC kedua akan digunakan untuk sumber daya yang dapat digunakan nanti di [Tutorial: Membuat kepercayaan dari Microsoft AD yang AWS Dikelola ke instalasi Direktori Aktif yang dikelola sendiri di Amazon EC2](#).

Informasi VPC Direktori Aktif Terkelola	Informasi VPC lokal
Tag nama: AWS-DS- VPC01	Tag nama: AWS- OnPrem - VPC01
IPv4 Blok CIDR: 10.0.0.0/16	IPv4 Blok CIDR: 10.100.0.0/16
IPv6 Blok CIDR: Tidak ada Blok IPv6 CIDR	IPv6 Blok CIDR: Tidak ada Blok IPv6 CIDR
Penghunian: Default	Penghunian: Default

Untuk instruksi detail, lihat [Membuat VPC](#).

Langkah 2: Buat dua subnet per VPC

Setelah Anda membuat, VPCs Anda perlu membuat dua subnet per VPC menggunakan parameter yang ditentukan dalam tabel berikut. Untuk laboratorium pengujian ini setiap subnet akan menjadi /24. Ini akan memungkinkan hingga 256 alamat yang dikeluarkan per subnet. Setiap subnet harus dalam AZ terpisah. Menempatkan setiap subnet secara terpisah di AZ adalah salah satu [Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS](#).

AWS-DS- Informasi VPC01 subnet:	AWS- OnPrem - informasi VPC01 subnet
Tag nama: AWS-DS- -Subnet01 VPC01	Tag nama: AWS- OnPrem - VPC01 -Subnet01
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx AWS VPC01	VPC: AWS vpc-xxxxxxxxxxxxxxxxxxx - - OnPrem VPC01
Availability Zone: us-west-2a	Availability Zone: us-west-2a
IPv4 Blok CIDR: 10.0.0.0/24	IPv4 Blok CIDR: 10.100.0.0/24
Tag nama: AWS-DS- -Subnet02 VPC01	Tag nama: AWS- OnPrem - VPC01 -Subnet02
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx AWS VPC01	VPC: AWS vpc-xxxxxxxxxxxxxxxxxxx - - OnPrem VPC01
Availability Zone: us-west-2b	Availability Zone: us-west-2b
	IPv4 Blok CIDR: 10.100.1.0/24

AWS-DS- Informasi VPC01 subnet:	AWS- OnPrem - informasi VPC01 subnet
IPv4 Blok CIDR: 10.0.1.0/24	

Untuk instruksi detail, lihat [Membuat subnet dalam VPC Anda](#).

Langkah 3: Buat dan lampirkan Internet Gateway ke Anda VPCs

Karena kita menggunakan VPC publik Anda akan perlu untuk membuat dan melampirkan gateway Internet ke VPC Anda menggunakan parameter yang ditentukan dalam tabel berikut. Hal ini akan memungkinkan Anda untuk terhubung ke dan mengelola instans EC2 Anda.

AWS-DS- Informasi VPC01 Internet Gateway	AWS- OnPrem - Informasi VPC01 Internet Gateway
Tag nama: AWS-DS- -IGW VPC01	Tag nama: AWS- OnPrem - VPC01 -IGW
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx AWS VPC01	VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxxx - - OnPrem VPC01

Untuk instruksi detail, lihat [Gateway internet](#).

Langkah 4: Konfigurasikan koneksi peering VPC antara AWS-DS- dan - - VPC01 AWS OnPrem VPC01

Karena Anda sudah membuat dua VPCs sebelumnya, Anda harus membuat jaringan mereka bersama-sama menggunakan VPC peering menggunakan parameter yang ditentukan dalam tabel berikut. Meskipun ada banyak cara untuk menghubungkan Anda VPCs, tutorial ini akan menggunakan VPC Peering. [AWS Microsoft AD yang dikelola mendukung banyak solusi untuk menghubungkan Anda VPCs, beberapa di antaranya termasuk peering VPC, Transit Gateway, dan VPN.](#)

Tag nama koneksi peering: AWS-DS- VPC01 &AWS- - OnPrem -Peer VPC01

VPC (Pemohon): vpc-xxxxxxxxxxxxxxxxxxxxx -DS- AWS VPC01

Akun: Akun Saya

Region: Region Ini

VPC (Penerima): vpc-xxxxxxxxxxxxxxxx - - AWS OnPrem VPC01

Untuk instruksi tentang cara membuat Koneksi Peering VPC dengan VPC lain dari dengan akun Anda, lihat [Membuat koneksi peering VPC dengan VPC lain di akun Anda](#).

Langkah 5: Tambahkan dua rute ke setiap tabel rute utama VPC

Agar Internet Gateways dan VPC Peering Connection yang dibuat pada langkah-langkah sebelumnya berfungsi, Anda perlu memperbarui tabel rute utama keduanya VPCs menggunakan parameter yang ditentukan dalam tabel berikut. Anda akan menambahkan dua rute; 0.0.0.0/0 yang akan merutekan ke semua tujuan yang tidak diketahui secara eksplisit ke tabel rute dan 10.0.0.0/16 atau 10.100.0.0/16 yang akan merutekan ke setiap VPC melalui Koneksi Peering VPC yang dibangun di atas.

Anda dapat dengan mudah menemukan tabel rute yang benar untuk setiap VPC dengan memfilter pada tag nama VPC (AWS-DS- atau - -). VPC01 AWS OnPrem VPC01

AWS-DS- informasi VPC01 rute 1	AWS-DS- informasi VPC01 rute 2	AWS- OnPrem - Informasi VPC01 rute 1	AWS- OnPrem - Informasi VPC01 rute 2
Tujuan: 0.0.0.0/0	Tujuan: 10.100.0.0/16	Tujuan: 0.0.0.0/0	Tujuan: 10.0.0.0/16
Target: igw-xxxxx xxxxxxxxxxxxxxxxxxxxx xx -IGW AWS VPC01	Target: pcx-xxxxx xxxxxxxxxxxxxxxxxxxxx x AWS-ds-& - - -rekan VPC01 AWS OnPrem VPC01	Target: igw-xxxxx xxxxxxxxxxxxxxxxxxxxx - Onprem- AWS VPC01	Target: pcx-xxxxx xxxxxxxxxxxxxxxxxxxxx x AWS-ds-& - - -rekan VPC01 AWS OnPrem VPC01

Untuk instruksi tentang cara menambahkan rute ke tabel rute VPC, lihat [Menambahkan dan menghapus rute dari tabel rute](#).

Membuat grup keamanan untuk instans Amazon EC2

Secara default, Microsoft AD yang AWS Dikelola membuat grup keamanan untuk mengelola lalu lintas di antara pengontrol domainnya. Pada bagian ini, Anda perlu membuat 2 grup keamanan (satu

untuk setiap VPC) yang akan digunakan untuk mengelola lalu lintas dalam VPC Anda untuk instans EC2 Anda menggunakan parameter yang ditentukan dalam tabel berikut. Anda juga menambahkan aturan yang mengizinkan RDP (3389) masuk dari mana saja dan untuk semua jenis lalu lintas masuk dari VPC lokal. Untuk informasi selengkapnya, lihat [Grup keamanan Amazon EC2 untuk instans Windows](#).

AWS-DS- Informasi kelompok VPC01 keamanan:

Nama grup keamanan: AWS DS Test Lab Security Group

Deskripsi: Grup Keamanan Lab Uji AWS DS

VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx AWS VPC01

Aturan Masuk Grup Keamanan untuk AWS-DS- VPC01

Tipe	Protokol	Rentang port	Sumber	Jenis lalu lintas
Aturan TCP Kustom	TCP	3389	IP saya	Desktop Jarak Jauh
Semua Lalu Lintas	Semua	Semua	10.0.0.0/16	Semua lalu lintas VPC lokal

Aturan Keluar Grup Keamanan untuk AWS-DS- VPC01

Tipe	Protokol	Rentang Port	Destinasi	Jenis lalu lintas
Semua Lalu Lintas	Semua	Semua	0.0.0.0/0	Semua Lalu lintas

AWS- OnPrem - informasi kelompok VPC01 keamanan:

Nama grup keamanan: Grup Keamanan Lab AWS OnPrem Uji.

AWS- OnPrem - informasi kelompok VPC01 keamanan:

Deskripsi: Kelompok Keamanan Lab AWS OnPrem Uji.

VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxx - - OnPrem VPC01

Aturan Masuk Grup Keamanan untuk AWS- - OnPrem VPC01

Tipe	Protokol	Rentang port	Sumber	Jenis lalu lintas
Aturan TCP Kustom	TCP	3389	IP saya	Desktop Jarak Jauh
Aturan TCP Kustom	TCP	53	10.0.0.0/16	DNS
Aturan TCP Kustom	TCP	88	10.0.0.0/16	Kerberos
Aturan TCP Kustom	TCP	389	10.0.0.0/16	LDAP
Aturan TCP Kustom	TCP	464	10.0.0.0/16	Kerberos mengubah / mengatur kata sandi
Aturan TCP Kustom	TCP	445	10.0.0.0/16	SMB / CIFS
Aturan TCP Kustom	TCP	135	10.0.0.0/16	Replikasi
Aturan TCP Kustom	TCP	636	10.0.0.0/16	LDAP SSL
Aturan TCP Kustom	TCP	49152 - 65535	10.0.0.0/16	RPC

Tipe	Protokol	Rentang port	Sumber	Jenis lalu lintas
Aturan TCP Kustom	TCP	3268 - 3269	10.0.0.0/16	LDAP GC & LDAP GC SSL
Aturan UDP Kustom	UDP	53	10.0.0.0/16	DNS
Aturan UDP Kustom	UDP	88	10.0.0.0/16	Kerberos
Aturan UDP Kustom	UDP	123	10.0.0.0/16	Waktu Windows
Aturan UDP Kustom	UDP	389	10.0.0.0/16	LDAP
Aturan UDP Kustom	UDP	464	10.0.0.0/16	Kerberos mengubah / mengatur kata sandi
Semua Lalu Lintas	Semua	Semua	10.100.0.0/16	Semua lalu lintas VPC lokal

Aturan Keluar Grup Keamanan untuk AWS- - OnPrem VPC01

Tipe	Protokol	Rentang Port	Destinasi	Jenis lalu lintas
Semua Lalu Lintas	Semua	Semua	0.0.0.0/0	Semua Lalu lintas

Untuk intruksi detail tentang cara membuat dan menambahkan aturan ke grup keamanan Anda, lihat [Cara menggunakan grup keamanan](#).

Langkah 2: Buat Direktori Aktif Microsoft AD AWS Terkelola

Anda dapat menggunakan tiga metode yang berbeda untuk membuat direktori Anda. Anda dapat menggunakan Konsol Manajemen AWS prosedur (direkomendasikan untuk tutorial ini) atau Anda dapat menggunakan AWS Tools for Windows PowerShell prosedur AWS CLI atau untuk membuat direktori Anda.

Metode 1: Untuk membuat direktori Microsoft AD yang AWS Dikelola (Konsol Manajemen AWS)

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori, lalu pilih Atur direktori.
2. Di halaman Pilih jenis direktori, pilih Microsoft AD yang Dikelola AWS , lalu pilih Selanjutnya.
3. Pada halaman Masukkan informasi direktori, berikan informasi berikut, dan pilih Selanjutnya.
 - Untuk Edisi, pilih salah satu antara Standard Edition atau Enterprise Edition. Untuk informasi selengkapnya tentang edisi, lihat [Directory Service AWS untuk Microsoft Active Directory](#).
 - Untuk Nama DNS direktori, ketik **corp.example.com**.
 - Untuk Nama NetBIOS direktori, ketik **corp**.
 - Untuk Deskripsi direktori, ketik **AWS DS Managed**.
 - Untuk Kata sandi admin, ketik kata sandi yang ingin Anda gunakan untuk akun ini dan ketik lagi kata sandi di Konfirmasi kata sandi. Akun Admin ini secara otomatis dibuat selama proses pembuatan direktori. Kata sandi tidak dapat menyertakan kata admin. Kata sandi administrator direktori peka akan huruf besar kecil dan harus terdiri dari 8 sampai 64 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:
 - Huruf kecil (a-z)
 - Huruf besar (A-Z)
 - Angka (0-9)
 - Karakter non-alfanumerik (~!@#\$%^&* _-+=`|(){}[]:;'"<>,.?/)
4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.
 - Untuk VPC, pilih opsi yang dimulai dengan AWS-DS- VPC01 dan diakhiri dengan (10.0.0.0/16).
 - Untuk Subnet, pilih subnet publik 10.0.0.0/24 dan 10.0.1.0/24.
5. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Membuat direktori membutuhkan waktu 20 sampai 40 menit. Setelah dibuat, nilai Status berubah ke Aktif.

Metode 2: Untuk membuat Microsoft AD yang AWS Dikelola (PowerShell) (Opsional)

1. Buka PowerShell.
2. Ketik perintah berikut ini. Pastikan untuk menggunakan nilai yang disediakan pada Langkah 4 dari prosedur sebelumnya. Konsol Manajemen AWS

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd -Description "AWS DS Managed" - VpcSettings_VpcId vpc-xxxxxxx - VpcSettings_SubnetId subnet-xxxxxxx, subnet-xxxxxxx
```

Metode 3: Untuk membuat Microsoft AD yang AWS Dikelola (AWS CLI) (Opsional)

1. Buka AWS CLI.
2. Ketik perintah berikut ini. Pastikan untuk menggunakan nilai yang disediakan pada Langkah 4 dari prosedur sebelumnya. Konsol Manajemen AWS

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-xxxxxxx,SubnetIds= subnet-xxxxxxx, subnet-xxxxxxx
```

Langkah 3: Menerapkan instans Amazon EC2 untuk mengelola Direktori Aktif Microsoft AD yang AWS Dikelola

Untuk lab ini, kami menggunakan instans Amazon EC2 yang memiliki alamat IP publik agar mudah mengakses instans manajemen dari mana saja. Dalam pengaturan produksi, Anda dapat menggunakan instance yang ada di VPC pribadi yang hanya dapat diakses melalui VPN Direct Connect atau tautan. Tidak ada persyaratan instans memiliki alamat IP publik.

Di bagian ini, Anda menelusuri berbagai tugas pasca deployment yang diperlukan untuk komputer klien untuk terhubung ke domain Anda menggunakan Windows Server baru di instans EC2 baru Anda. Anda menggunakan Windows Server pada langkah berikutnya untuk memverifikasi bahwa laboratorium beroperasi.

Opsional: Buat opsi DHCP diatur dalam AWS-DS- VPC01 untuk direktori Anda

Dalam prosedur opsional ini, Anda menyiapkan cakupan opsi DHCP sehingga instans EC2 di VPC Anda secara otomatis menggunakan AD AWS Microsoft Terkelola untuk resolusi DNS. Untuk informasi selengkapnya, lihat [Set pilihan DHCP](#).

Untuk membuat set opsi DHCP untuk direktori Anda

1. Buka konsol Amazon VPC di. <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Set Opsi DHCP, lalu pilih Buat set opsi DHCP.
3. Pada halaman Buat set opsi DHCP, berikan nilai berikut untuk direktori Anda:
 - Untuk Nama, ketik **AWS_DS_DHCP**.
 - Untuk Nama domain, ketik **corp.example.com**.
 - Untuk Server nama domain, ketik alamat IP dari server DNS direktori yang disediakan AWS .

Note

Untuk menemukan alamat ini, buka halaman Directory Service Direktori, lalu pilih ID direktori yang berlaku. Pada halaman Detail, identifikasi dan gunakan IPs yang ditampilkan di alamat DNS.

Atau, untuk menemukan alamat ini, buka halaman Directory Service Direktori, dan pilih ID direktori yang berlaku. Kemudian, pilih Skala & bagian. Di bawah pengontrol Domain, identifikasi dan gunakan IPs yang ditampilkan di alamat IP.

- Biarkan pengaturan kosong untuk Server NTP, Server nama NetBIOS, dan Jenis simpul NetBIOS.
4. Pilih Buat set opsi DHCP, lalu pilih Tutup. Set pilihan DHCP yang baru muncul dalam daftar pilihan DHCP Anda.
 5. Catat ID set baru opsi DHCP (dopt- **xxxxxxxx**). Anda menggunakannya pada akhir prosedur ini ketika Anda mengasosiasikan set pilihan yang baru dengan VPC Anda.

Note

Penggabungan domain yang mulus bekerja tanpa harus mengkonfigurasi Set Pilihan DHCP.

6. Di panel navigasi, pilih Your VPCs.
7. Dalam daftar VPCs, pilih AWS_DS_VPC, pilih Tindakan, lalu pilih Edit opsi DHCP set.
8. Pada halaman Edit set pilihan DHCP, pilih set pilihan yang Anda catat di Langkah 5, dan kemudian pilih Simpan.

Membuat peran untuk menggabungkan instans Windows ke domain Microsoft AD AWS Terkelola

Gunakan prosedur ini untuk mengonfigurasi peran yang menggabungkan instans Amazon EC2 Windows ke domain. Untuk informasi selengkapnya, lihat [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#).

Untuk mengkonfigurasi EC2 untuk menggabungkan instans Windows ke domain Anda

1. Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi konsol IAM, pilih Peran, dan lalu pilih Buat peran.
3. Di bawah Pilih jenis entitas terpercaya, pilih AWS layanan.
4. Segera di bawah Pilih layanan yang akan menggunakan peran ini, pilih EC2, lalu pilih Berikutnya: Izin.
5. Di halaman Kebijakan izin terlampir, lakukan hal berikut:
 - Pilih kotak di sebelah kebijakan SSMManged InstanceCore terkelola Amazon. Kebijakan ini menyediakan izin minimum yang diperlukan untuk menggunakan layanan Systems Manager.
 - Pilih kotak di samping kebijakan SSMDirectory ServiceAccess terkelola Amazon. Kebijakan ini menyediakan izin untuk menggabungkan instans ke Direktori Aktif yang dikelola oleh Directory Service.

Untuk informasi tentang kebijakan terkelola ini dan kebijakan lain yang dapat dilampirkan ke profil instans IAM untuk Systems Manager, lihat [Buat profil instans IAM untuk Systems Manager](#) dalam Panduan Pengguna AWS Systems Manager . Untuk informasi selengkapnya tentang kebijakan terkelola , lihat [Kebijakan yang dikelola AWS](#) dalam Panduan Pengguna IAM.

6. Pilih Berikutnya: Tag.
7. (Opsional) Tambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk peran ini, lalu pilih Selanjutnya: Tinjau.
8. Untuk nama Peran, masukkan nama untuk peran yang menjelaskan bahwa itu digunakan untuk menggabungkan instance ke domain, seperti EC2DomainJoin.
9. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
10. Pilih Buat peran. Sistem mengembalikan Anda ke halaman Peran.

Buat instans Amazon EC2 dan secara otomatis bergabung dengan direktori

Dalam prosedur ini Anda mengatur sistem Windows Server dalam instans EC2 yang dapat digunakan nanti untuk mengelola pengguna, grup, dan kebijakan di Active Directory.

Untuk membuat instans EC2 dan menggabungkan direktori secara otomatis

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Pilih Luncurkan Instans.
3. Pada halaman Langkah 1, di sebelah Microsoft Windows Server 2019 Base - ami-
xxxxxxxxxxxxxxxxxxxx pilih Pilih.
4. Pada halaman Langkah 2, pilih t3.micro (ingat, Anda dapat memilih jenis instans yang lebih besar), kemudian pilih Selanjutnya: Konfigurasi Detail Instans.
5. Pada halaman Langkah 3, lakukan hal berikut:
 - Untuk Jaringan, pilih VPC yang diakhiri dengan AWS-DS- VPC01 (misalnya, vpc-
xxxxxxxxxxxxxxxxxxxx | AWS-DS-). VPC01
 - Untuk Subnet pilih Public subnet 1, yang harus dikonfigurasi sebelumnya untuk Availability Zone pilihan Anda (misalnya, subnet- **xxxxxxxxxxxxxxxxxxxx** | AWS-DS- -Subnet01 |). VPC01
us-west-2a
 - Untuk Tetapkan Otomatis IP Publik, pilih Aktifkan (jika pengaturan subnet tidak diatur untuk mengaktifkan secara default).
 - Untuk direktori Gabung Domain, pilih corp.example.com (d-). **xxxxxxxxxx**
 - Untuk peran IAM pilih nama yang Anda berikan peran instans Anda [Membuat peran untuk menggabungkan instans Windows ke domain Microsoft AD AWS Terkelola](#), seperti EC2DomainJoin.
 - Biarkan pengaturan lainnya pada default.
 - Pilih Berikutnya: Tambahkan Penyimpanan.
6. Pada halaman Langkah 4, biarkan pengaturan default, kemudian pilih Berikutnya: Tambahkan Tanda.
7. Pada halaman Langkah 5, pilih Tambahkan Tanda. Di bawah Kunci ketik **corp.example.com-mgmt** kemudian pilih Berikutnya: Konfigurasi Grup Keamanan.
8. Pada halaman Langkah 6, pilih Pilih grup keamanan yang ada, pilih AWS DS Test Lab Security Group (yang sebelumnya Anda atur dalam [tutorial Dasar](#)), lalu pilih Tinjau dan Luncurkan untuk meninjau instance Anda.

9. Pada halaman Langkah 7, tinjau halaman, dan kemudian pilih Luncurkan.
10. Pada kotak dialog Pilih key pair yang sudah ada atau buat key pair baru, lakukan hal berikut:
 - Pilih key pair yang sudah ada.
 - Di bawah Pilih key pair, pilih AWS-DS-KP.
 - Pilih kotak centang Saya mengakui....
 - Pilih Luncurkan Instans.
11. Pilih Lihat Instans untuk kembali ke konsol Amazon EC2 dan melihat status deployment.

Menginstal alat Direktori Aktif pada instans EC2 Anda

Anda dapat memilih dari dua metode untuk menginstal Active Directory Domain Management Tools pada instans EC2 Anda. Anda dapat menggunakan UI Server Manager (direkomendasikan untuk tutorial ini) atau PowerShell.

Untuk menginstal alat Direktori Aktif pada instans EC2 Anda (Pengelola Server)

1. Di konsol Amazon EC2, pilih Instans, pilih Instans yang baru saja Anda buat, kemudian pilih Hubungkan.
2. Di kotak dialog Connect To Your Instance, pilih Dapatkan Kata Sandi untuk mengambil kata sandi jika Anda belum melakukannya, lalu pilih Unduh File Desktop Jarak Jauh.
3. Di kotak dialog Keamanan Windows, ketik kredensial administrator lokal Anda untuk Windows Server komputer untuk masuk (misalnya, **administrator**).
4. Dari menu Mulai, pilih Pengelola Server.
5. Di Dasbor, pilih Tambah Peran dan Fitur.
6. Di Tambahkan Wizard Peran dan Fitur, pilih Selanjutnya.
7. Pada halaman Pilih jenis instalasi, pilih Instalasi berbasis peran atau berbasis fitur, lalu pilih Selanjutnya.
8. Pada halaman Pilih server tujuan, pastikan bahwa server lokal dipilih, dan kemudian pilih Selanjutnya.
9. Pada halaman Pilih peran server, pilih Selanjutnya.
10. Pada halaman Pilih fitur, lakukan hal berikut:
 - Pilih kotak centang Pengelolaan Kebijakan Grup.

- Perluas Alat Administrasi Server Jarak Jauh, dan kemudian perluas Alat Administrasi Peran.
 - Pilih kotak centang Alat AD DS dan AD LDS.
 - Pilih kotak centang Alat Server DNS.
 - Pilih Berikutnya.
11. Pada halaman Konfirmasi pilihan instalasi, tinjau informasi, lalu pilih Instal. Setelah penginstalan fitur selesai, alat baru berikut atau snap-in akan tersedia di folder Alat Administratif Windows di menu Mulai.
- Pusat Administrasi Direktori Aktif
 - Domain dan Kepercayaan Direktori Aktif.
 - Modul Direktori Aktif untuk PowerShell
 - Situs dan Layanan Direktori Aktif.
 - Pengguna dan Komputer Direktori Aktif
 - Edit ADSI
 - DNS
 - Pengelolaan Kebijakan Grup

Untuk menginstal alat Active Directory pada instans EC2 Anda (PowerShell) (Opsional)

1. Mulai PowerShell.
2. Ketik perintah berikut ini.

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-Tools,RSAT-DNS-Server
```

Langkah 4: Verifikasi bahwa laboratorium pengujian dasar beroperasi

Gunakan prosedur berikut untuk memverifikasi bahwa laboratorium pengujian telah diatur dengan sukses sebelum menambahkan modul panduan laboratorium pengujian tambahan. Prosedur ini memverifikasi bahwa Windows Server Anda dikonfigurasi dengan tepat, dapat terhubung ke domain corp.example.com, dan digunakan untuk mengelola hutan AD Microsoft Terkelola Anda. AWS

Untuk memverifikasi bahwa laboratorium pengujian dasar beroperasi

1. Keluar dari instans EC2 di mana Anda masuk sebagai administrator lokal.

2. Kembali ke konsol Amazon EC2, pilih Instans pada panel navigasi. Kemudian pilih instans yang Anda buat. Pilih Hubungkan.
3. Di kotak dialog Hubungkan ke Instans Anda, pilih Unduh File Remote Desktop.
4. Di kotak dialog Keamanan Windows, ketik kredensial administrator Anda untuk domain CORP untuk masuk (misalnya, **corp\admin**).
5. Setelah Anda masuk, di menu Mulai, di bawah Alat Administratif Windows, pilih Pengguna dan Komputer Direktori Aktif.
6. Anda akan melihat corp.example.com ditampilkan dengan semua default OUs dan akun yang terkait dengan domain baru. Di bawah Pengontrol Domain, perhatikan nama pengontrol domain yang dibuat secara otomatis saat Anda membuat AD AWS Microsoft Terkelola kembali di Langkah 2 tutorial ini.

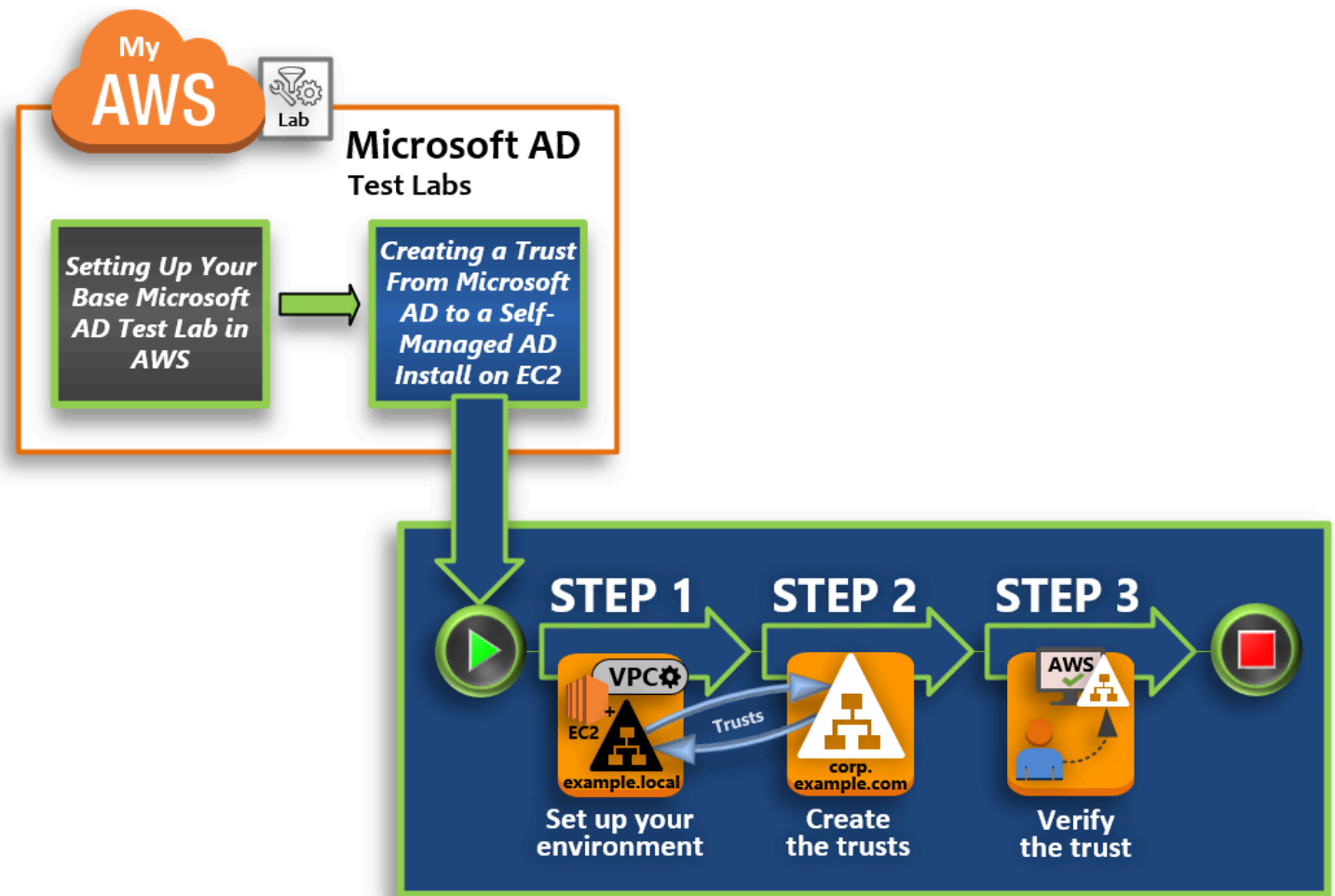
Selamat! Lingkungan lab pengujian dasar Microsoft AD AWS Terkelola Anda kini telah dikonfigurasi. Anda siap untuk mulai menambahkan laboratorium pengujian berikutnya dalam seri.

Tutorial berikutnya: [Tutorial: Membuat kepercayaan dari Microsoft AD yang AWS Dikelola ke instalasi Direktori Aktif yang dikelola sendiri di Amazon EC2](#)

Tutorial: Membuat kepercayaan dari Microsoft AD yang AWS Dikelola ke instalasi Direktori Aktif yang dikelola sendiri di Amazon EC2

Dalam tutorial ini, Anda belajar cara membuat kepercayaan antara AWS Directory Service untuk Microsoft Active Directory forest yang Anda buat di [tutorial Base](#). Anda juga belajar untuk membuat forest Direktori Aktif asli yang baru pada Windows Server di Amazon EC2. Seperti yang ditunjukkan pada ilustrasi berikut, lab yang Anda buat dari tutorial ini adalah blok bangunan kedua yang diperlukan saat menyiapkan lab pengujian Microsoft AD AWS Terkelola lengkap. Anda dapat menggunakan lab uji untuk menguji solusi berbasis cloud murni atau cloud hybrid. AWS

Anda hanya perlu membuat tutorial ini sekali. Setelah itu Anda dapat menambahkan tutorial opsional bila diperlukan untuk pengalaman lebih.



Langkah 1: Atur lingkungan Anda untuk kepercayaan

Sebelum Anda dapat membuat kepercayaan antara forest Direktori Aktif baru dan forest Microsoft AD yang Dikelola AWS yang Anda buat di [Tutorial dasar](#), Anda perlu mempersiapkan lingkungan Amazon EC2 Anda. Untuk melakukannya, pertama Anda membuat server Windows Server 2019, promosikan server tersebut ke pengendali domain, dan kemudian konfigurasi VPC Anda sesuai dengannya.

Langkah 2: Buat trust

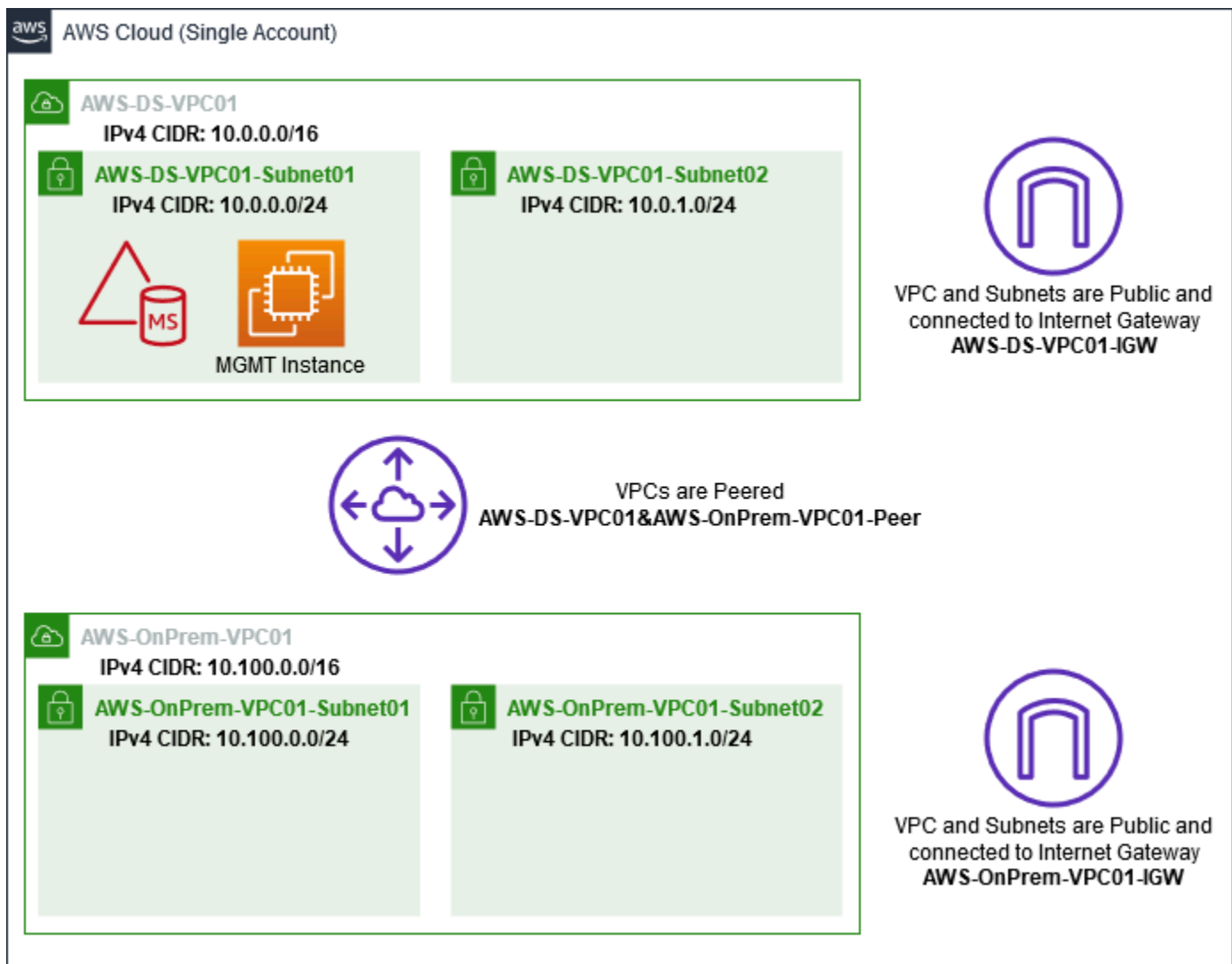
Pada langkah ini, Anda membuat hubungan kepercayaan hutan dua arah antara hutan Direktori Aktif yang baru dibuat yang dihosting di Amazon EC2 dan hutan Microsoft AD AWS Terkelola di AWS.

Langkah 3: Verifikasi kepercayaan

Terakhir, sebagai administrator, Anda menggunakan Directory Service konsol untuk memverifikasi bahwa trust baru beroperasi.

Langkah 1: Atur lingkungan Anda untuk kepercayaan

Di bagian ini, Anda mengatur lingkungan Amazon EC2, menyebarkan hutan baru, dan menyiapkan VPC Anda untuk dipercaya. AWS



Membuat instans EC2 Windows Server 2019

Gunakan prosedur berikut untuk membuat server anggota Windows Server 2019 di Amazon EC2.

Untuk membuat instans EC2 Windows Server 2019

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Di konsol Amazon EC2, pilih Luncurkan Instans.
3. Pada halaman Langkah 1, cari Microsoft Windows Server 2019 Base - ami-
xxxxxxxxxxxxxxxxxxxx dalam daftar. Lalu pilih Pilih.

4. Pada halaman Langkah 2, pilih t2.large, lalu pilih Berikutnya: Konfigurasi Detail Instans.
5. Pada halaman Langkah 3, lakukan hal berikut:
 - Untuk Jaringan, pilih vpc- **xxxxxxxxxxxxxxxxxxxx** AWS- OnPrem - VPC01 (yang sebelumnya Anda atur di [tutorial Base](#)).
 - Untuk Subnet, pilih subnet- **xxxxxxxxxxxxxxxxxxxx** | AWS- - VPC01 -Subnet01 | OnPrem - -. AWS OnPrem VPC01
 - Untuk daftar Tetapkan Otomatis IP Publik, pilih Aktifkan (jika pengaturan subnet tidak diatur ke Aktifkan secara default).
 - Biarkan pengaturan lainnya pada default.
 - Pilih Berikutnya: Tambahkan Penyimpanan.
6. Pada halaman Langkah 4, biarkan pengaturan default, kemudian pilih Berikutnya: Tambahkan Tanda.
7. Pada halaman Langkah 5, pilih Tambahkan Tanda. Di bawah Kunci ketik **example.local-DC01**, kemudian pilih Berikutnya: Konfigurasi Grup Keamanan.
8. Pada halaman Langkah 6, pilih Pilih grup keamanan yang ada, pilih AWS On-Prem Test Lab Security Group (yang sebelumnya Anda atur dalam [tutorial Dasar](#)), lalu pilih Tinjau dan Luncurkan untuk meninjau instance Anda.
9. Pada halaman Langkah 7, tinjau halaman, dan kemudian pilih Luncurkan.
10. Pada kotak dialog Pilih key pair yang sudah ada atau buat key pair baru, lakukan hal berikut:
 - Pilih Pilih key pair yang sudah ada.
 - Di bawah Pilih key pair, pilih AWS-DS-KP (yang sebelumnya Anda atur di [Tutorial dasar](#)).
 - Pilih kotak centang Saya mengakui....
 - Pilih Luncurkan Instans.
11. Pilih Lihat Instans untuk kembali ke konsol Amazon EC2 dan melihat status deployment.

Promosikan server Anda ke pengendali domain

Sebelum Anda dapat membuat kepercayaan, Anda harus membangun dan men-deploy pengendali domain pertama untuk forest baru. Selama proses ini Anda mengkonfigurasi forest Direktori Aktif baru, menginstal DNS, dan mengatur server ini untuk menggunakan server DNS lokal untuk resolusi nama. Anda harus me-reboot server pada akhir prosedur ini.

 Note

Jika Anda ingin membuat pengontrol domain dalam replikasi AWS tersebut dengan jaringan lokal, pertama-tama Anda akan menggabungkan instans EC2 secara manual ke domain lokal Anda. Setelah itu Anda dapat mempromosikan server ke pengendali domain.

Untuk mempromosikan server Anda ke pengendali domain

1. Di konsol Amazon EC2, pilih Instans, pilih Instans yang baru saja Anda buat, kemudian pilih Hubungkan.
2. Di kotak dialog Hubungkan ke Instans Anda, pilih Unduh File Remote Desktop.
3. Di kotak dialog Keamanan Windows, ketik kredensial administrator lokal Anda untuk komputer Windows Server untuk masuk (misalnya, **administrator**). Jika Anda belum memiliki kata sandi administrator lokal, kembali ke konsol Amazon EC2, klik kanan pada instans, dan pilih Dapatkan Kata Sandi Windows. Arahkan ke file AWS_DS_KP.pem Anda atau kunci .pem pribadi Anda, dan kemudian pilih Dekripsi Kata sandi.
4. Dari menu Mulai, pilih Pengelola Server.
5. Di Dasbor, pilih Tambah Peran dan Fitur.
6. Di Tambahkan Wizard Peran dan Fitur, pilih Selanjutnya.
7. Pada halaman Pilih jenis instalasi, pilih Instalasi berbasis peran atau berbasis fitur, lalu pilih Selanjutnya.
8. Pada halaman Pilih server tujuan, pastikan bahwa server lokal dipilih, dan kemudian pilih Selanjutnya.
9. Pada halaman Pilih peran server, pilih Layanan Domain Direktori Aktif. Di kotak dialog Tambahkan Wizard Peran dan Fitur, verifikasi bahwa kotak centang Sertakan alat manajemen (jika ada) dipilih. Pilih Tambahkan Fitur, lalu pilih Selanjutnya.
10. Pada halaman Pilih fitur, pilih Selanjutnya.
11. Pada halaman Layanan Domain Direktori Aktif, pilih Selanjutnya.
12. Pada halaman Konfirmasi pilihan instalasi, pilih Instal.
13. Setelah binari Direktori Aktif diinstal, pilih Tutup.
14. Ketika Pengelola Server terbuka, cari bendera di atas sebelah kata Kelola. Ketika bendera ini berubah kuning, server siap untuk dipromosikan.
15. Pilih bendera kuning, dan kemudian pilih Mempromosikan server ini ke pengendali domain.

16. Pada halaman Konfigurasi Deployment, pilih Menambahkan forest baru. Di Nama domain root ketik **example.local**, lalu pilih Selanjutnya.
17. Pada halaman Opsi Pengendali Domain, lakukan hal berikut:
 - Di Tingkat fungsional forest dan Tingkat fungsional domain, pilih Windows Server 2016.
 - Di bawah Tentukan kemampuan pengontrol domain, verifikasi bahwa server DNS dan Katalog Global (GC) dipilih.
 - Ketik dan kemudian konfirmasi kata sandi Directory Services Restore Mode (DSRM). Lalu pilih Selanjutnya.
18. Pada halaman Opsi DNS, abaikan peringatan tentang delegasi dan pilih Selanjutnya.
19. Pada halaman Opsi tambahan, pastikan EXAMPLE terdaftar sebagai nama NetBios domain.
20. Pada halaman Jalur, biarkan default, dan kemudian pilih Selanjutnya.
21. Pada halaman Tinjau opsi, pilih Selanjutnya. Server sekarang memeriksa untuk memastikan semua prasyarat untuk pengendali domain terpenuhi. Anda mungkin melihat beberapa peringatan ditampilkan, namun Anda dapat mengabaikannya dengan aman.
22. Pilih Instal. Setelah instalasi selesai, server akan reboot dan kemudian menjadi pengendali domain fungsional.

Mengkonfigurasi VPC Anda

Tiga prosedur berikut memandu Anda melalui langkah-langkah untuk mengkonfigurasi VPC Anda untuk konektivitas dengan AWS.

Untuk mengkonfigurasi aturan keluar VPC Anda

1. [Di AWS Directory Service konsol, catat ID direktori Microsoft AD AWS Terkelola untuk corp.example.com yang sebelumnya Anda buat di tutorial Base.](#)
2. Buka konsol Amazon VPC di <https://console.aws.amazon.com/vpc/>
3. Pada panel navigasi, pilih Grup Keamanan.
4. Cari ID direktori Microsoft AD AWS Terkelola Anda. Dalam hasil pencarian, pilih item dengan deskripsi yang AWS dibuat grup keamanan untuk pengontrol **xxxxxx** direktori d.

Note

Grup keamanan ini secara otomatis dibuat ketika Anda awalnya membuat direktori Anda.

5. Pilih tab Aturan Keluar di bawah grup keamanan tersebut. Pilih Edit, pilih Tambahkan aturan lain, dan kemudian tambahkan nilai-nilai berikut:
 - Untuk Jenis, pilih Semua lalu lintas.
 - Untuk Tujuan, ketik **0.0.0.0/0**.
 - Biarkan pengaturan lainnya pada default.
 - Pilih Simpan.

Untuk memverifikasi praautentikasi kerberos diaktifkan

1. Pada pengendali domain example.local, buka Pengelola Server.
2. Pada menu Alat, pilih Pengguna dan komputer Direktori Aktif.
3. Arahkan ke direktori Pengguna, klik kanan pada pengguna mana pun dan pilih Properti, dan kemudian pilih tab Akun. Di daftar Opsi akun, gulir ke bawah dan pastikan bahwa Tidak memerlukan praautentikasi Kerberos tidak dicentang.
4. Lakukan langkah yang sama untuk domain corp.example.com dari instans corp.example.com-mgmt.

Untuk mengkonfigurasi DNS penerus bersyarat

 Note

Penerus bersyarat adalah server DNS pada jaringan yang digunakan untuk meneruskan kueri DNS sesuai dengan nama domain DNS dalam kueri tersebut. Sebagai contoh, server DNS dapat dikonfigurasi untuk meneruskan semua kueri yang diterima untuk nama yang berakhir dengan widgets.example.com ke alamat IP server DNS tertentu atau ke alamat IP dari beberapa server DNS.

1. Buka [konsol AWS Directory Service](#).
2. Di panel navigasi, pilih Direktori.
3. Pilih ID direktori iklan Microsoft AWS Terkelola Anda.
4. Perhatikan nama domain yang memenuhi syarat (FQDN), corp.example.com, dan alamat DNS dari direktori Anda.
5. Sekarang, kembali ke pengendali domain example.local, dan kemudian buka Pengelola Server.

6. Pada menu Alat, pilih DNS.
7. Pada pohon konsol, perluas server DNS dari domain di mana Anda mengatur kepercayaan, dan arahkan ke Penerus Bersyarat.
8. Klik kanan Penerus Bersyarat, lalu pilih Penerus Bersyarat Baru.
9. Dalam domain DNS, ketik **corp.example.com**.
10. Di bawah alamat IP server utama, pilih <Klik di sini untuk menambahkan... >, ketik alamat DNS pertama dari direktori Microsoft AD AWS Terkelola Anda (yang Anda catat dalam prosedur sebelumnya), lalu tekan Enter. Lakukan hal yang sama untuk alamat DNS kedua. Setelah memasukkan alamat DNS, Anda mungkin mendapatkan kesalahan “timeout” atau “tidak dapat menyelesaikan”. Anda biasanya dapat mengabaikan error ini.
11. Pilih kotak centang Menyimpan penerus bersyarat ini di Direktori Aktif dan mereplikasi sebagai berikut. Di menu drop-down, pilih Semua server DNS di Forest ini, lalu pilih OK.

Langkah 2: Buat trust

Di bagian ini, Anda membuat dua kepercayaan forest yang terpisah. Satu kepercayaan dibuat dari domain Direktori Aktif pada instans EC2 Anda dan yang lainnya dari Microsoft AD yang AWS Dikelola. AWS



Untuk membuat kepercayaan dari domain EC2 Anda ke Microsoft AD yang AWS Dikelola

1. Masuk ke example.local.
2. Buka Pengelola Server dan di pohon konsol pilih DNS. Catat IPv4 alamat yang tercantum untuk server. Anda akan membutuhkan ini dalam prosedur berikutnya ketika Anda membuat penerus bersyarat dari corp.example.com ke direktori example.local.
3. Pada menu Alat, pilih Domain Direktori Aktif dan Kepercayaan.
4. Pada pohon konsol tersebut, klik kanan example.local lalu pilih Properti.
5. Pada tab Kepercayaan, pilih Kepercayaan Baru, lalu pilih Selanjutnya.
6. Pada halaman Nama Kepercayaan, ketik **corp.example.com**, lalu pilih Selanjutnya.

7. Pada halaman Jenis kepercayaan, pilih Kepercayaan forest, lalu pilih Selanjutnya.

 Note

AWS Microsoft AD yang dikelola juga mendukung kepercayaan eksternal. Namun, untuk tujuan tutorial ini, Anda akan membuat kepercayaan forest dua arah.

8. Pada halaman Arah kepercayaan, pilih Dua arah, lalu pilih Selanjutnya.

 Note

Jika nanti Anda memutuskan untuk mencoba ini dengan kepercayaan satu arah, pastikan arah kepercayaan diatur dengan benar (Keluar pada domain terpercaya, Masuk pada domain terpercaya). Untuk informasi umum, lihat [Memahami arah kepercayaan](#) pada situs web Microsoft.

9. Pada halaman Sisi Kepercayaan, pilih Hanya domain ini, lalu pilih Selanjutnya.
10. Pada halaman Autentikasi Kepercayaan Keluar, pilih Autentikasi seluruh forest, lalu pilih Selanjutnya.

 Note

Meskipun Autentikasi selektif dalam pilihan, untuk kesederhanaan dari tutorial ini kami sarankan Anda tidak mengaktifkannya di sini. Saat dikonfigurasi itu membatasi akses melalui kepercayaan eksternal atau forest hanya untuk pengguna di domain terpercaya atau forest yang telah secara eksplisit diberikan izin autentikasi ke objek komputer (komputer sumber daya) yang berada di domain atau forest terpercaya. Untuk informasi selengkapnya, lihat [Mengkonfigurasi pengaturan autentikasi selektif](#).

11. Pada halaman Kata sandi Kepercayaan, ketik kata sandi kepercayaan dua kali, dan kemudian pilih Selanjutnya. Anda akan menggunakan kata sandi yang sama ini pada prosedur berikutnya.
12. Pada halaman Pilihan Kepercayaan Selesai, tinjau hasilnya, dan kemudian pilih Selanjutnya.
13. Pada halaman Pembuatan Kepercayaan Selesai, tinjau hasilnya, dan kemudian pilih Selanjutnya.
14. Pada halaman Konfirmasi Kepercayaan Keluar, pilih Tidak, jangan mengkonfirmasi kepercayaan keluar. Lalu pilih Selanjutnya

15. Pada halaman Konfirmasi Kepercayaan Masuk, pilih Tidak, jangan mengonfirmasi kepercayaan masuk. Lalu pilih Selanjutnya
16. Pada halaman Menyelesaikan Wizard Kepercayaan Baru, pilih Selesai.

 Note

Hubungan kepercayaan adalah fitur global dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan [Konfigurasi replikasi Multi-Wilayah untuk AWS Microsoft AD yang Dikelola](#), prosedur berikut harus dilakukan di [Region primer](#). Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat [Fitur Global vs Regional](#).

Untuk membuat kepercayaan dari Microsoft AD yang AWS Dikelola ke domain EC2 Anda

1. Buka [konsol AWS Directory Service](#).
2. Pilih direktori corp.example.com.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. Di kotak dialog Tambahkan hubungan kepercayaan, lakukan hal berikut:
 - Di bawah Jenis kepercayaan pilih Kepercayaan forest.

 Note

Pastikan jenis Trust yang Anda pilih di sini cocok dengan jenis kepercayaan yang sama yang dikonfigurasi dalam prosedur sebelumnya (Untuk membuat kepercayaan dari domain EC2 Anda ke Microsoft AD yang AWS Dikelola).

- Untuk Nama domain jarak jauh yang ada atau baru, ketik example.local.

- Untuk Kata sandi kepercayaan, ketik kata sandi yang sama yang Anda berikan dalam prosedur sebelumnya.
- Di bawah Arah kepercayaan, pilih Dua Arah.

 Note

- Jika nanti Anda memutuskan untuk mencoba ini dengan kepercayaan satu arah, pastikan arah kepercayaan diatur dengan benar (Keluar pada domain terpercaya, Masuk pada domain terpercaya). Untuk informasi umum, lihat [Memahami arah kepercayaan](#) pada situs web Microsoft.
 - Meskipun Autentikasi selektif dalam pilihan, untuk kesederhanaan dari tutorial ini kami sarankan Anda tidak mengaktifkannya di sini. Saat dikonfigurasi itu membatasi akses melalui kepercayaan eksternal atau forest hanya untuk pengguna di domain terpercaya atau forest yang telah secara eksplisit diberikan izin autentikasi ke objek komputer (komputer sumber daya) yang berada di domain atau forest terpercaya. Untuk informasi selengkapnya, lihat [Mengkonfigurasi pengaturan autentikasi selektif](#).
- Untuk Penerus bersyarat, ketik alamat IP server DNS Anda di forest example.local (yang Anda catat dalam prosedur sebelumnya).

 Note

Penerus bersyarat adalah server DNS pada jaringan yang digunakan untuk meneruskan kueri DNS sesuai dengan nama domain DNS dalam kueri tersebut. Sebagai contoh, server DNS dapat dikonfigurasi untuk meneruskan semua kueri yang diterima untuk nama yang berakhir dengan widgets.example.com ke alamat IP server DNS tertentu atau ke alamat IP dari beberapa server DNS.

6. Pilih Tambahkan.

Langkah 3: Verifikasi kepercayaan

Di bagian ini, Anda menguji apakah kepercayaan berhasil diatur antara AWS dan Direktori Aktif di Amazon EC2.

Untuk memverifikasi kepercayaan

1. Buka [konsol AWS Directory Service](#).
2. Pilih direktori corp.example.com.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
 - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).
 - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih hubungan kepercayaan yang baru saja Anda buat.
5. Pilih Tindakan, lalu pilih Verifikasi hubungan kepercayaan.

Setelah verifikasi selesai, Anda akan melihat Diverifikasi ditampilkan di bawah kolom Status.

Selamat telah menyelesaikan tutorial ini! Anda sekarang memiliki lingkungan multiforest Direktori Aktif berfungsi penuh dari mana Anda dapat mulai menguji berbagai skenario. Tutorial laboratorium pengujian tambahan direncanakan pada tahun 2018, jadi periksa kembali sesekali untuk melihat apa yang baru.

AWS Kuota Microsoft AD yang dikelola

Berikut ini adalah kuota default untuk Microsoft AD yang AWS Dikelola. Kecuali dinyatakan lain, masing-masing kuota adalah per Region.

AWS Kuota Microsoft AD yang dikelola

Sumber daya	Kuota bawaan
AWS Direktori Microsoft AD yang dikelola (Edisi Standar dan Perusahaan)	20
AWS Direktori Microsoft AD yang dikelola (Edisi Hybrid)	5
Cuplikan manual (Edisi Standar dan Perusahaan) *	5 per Microsoft AD yang AWS Dikelola

Sumber daya	Kuota bawaan
Umur snapshot manual **	180 hari
Jumlah maksimum pengendali domain per direktori	20
Domain bersama untuk Microsoft AD Standar** *	25
Domain bersama untuk Microsoft AD Perusahaan***	500
Domain bersama untuk Microsoft AD Hybrid ***	125
Jumlah maksimum dari sertifikat otoritas sertifikasi (CA) terdaftar per direktori	5
Jumlah maksimum total AWS Wilayah dalam satu direktori Microsoft AD (Enterprise Edition) AWS Terkelola ****	5

* Kuota snapshot manual tidak dapat diubah.

** Usia maksimum yang didukung dari snapshot manual adalah 180 hari dan tidak dapat diubah. Hal ini disebabkan oleh atribut Masa Hidup-Tombstone dari objek dihapus yang menentukan umur simpan yang berguna dari backup keadaan sistem dari Direktori Aktif. Tidak mungkin memulihkan dari snapshot yang lebih tua dari 180 hari. Untuk informasi selengkapnya, lihat [Masa simpan yang berguna dari backup keadaan sistem Direktori Aktif](#) di situs web Microsoft.

*** Kuota default domain bersama mengacu pada jumlah akun yang masing-masing direktori dapat dibagikan.

**** Ini termasuk 1 Wilayah utama dan hingga 4 Wilayah tambahan. Untuk informasi selengkapnya, lihat [Region utama vs tambahan](#).

Note

Anda tidak dapat melampirkan alamat IP publik ke AWS elastic network interface (ENI) Anda.

Untuk informasi mengenai desain aplikasi dan distribusi beban, lihat [Praktik terbaik saat memprogram aplikasi Anda untuk Microsoft AD yang AWS Dikelola](#).

Untuk kuota penyimpanan dan objek, lihat Tabel Perbandingan pada halaman [Penetapan harga Directory Service AWS](#).

Pemecahan Masalah AWS Microsoft AD yang Dikelola

Berikut ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temui saat membuat atau menggunakan Direktori Aktif AWS Microsoft AD Terkelola.

Masalah dengan Microsoft AD yang AWS Dikelola

Beberapa tugas pemecahan masalah hanya dapat diselesaikan oleh Dukungan. Berikut adalah beberapa tugasnya:

- Mulai ulang pengontrol domain Directory Service yang disediakan.
- [Memutakhirkan Microsoft AD yang AWS Dikelola](#).

Untuk membuat kasus dukungan, lihat [Membuat kasus dukungan dan manajemen kasus](#).

Masalah dengan Netlogon dan komunikasi saluran aman

Sebagai mitigasi terhadap [CVE-2020-1472](#), Microsoft telah merilis patching yang memodifikasi cara komunikasi saluran aman Netlogon diproses oleh pengontrol domain. Sejak diperkenalkannya perubahan Netlogon aman ini, beberapa koneksi Netlogon (server, workstation, dan validasi kepercayaan) mungkin tidak diterima oleh Microsoft AD yang Dikelola Anda. AWS

Untuk memverifikasi apakah masalah Anda terkait dengan Netlogon atau komunikasi saluran aman, cari CloudWatch Log Amazon Anda untuk peristiwa IDs 5827 (untuk masalah terkait otentikasi perangkat) atau 5828 (untuk masalah terkait validasi kepercayaan AD). Untuk selengkapnya tentang CloudWatch di Microsoft AD yang AWS Dikelola, lihat [Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS](#).

Untuk informasi lebih lanjut tentang mitigasi terhadap CVE-2020-1472, lihat [Cara mengelola perubahan dalam koneksi saluran aman Netlogon yang terkait dengan CVE-2020-1472 di situs web. Microsoft](#)

Anda menerima kesalahan 'Status Respons: 400 Permintaan Buruk' saat mencoba mengatur ulang kata sandi pengguna

Anda menerima pesan galat yang mirip dengan berikut ini saat mencoba mengatur ulang kata sandi pengguna:

Response Status: 400 Bad Request

Anda mungkin mengalami masalah ini ketika ada objek duplikat di Unit Organisasi Microsoft AD AWS Terkelola (OU) dengan nama login pengguna yang identik. Nama login pengguna harus unik. Lihat [Memecahkan masalah Data Direktori](#) dalam Microsoft dokumentasi untuk informasi selengkapnya.

Pemulihan kata sandi

Jika pengguna lupa kata sandi atau mengalami masalah saat masuk ke direktori Microsoft AD AWS Terkelola, Anda dapat mengatur ulang kata sandi mereka menggunakan file Konsol Manajemen AWS, PowerShell atau file. AWS CLI

Untuk informasi selengkapnya, lihat [Menyetel ulang kata sandi pengguna Microsoft AD yang AWS Dikelola](#).

Sumber daya tambahan

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengannya. AWS

- [AWS Pusat Pengetahuan](#) —Temukan FAQs dan tautkan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- [AWS Support Center](#) —Dapatkan dukungan teknis.
- [AWS Pusat Support Premium](#) —Dapatkan dukungan teknis premium.

Sumber daya berikut dapat membantu Anda memecahkan masalah Active Directory yang umum.

- [Dokumentasi Direktori Aktif](#)
- [AD DS Memecahkan masalah](#)

Topik

- [Kesalahan gabungan domain instans Amazon EC2 Linux](#)

- [AWS Microsoft AD yang dikelola ruang penyimpanan rendah yang tersedia](#)
- [Kesalahan ekstensi skema](#)
- [Alasan status pembuatan kepercayaan](#)
- [Pemecahan Masalah AWS Pemanfaatan CPU tinggi Microsoft AD yang Dikelola](#)

Kesalahan gabungan domain instans Amazon EC2 Linux

Berikut ini dapat membantu Anda memecahkan masalah beberapa pesan galat yang mungkin Anda temui saat menggabungkan instans Amazon EC2 Linux ke direktori AD Microsoft AWS Terkelola.

Instans Linux tidak dapat menggabungkan domain atau mengautentikasi

Instans Ubuntu 14.04, 16.04, dan 18.04 harus reverse-resolvable di DNS sebelum ranah dapat bekerja dengan Microsoft Active Directory. Jika tidak, Anda mungkin akan menjumpai salah satu dari dua skenario berikut:

Skenario 1: Instans Ubuntu yang belum bergabung ke ranah

Untuk instans Ubuntu yang mencoba bergabung dengan ranah, perintah `sudo realm join` mungkin tidak memberikan izin yang diperlukan untuk menggabungkan domain dan mungkin menampilkan kesalahan berikut:

```
! Tidak dapat mengautentikasi ke direktori aktif: SASL (-1): kegagalan generik: GSSAPI Kesalahan:
Nama yang tidak valid diberikan (Sukses) adcli: tidak dapat terhubung ke EXAMPLE.COM domain:
Tidak dapat mengautentikasi ke direktori aktif: SASL (-1): kegagalan generik: GSSAPI Kesalahan:
Nama yang tidak valid diberikan (Sukses)! Izin tidak mencukupi untuk bergabung dengan ranah
domain: Tidak dapat bergabung dengan ranah: Izin tidak mencukupi untuk bergabung dengan
domain
```

Skenario 2: Instans Ubuntu yang bergabung ke ranah

Untuk instance Ubuntu yang sudah bergabung dengan domain Microsoft Active Directory, upaya SSH ke instance menggunakan kredensial domain mungkin gagal dengan kesalahan berikut:

```
$ ssh admin@EXAMPLE.COM @198 .51.100
```

tidak ada identitas seperti itu:/Users/username/.ssh/id_ed25519: Tidak ada file atau direktori seperti itu

Kata sandi admin@EXAMPLE.COM @198 .51.100:

Izin ditolak, silakan coba lagi.

Kata sandi admin@EXAMPLE.COM @198.51.100:

Jika Anda masuk ke instans dengan kunci publik dan mencentang `/var/log/auth.log`, Anda mungkin melihat kesalahan berikut tentang tidak dapat menemukan pengguna:

```
12 Mei 01:02:12 ip-192-0-2-0 sshd [2251]: pam_unix (sshd: auth): kegagalan otentikasi; nama log = uid = 0 euid = 0 tty = ssh ruser = rhost = 203.0.113.0
```

```
12 Mei 01:02:12 ip-192-0-2-0 sshd [2251]: pam_sss (sshd: auth): kegagalan otentikasi; nama log = uid = 0 euid = 0 tty = ssh ruser= rhost = 203.0.113.0 pengguna = admin@EXAMPLE.COM
```

```
12 Mei 01:02:12 ip-192-0-2-0 sshd [2251]: pam_sss (sshd:auth): diterima untuk pengguna admin@EXAMPLE.COM: 10 (Pengguna tidak diketahui modul otentikasi yang mendasarinya)
```

```
12 Mei 01:02:14 ip-192-0-2-0 sshd [2251]: Kata sandi gagal untuk pengguna yang tidak valid admin@EXAMPLE.COM dari 203.0.113.0 port 13344 ssh2
```

```
12 Mei 01:02:15 ip-192-0-2-0 sshd [2251]: Koneksi ditutup oleh 203.0.113.0 [preauth]
```

Namun, kinit untuk pengguna masih bekerja. Lihat contoh ini:

```
ubuntu @ip -192-0-2-0: ~$ kinit admin@EXAMPLE.COM Kata sandi untuk admin@EXAMPLE.COM:
ubuntu @ip -192-0-2-0: ~$ klist Cache tiket: FILE: /tmp/krb5cc_1000 Prinsip default:
admin@EXAMPLE.COM
```

Solusi

Solusi yang direkomendasikan saat ini untuk kedua skenario ini adalah untuk menonaktifkan DNS terbalik di `/etc/krb5.conf` di bagian `[libdefaults]` seperti yang ditunjukkan di bawah ini:

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

Masalah autentikasi kepercayaan satu arah dengan penggabungan domain secara mulus.

Jika Anda memiliki kepercayaan keluar satu arah yang dibuat antara iklan Microsoft AWS Terkelola dan Direktori Aktif lokal, Anda mungkin mengalami masalah autentikasi saat mencoba

mengautentikasi terhadap instance Linux yang bergabung dengan domain menggunakan kredensi Direktori Aktif tepercaya Anda dengan Winbind.

Kesalahan

31 Juli 00:00:00 EC2 AMAZ- LSMWq T sshd [23832]: Kata sandi gagal untuk user@corp.example.com dari xxx.xxx.xxx.xxx port 18309 ssh2

31 Jul 00:05:00 EC2 AMAZ- LSMWq T sshd [23832]: pam_winbind (sshd: auth): mendapatkan kata sandi (0x00000390)

31 Jul 00:05:00 EC2 AMAZ- LSMWq T sshd [23832]: pam_winbind (sshd:auth): pam_get_item mengembalikan kata sandi

31 Jul 00:05:00 EC2 AMAZ- LSMWq T sshd [23832]: pam_winbind (sshd:auth): permintaan wbcLogonUser gagal: WBC_ERR_AUTH_ERROR, kesalahan PAM: PAM_SYSTEM_ERR (4), NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_FOUND**, Pesan kesalahan adalah: Nama objek tidak ditemukan.

31 Juli 00:05:00 EC2 AMAZ- LSMWq T sshd [23832]: pam_winbind (sshd:auth): kesalahan modul internal (retval = PAM_SYSTEM_ERR (4), pengguna = 'CORP\ user')

Solusi

Untuk mengatasi masalah ini, Anda perlu untuk mengomentari atau menghapus direktif dari file konfigurasi modul PAM (/etc/security/pam_winbind.conf) menggunakan langkah-langkah berikut.

1. Buka file /etc/security/pam_winbind.conf di editor teks.

```
sudo vim /etc/security/pam_winbind.conf
```

2. Mengomentari atau menghapus direktif berikut krb5_auth = yes.

```
[global]

cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. Menghentikan layanan Winbind, dan kemudian mulai lagi.

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

AWS Microsoft AD yang dikelola ruang penyimpanan rendah yang tersedia

Jika iklan Microsoft AWS Terkelola Anda terganggu karena Active Directory memiliki ruang penyimpanan yang tersedia rendah, tindakan segera diperlukan untuk mengembalikan direktori ke status aktif. Dua penyebab paling umum dari gangguan ini dibahas pada bagian di bawah ini:

1. [Folder SYSVOL menyimpan lebih dari objek kebijakan grup yang esensial](#)
2. [Basis data Direktori Aktif telah mengisi volume](#)

Untuk informasi harga tentang penyimpanan Microsoft AD AWS Terkelola, lihat [Directory Service Harga](#).

Folder SYSVOL menyimpan lebih dari objek kebijakan grup yang esensial

Penyebab umum dari gangguan ini adalah karena untuk menyimpan file yang non-esensial untuk pemrosesan kebijakan grup di folder SYSVOL. File-file yang tidak penting ini dapat berupa EXEs MSIs,, atau file lain yang tidak penting untuk diproses oleh Kebijakan Grup. Objek penting untuk memproses Kebijakan Grup adalah Objek Kebijakan Grup, Logon/off Skrip, dan [objek Central Store for Group Policy](#). File yang tidak penting harus disimpan di server file selain pengontrol domain Microsoft AD yang AWS Dikelola.

Jika file untuk [Instalasi Perangkat Lunak Kebijakan Grup](#) diperlukan Anda harus menggunakan server file untuk menyimpan file-file instalasi tersebut. Jika Anda memilih untuk tidak mengelola sendiri server file, AWS menyediakan opsi server file terkelola, [Amazon FSx](#).

Untuk menghapus file yang tidak perlu, Anda dapat mengakses berbagi SYSVOL melalui jalur konvensi penamaan universal (UNC). Misalnya, jika nama domain yang sepenuhnya memenuhi syarat (FQDN) domain Anda adalah example.com, jalur UNC untuk SYSVOL adalah "\\example.local\\SYSVOL\\example.local\\". Setelah Anda menemukan dan menghapus objek yang non-esensial bagi kebijakan grup untuk memproses direktori, itu akan kembali ke keadaan Aktif dalam waktu 30 menit. Jika setelah 30 menit direktori tidak aktif, silakan hubungi AWS Support.

Menyimpan file Kebijakan Grup penting saja di bagian SYSVOL Anda akan memastikan bahwa Anda tidak akan mengganggu direktori Anda karena SYSVOL penuh.

Basis data Direktori Aktif telah mengisi volume

Penyebab umum dari gangguan ini adalah karena basis data Direktori Aktif memenuhi volume. Untuk memverifikasi apakah ini masalahnya, Anda dapat meninjau jumlah total objek dalam direktori anda. Kami menebalkan kata total untuk memastikan bahwa Anda memahami objek yang dihapus masih dihitung dalam jumlah total objek dalam sebuah direktori.

Secara default Microsoft AD yang AWS Dikelola menyimpan item di Tempat Daur Ulang AD selama 180 hari sebelum menjadi Objek Daur Ulang. Setelah objek menjadi Objek-Daur ulang (tombstoned), objek itu dipertahankan selama 180 hari sebelum akhirnya dibersihkan dari direktori. Jadi ketika sebuah objek dihapus itu ada di dalam basis data direktori untuk 360 hari sebelum dibersihkan. Inilah sebabnya mengapa jumlah total objek perlu dievaluasi.

Untuk detail selengkapnya tentang jumlah objek yang didukung Microsoft AD yang AWS dikelola, lihat [Directory Service Harga](#).

Untuk mendapatkan jumlah total objek dalam direktori yang menyertakan objek yang dihapus, Anda dapat menjalankan PowerShell perintah berikut dari instance Windows yang bergabung dengan domain. Untuk langkah-langkah cara mengatur instans pengelolaan, lihat [Manajemen pengguna dan grup di Microsoft AD yang AWS Dikelola](#).

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |  
Select-Object -Property 'Count'
```

Di bawah ini adalah contoh output dari perintah di atas:

```
Count  
10000
```

Jika jumlah total di atas jumlah objek yang didukung untuk ukuran direktori yang tercantum dalam catatan di atas, Anda telah melampaui kapasitas direktori Anda.

Di bawah ini adalah pilihan untuk mengatasi gangguan ini:

1. Pembersihan AD

- a. Menghapus objek AD yang tidak diinginkan.

- b. Menghapus objek yang tidak diinginkan dari Keranjang Sampah AD. Ingat bahwa ini merusak dan satu-satunya cara untuk memulihkan objek yang dihapus itu adalah dengan melakukan pemulihan direktori.
- c. Perintah berikut akan menghapus semua objek yang dihapus dari Keranjang Sampah AD.

 Important

Gunakan perintah ini dengan hati-hati karena ini merusak dan satu-satunya cara untuk memulihkan objek yang dihapus itu adalah dengan melakukan pemulihan direktori.

```
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
{ ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like
'*\0ADEL:') }
Foreach ($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
$ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

- d. Buka kasing dengan AWS Support untuk meminta yang Directory Service merebut kembali ruang kosong.
2. Jika jenis direktori Anda adalah Edisi Standar Buka kasus dengan AWS Support yang meminta direktori Anda ditingkatkan ke Enterprise Edition. Ini juga akan meningkatkan biaya direktori Anda. Untuk informasi harga, lihat [Harga Directory Service](#).

Di Microsoft AD yang AWS Dikelola, anggota grup Administrator Seumur Hidup Objek yang Dihapus AWS Delegasi memiliki kemampuan untuk mengubah msDS-DeletedObjectLifetime atribut yang menetapkan jumlah waktu dalam hari objek yang dihapus disimpan di Tempat Daur Ulang AD sebelum menjadi Objek Daur Ulang.

 Note

Ini adalah topik lanjutan. Jika dikonfigurasi secara tidak tepat, dapat mengakibatkan kehilangan data. Kami sangat menyarankan Anda untuk meninjau terlebih dulu [Keranjang](#)

[Sampah AD: Memahami, Menerapkan, Praktik Terbaik, dan Pemecahan Masalah](#) untuk mendapatkan pemahaman yang lebih baik tentang proses-proses ini.

Kemampuan untuk mengubah nilai atribut `msDS-DeletedObjectLifetime` ke angka yang lebih rendah dapat membantu memastikan jumlah objek Anda tidak melebihi tingkat yang didukung. Nilai valid terendah atribut ini dapat diatur ke adalah 2 hari. Setelah nilai tersebut melampaui Anda tidak akan lagi dapat memulihkan objek yang dihapus menggunakan Keranjang Sampah AD. Ini akan perlu memulihkan direktori Anda dari snapshot untuk memulihkan objek. Untuk informasi selengkapnya, lihat [Memulihkan iklan Microsoft AWS Terkelola Anda dengan snapshot](#). Setiap pemulihan dari snapshot dapat mengakibatkan hilangnya data karena merupakan titik waktu.

Untuk mengubah Masa Hidup Objek yang Dihapus dari direktori Anda jalankan perintah berikut:

Note

Jika Anda menjalankan perintah seperti adanya, itu akan mengatur nilai atribut Masa Hidup Objek yang Dihapus untuk 30 hari. Jika Anda ingin membuatnya lebih panjang atau lebih pendek ganti "30" dengan nomor apa pun yang Anda inginkan. Namun, kami merekomendasikan agar Anda tidak mengaturnya lebih dari angka default 180.

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,$BaseDn" -Partition "CN=Configuration,$BaseDn" -
Replace:@{ "msDS-DeletedObjectLifetime" = $DeletedObjectLifetime }
```

Kesalahan ekstensi skema

Berikut ini dapat membantu Anda memecahkan masalah beberapa pesan galat yang mungkin Anda temui saat memperluas skema untuk direktori AWS Microsoft AD yang Dikelola.

Referensi

Kesalahan

Menambahkan kesalahan pada entri yang dimulai pada baris 1: Referral Kesalahan sisi server adalah: 0x202b Referral dikembalikan dari server. Kesalahan server yang diperluas adalah: 0000202B: RefErr: DSID-0310082F, data 0, 1 titik akses\ tref 1: 'example.com' Jumlah Objek yang Dimodifikasi: 0

Pemecahan masalah

Pastikan bahwa semua bidang nama yang dibedakan memiliki nama domain yang benar. Dalam contoh di atas, DC=example,dc=com harus diganti dengan DistinguishedName yang ditunjukkan oleh cmdlet Get-ADDomain.

Tidak dapat membaca file impor

Kesalahan

Tidak dapat membaca file impor Jumlah Objek yang Dimodifikasi: 0

Pemecahan masalah

File LDIF yang diimpor kosong (0 byte). Pastikan file yang benar telah diunggah.

Kesalahan sintaks

Kesalahan

Ada kesalahan sintaks dalam file input Gagal pada baris 21. Token terakhir dimulai dengan 'q'.
Jumlah Objek yang Dimodifikasi: 0

Pemecahan masalah

Teks pada baris 21 tidak diformat dengan benar. Huruf pertama dari teks yang tidak valid adalah A. Memperbarui baris 21 dengan sintaks LDIF valid. Untuk informasi selengkapnya tentang format file dalam jumlah besar, lihat [Langkah 1: Buat file LDIF Anda](#).

Atribut atau nilai ada

Kesalahan

Menambahkan kesalahan pada entri yang dimulai pada baris 1: Atribut atau Nilai Ada Kesalahan sisi server adalah: 0x2083 nilai yang ditentukan sudah ada. Kesalahan server yang diperluas adalah: 00002083:: DSID-03151830, #1 AtrErr:\ t0:00002083: DSID-03151830, masalah 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (MayContain) :len 4 Jumlah Objek yang Dimodifikasi: 0

Pemecahan masalah

Perubahan skema telah diterapkan.

Tidak ada atribut tersebut

Kesalahan

Menambahkan kesalahan pada entri yang dimulai pada baris 1: Tidak Ada Atribut Tersebut Kesalahan sisi server adalah: 0x2085 Nilai atribut tidak dapat dihapus karena tidak ada pada objek. Kesalahan server yang diperluas adalah: 00002085:: DSID-03152367, #1 AtrErr:\ t0:00002085: DSID-03152367, masalah 1001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20019 (MayContain) :len 4 Jumlah Objek yang Dimodifikasi: 0

Pemecahan masalah

File LDIF mencoba untuk menghapus atribut dari kelas, tapi atribut saat ini tidak melekat pada kelas. Perubahan skema mungkin sudah diterapkan.

Kesalahan

Menambahkan kesalahan pada entri mulai pada baris 41: Tidak ada atribut tersebut 0x57 Parameter tidak benar. Kesalahan server yang diperpanjang adalah: 0x208d Objek direktori tidak ditemukan. Kesalahan server yang diperluas adalah: "00000057:: DSID-0C090D8A, komentar LdapErr: Kesalahan dalam operasi konversi atribut, data 0, v2580" Jumlah Objek Dimodifikasi: 0

Pemecahan masalah

Atribut yang tercantum pada baris 41 tidak benar. Periksa kembali ejaannya.

Tidak ada objek tersebut

Kesalahan

Menambahkan kesalahan pada entri mulai pada baris 1: Tidak Ada Objek Tersebut Kesalahan sisi server adalah: 0x208d Objek direktori tidak ditemukan. Kesalahan server yang diperluas adalah: 0000208D: NameErr: DSID-03100238, masalah 2001 (NO_OBJECT), data 0, kecocokan terbaik: 'Cn = Skema, CN = konfigurasi, DC = Contoh, DC = com' Jumlah Objek yang Dimodifikasi: 0

Pemecahan masalah

Objek yang direferensikan oleh nama yang dibedakan (DN) tidak ada.

Alasan status pembuatan kepercayaan

Jika pembuatan kepercayaan gagal untuk Microsoft AD yang AWS Dikelola, pesan status berisi informasi tambahan. Berikut ini dapat membantu Anda memahami apa arti pesan-pesan itu.

Akses ditolak

Akses ditolak ketika mencoba untuk membuat kepercayaan. Entah kata sandi kepercayaan salah atau pengaturan keamanan domain jarak jauh tidak memungkinkan kepercayaan untuk dikonfigurasi. Untuk informasi lebih lanjut tentang trust, lihat [Meningkatkan Efisiensi Kepercayaan dengan Nama Situs dan DCLocator](#). Untuk menyelesaikan masalah ini, coba hal berikut:

- Verifikasi bahwa Anda menggunakan kata sandi kepercayaan yang sama yang Anda gunakan saat membuat kepercayaan yang sesuai pada domain jarak jauh.
- Verifikasi bahwa pengaturan keamanan domain Anda mengizinkan pembuatan kepercayaan.
- Verifikasi bahwa kebijakan keamanan lokal Anda diatur dengan benar. Periksa secara khusus Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously dan pastikan bahwa itu berisi setidaknya tiga pipe bernama berikut:
 - netlogon
 - samr
 - lsarpc
- Verifikasi bahwa pipa bernama di atas ada sebagai nilai pada kunci NullSessionPipesregistri yang ada di jalur registri HKLM\SYSTEM\services\CurrentControlSet\Parameters LanmanServer. Nilai-nilai ini harus disisipkan pada baris yang terpisah.

 Note

Secara default, Network access: Named Pipes that can be accessed anonymously tidak diatur dan akan menampilkan Not Defined. Ini adalah normal, sebagai pengendali domain efektif pengaturan default untuk Network access: Named Pipes that can be accessed anonymously adalah netlogon, samr, lsarpc.

- Verifikasi Pengaturan Penandatanganan Blok Pesan Server (SMB) berikut dalam Kebijakan Pengontrol Domain Default. Pengaturan ini dapat ditemukan di bawah Konfigurasi Komputer> Pengaturan Windows> Pengaturan Keamanan> Kebijakan Lokal/Opsi Keamanan. Mereka harus cocok dengan pengaturan berikut:
 - Microsoftklien jaringan: Komunikasi tanda tangani secara digital (selalu): Default: Diaktifkan
 - Microsoftserver jaringan: Komunikasi tanda tangani secara digital (selalu): Diaktifkan

Meningkatkan Efisiensi Kepercayaan dengan Nama Situs dan DCLocator

Nama Situs Pertama seperti Default-First-Site-Name bukan persyaratan untuk membangun hubungan kepercayaan antar domain. Namun, menyelaraskan nama situs antar domain dapat secara signifikan meningkatkan efisiensi proses Domain Controller Locator ()DCLocator. Penyelarasan ini meningkatkan prediksi dan pengendalian pemilihan pengendali domain di seluruh perwalian hutan.

DCLocator Proses ini sangat penting untuk menemukan pengontrol domain di berbagai domain dan hutan. Untuk informasi lebih lanjut tentang DCLocator proses, lihat [Microsoftdokumentasi](#). Konfigurasi situs yang efisien memungkinkan lokasi pengontrol domain yang lebih cepat dan akurat, yang mengarah pada kinerja dan keandalan yang lebih baik dalam operasi lintas hutan.

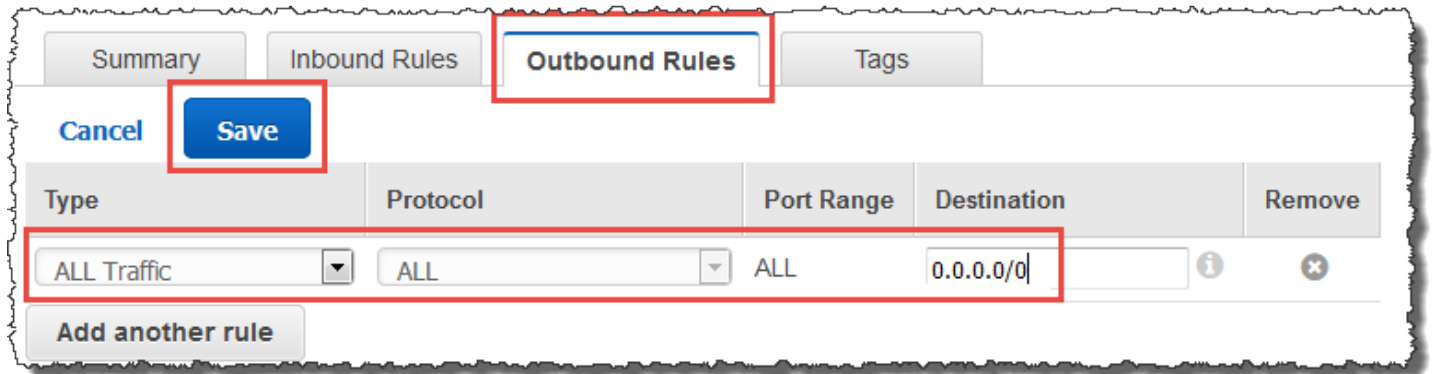
Untuk informasi selengkapnya tentang cara nama situs dan DCLocator proses berinteraksi, lihat Microsoft artikel berikut:

- [Bagaimana Pengontrol Domain Berlokasi di Seluruh Perwalian](#)
- [Pencari Lokasi Domain Lintas Hutan](#)

Nama domain yang ditentukan tidak ada atau tidak dapat dihubungi

Untuk mengatasi masalah ini, pastikan pengaturan grup keamanan untuk domain dan daftar kontrol akses (ACL) untuk VPC Anda sudah benar dan Anda telah memasukkan informasi untuk forwarder

bersyarat Anda secara akurat. AWS mengkonfigurasi grup keamanan untuk membuka hanya port yang diperlukan untuk komunikasi Active Directory. Dalam konfigurasi default, grup keamanan menerima lalu lintas ke port-port ini dari alamat IP mana pun. Lalu lintas keluar dibatasi untuk grup keamanan. Anda perlu memperbarui aturan keluar pada grup keamanan untuk mengizinkan lalu lintas ke jaringan on-premise Anda. Untuk informasi lebih lanjut tentang persyaratan keamanan, silakan lihat [Langkah 2: Siapkan Microsoft AD yang AWS Dikelola](#).



Jika server DNS untuk jaringan direktori lain menggunakan alamat IP publik (non-RFC 1918), Anda perlu menambahkan rute IP pada direktori dari konsol Directory Services untuk Server DNS. Untuk informasi selengkapnya, lihat [Membuat, memverifikasi, atau menghapus hubungan kepercayaan dan Prasyarat](#).

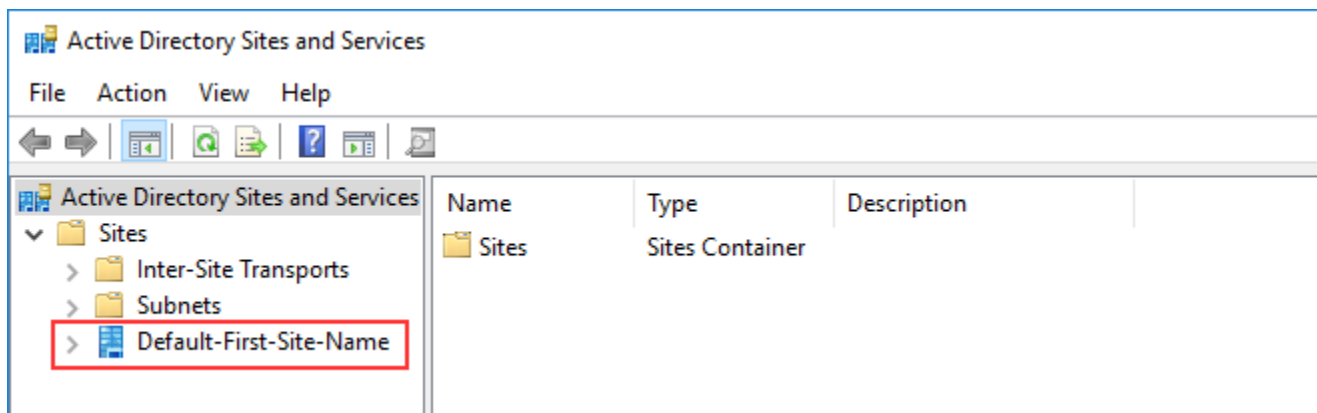
Internet Assigned Numbers Authority (IANA) telah menyediakan tiga blok dari ruang alamat IP berikut untuk internet pribadi:

- 10.0.0.0 - 10.255.255.255 (prefiks 10/8)
- 172.16.0.0 - 172.31.255.255 (prefiks 172.16/12)
- 192.168.0.0 - 192.168.255.255 (prefiks 192.168/16)

Untuk informasi lebih lanjut, lihat <https://tools.ietf.org/html/rfc1918>.

Verifikasi bahwa Nama Situs AD Default untuk iklan Microsoft AWS Terkelola cocok dengan Nama Situs AD Default di infrastruktur lokal Anda. Komputer menentukan nama situs menggunakan domain yang di mana komputer adalah anggota, bukan domain pengguna. Mengganti nama situs agar sesuai dengan on-premise terdekat memastikan pencari lokasi DC akan menggunakan pengendali domain dari situs terdekat. Jika ini tidak menyelesaikan masalah, ada kemungkinan bahwa informasi dari penerus bersyarat yang dibuat sebelumnya telah di-cache, mencegah pembuatan kepercayaan baru. Tunggu beberapa menit, dan kemudian coba buat kepercayaan dan penerus bersyarat lagi.

Untuk informasi selengkapnya tentang cara kerjanya, lihat [Domain Locator Across a Forest Trust](#) di Microsoft situs web.



Operasi tidak dapat dilakukan pada domain ini

Untuk mengatasi hal ini, pastikan kedua domain / direktori tidak memiliki nama NETBIOS yang tumpang tindih. Jika domain / direktori memiliki nama NETBIOS yang tumpang tindih, buat kembali salah satu dari mereka dengan nama NETBIOS yang berbeda, dan kemudian coba lagi.

Pembuatan kepercayaan gagal karena kesalahan “Nama domain yang diperlukan dan valid”

Nama DNS hanya bisa berisi karakter abjad (A-Z), karakter numerik (0-9), tanda minus (-), dan titik (.). Karakter titik diperbolehkan hanya ketika mereka digunakan untuk membatasi komponen nama gaya domain. Juga, pertimbangkan hal berikut:

- AWS Microsoft AD yang dikelola tidak mendukung kepercayaan dengan domain label tunggal. Untuk informasi selengkapnya, lihat [Microsoft dukungan untuk Domain Label Tunggal](#).
- Menurut RFC 1123 (<https://tools.ietf.org/html/rfc1123>), satu-satunya karakter yang dapat digunakan dalam label DNS adalah “A” hingga “Z”, “a” hingga “z”, “0” hingga “9”, dan tanda hubung (“-”). Titik [.] juga digunakan dalam nama DNS, tetapi hanya antara label DNS dan pada akhir dari FQDN.
- Menurut RFC 952 (<https://tools.ietf.org/html/rfc952>), “nama” (Net, Host, Gateway, atau nama Domain) adalah string teks hingga 24 karakter yang diambil dari alfabet (A-Z), digit (0-9), tanda minus (-), dan titik (.). Perhatikan bahwa titik hanya diperbolehkan ketika berfungsi untuk membatasi komponen “nama gaya domain”.

Untuk informasi selengkapnya, lihat [Mematuhi Pembatasan Nama untuk Host dan Domain di Microsoft situs web](#).

Alat umum untuk menguji kepercayaan

Berikut ini adalah alat yang dapat digunakan untuk memecahkan berbagai masalah terkait kepercayaan.

AWS Alat pemecahan masalah Otomasi Systems Manager

[Support Automation Workflows \(SAW\)](#) memanfaatkan AWS Systems Manager Automation untuk memberi Anda runbook yang telah ditentukan sebelumnya. Directory Service Alat [AWS Support-TroubleshootDirectoryTrust](#) runbook membantu Anda mendiagnosis masalah pembuatan kepercayaan umum antara Microsoft AD yang AWS Dikelola dan Direktori Microsoft Aktif lokal.

DirectoryServicePortTest alat

Alat [DirectoryServicePortTest](#) pengujian dapat membantu saat memecahkan masalah pembuatan kepercayaan antara AWS Microsoft AD yang Dikelola dan Direktori Aktif lokal. Sebagai contoh tentang bagaimana alat dapat digunakan, lihat [Uji AD Connector Anda](#).

Alat NETDOM dan NLTEST

Administrator dapat menggunakan alat baris perintah Netdom dan Nltest untuk menemukan, menampilkan, membuat, menghapus, dan mengelola kepercayaan. Alat-alat ini berkomunikasi secara langsung dengan otoritas LSA pada pengendali domain. Untuk contoh tentang cara menggunakan alat ini, lihat [Netdom](#) dan [NLTEST](#) di situs web. Microsoft

Alat penangkap paket

Anda dapat menggunakan utilitas pengambilan paket Windows bawaan untuk menyelidiki dan memecahkan masalah jaringan potensial. Untuk informasi selengkapnya, lihat [Mengambil Jejak Jaringan tanpa menginstal apa pun](#).

Pemecahan Masalah AWS Pemanfaatan CPU tinggi Microsoft AD yang Dikelola

Berikut ini dapat membantu Anda memecahkan masalah CPU tinggi pada pengontrol domain AWS Microsoft AD Terkelola.

Menemukan akar penyebabnya

Langkah pertama dalam memecahkan masalah pemanfaatan CPU yang tinggi adalah menganalisis CloudWatch metrik untuk mengidentifikasi pola yang dapat menjelaskan peningkatan konsumsi sumber daya.

Langkah 1: Tinjau Directory Service CloudWatch metrik

Pantau performa Microsoft AD yang AWS Dikelola menggunakan CloudWatch metrik untuk mengidentifikasi pola lalu lintas yang berkorelasi dengan penggunaan CPU yang tinggi. Untuk informasi rinci tentang melihat dan menafsirkan Directory Service metrik, lihat. [Menggunakan CloudWatch untuk memantau kinerja pengontrol domain Microsoft AD yang AWS Dikelola](#)

Cari pola pergeseran dalam metrik kunci berikut yang mungkin menjelaskan peningkatan CPU:

- Kueri DNS per detik — Lonjakan mendadak dapat mengindikasikan masalah resolusi DNS atau aplikasi yang salah dikonfigurasi.
- Otentikasi Kerberos/NTLM — Tingkat otentikasi yang lebih tinggi dari login pengguna atau akun layanan.
- Kueri LDAP per detik — Peningkatan lalu lintas LDAP dari aplikasi atau layanan.

Bandingkan metrik saat ini dengan garis dasar historis untuk mengidentifikasi kapan pemanfaatan CPU yang tinggi dimulai dan menghubungkannya dengan peningkatan lalu lintas tertentu. Jika tidak ada korelasi yang ditemukan dalam metrik maka akar penyebabnya bukanlah peningkatan lalu lintas yang luar biasa. Alih-alih akar penyebabnya kemungkinan adalah kueri LDAP yang tidak efisien, lewati ke. [Langkah 3: Tangkap analisis lalu lintas terperinci dengan Traffic Mirroring](#)

Langkah 2: Identifikasi mesin sumber menggunakan VPC Flow Logs

VPC Flow Logs menyediakan metode yang efektif untuk mengidentifikasi alamat IP sumber mesin yang menghasilkan lalu lintas ke pengontrol domain Anda. Untuk informasi selengkapnya, lihat [Mencatat lalu lintas IP menggunakan Log Aliran VPC](#). Gunakan nomor port tujuan untuk membedakan antara layanan:

- Port 53 - Kueri DNS
- Port 88 — Otentikasi Kerberos
- Port 123 - Sinkronisasi jam NTP
- Pelabuhan 135, 49152-65535 — RPC
- Port 389, 636, 3268, 3269 - kueri LDAP (389 atau 3268 untuk LDAP standar, 636 atau 3269 untuk LDAPS)
- Port 445 - Berbagi file SMB (Kebijakan Grup)
- Port 464 — Perubahan kata sandi Kerberos
- Port 9389 — Layanan Web Direktori Aktif

Untuk mengaktifkan dan menganalisis Log Aliran VPC:

- Aktifkan Log Aliran VPC untuk subnet yang berisi pengontrol domain Anda. ENIs
- Filter log berdasarkan port tujuan untuk mengidentifikasi pola lalu lintas.
- Atur oleh sebagian and/or besar paket sebagian besar byte selama periode waktu.
- Analisis alamat IP sumber untuk menentukan mesin mana yang menghasilkan lalu lintas terbanyak.

Langkah 3: Tangkap analisis lalu lintas terperinci dengan Traffic Mirroring

VPC Flow Logs memberikan informasi terbatas tentang konten permintaan yang sebenarnya. Untuk analisis yang lebih rinci, pertimbangkan Traffic Mirroring untuk menangkap data paket lengkap. Untuk informasi selengkapnya, lihat [Memulai menggunakan Pencermatan Lalu Lintas untuk memantau lalu lintas jaringan](#). Ini sangat berguna ketika Anda perlu menganalisis:

- Kompleksitas dan efisiensi filter LDAP
- Pola kueri DNS tertentu
- Detail permintaan otentikasi

Traffic Mirroring memungkinkan Anda untuk menangkap paket jaringan lengkap yang dikirim ke instance pengontrol domain Anda, memungkinkan analisis mendalam tentang lalu lintas yang menyebabkan pemanfaatan CPU tinggi.

Langkah 4: Selidiki aplikasi sumber dan optimalkan lalu lintas

Setelah Anda mengidentifikasi mesin sumber dan pola lalu lintas, selidiki aplikasi yang menghasilkan lalu lintas:

- Tinjau konfigurasi aplikasi — Periksa apakah aplikasi membuat kueri yang tidak efisien atau permintaan yang berlebihan. Hindari hard coding aplikasi ke pengontrol domain tunggal.
- Analisis kueri LDAP - Kueri LDAP yang tidak efisien adalah penyebab paling umum dari CPU pengontrol domain tinggi. Cari filter kompleks yang bisa mendapatkan keuntungan dari pengindeksan atribut.
- Periksa cache DNS — Verifikasi bahwa caching klien DNS diaktifkan untuk mengurangi kueri berulang.
- Periksa pola otentikasi — Identifikasi apakah akun layanan terlalu sering mengautentikasi.

Strategi resolusi

Berdasarkan penyelidikan Anda, terapkan strategi pengoptimalan yang tepat:

Optimalkan aplikasi

- Optimalkan kueri LDAP — Tulis ulang kueri LDAP yang kompleks. Hindari pengaturan basis pencarian ke root domain dan sebagai gantinya konfigurasi ke OU di mana objek yang Anda cari berada. Hindari menggunakan lingkup pencarian yang melakukan pencarian subtree. Alih-alih menggunakan basis atau lingkup tingkat tunggal. Sertakan kelas objek dalam filter Anda. Misalnya, `(objectClass=user)` atau `(objectClass=computer)`. Hindari menggunakan wildcard di filter kecuali atribut diindeks. Tambahkan indeks jika pemindaian wildcard diperlukan. Untuk informasi selengkapnya, lihat [Perluas skema AD Microsoft AWS Terkelola Anda](#). Jangan mengindeks semuanya karena proses pengindeksan juga meningkatkan pemanfaatan CPU.

```
# Sample LDIF code to index the email attribute
dn: CN=mail,CN=Schema,CN=Configuration,DC=yourdomain,DC=com
changetype: modify
replace: searchFlags
searchFlags: 1
```

- Aktifkan cache klien DNS — Konfigurasi klien untuk menyimpan respons DNS secara lokal untuk mengurangi beban server.
- Implementasikan penyatuan koneksi — Konfigurasi aplikasi untuk menggunakan kembali koneksi LDAP daripada membuat yang baru untuk setiap kueri.

Skalakan infrastruktur direktori Anda

Jika optimasi lalu lintas tidak menyelesaikan pemanfaatan CPU yang tinggi:

- Tambahkan lebih banyak pengontrol domain — Skalakan dengan menggunakan pengontrol domain tambahan untuk mendistribusikan beban. Untuk informasi selengkapnya, lihat [Menerapkan pengontrol domain tambahan untuk AWS Microsoft AD yang Dikelola](#).
- Tingkatkan ke Enterprise Edition - Jika menggunakan Edisi Standar, tingkatkan ke Enterprise Edition untuk meningkatkan kapasitas dan kinerja CPU. Untuk informasi selengkapnya, lihat [Memutakhirkan Microsoft AD yang AWS Dikelola](#). Jika sudah menggunakan Enterprise Edition, Hubungi [AWS Dukungan](#) untuk peningkatan kapasitas.

Untuk informasi harga tentang edisi Microsoft AD AWS Terkelola, lihat [Directory Service Harga](#).

AD Connector

AD Connector adalah gateway direktori yang dapat digunakan untuk mengarahkan permintaan direktori ke lokal Microsoft Active Directory tanpa menyimpan informasi apa pun di cloud. AD Connector ada dalam dua ukuran, kecil dan besar. Konektor AD kecil dirancang untuk organisasi yang lebih kecil dan dimaksudkan untuk menangani jumlah operasi per detik yang rendah. Konektor AD besar dirancang untuk organisasi yang lebih besar dan dimaksudkan untuk menangani jumlah operasi per detik sedang hingga tinggi. Anda dapat menyebarkan beban aplikasi di beberapa AD Connector untuk diskalakan dengan kebutuhan performa Anda. Tidak ada batasan pengguna atau koneksi yang ditegakkan.

AD Connector tidak mendukung trust transitif Active Directory. Konektor AD dan domain Active Directory lokal Anda memiliki hubungan 1-ke-1. Artinya, untuk setiap domain lokal, termasuk domain anak di hutan Direktori Aktif yang ingin Anda autentikasi, Anda harus membuat AD Connector yang unik.

Note

AD Connector tidak dapat dibagikan dengan AWS akun lain. Jika ini adalah persyaratan, pertimbangkan untuk menggunakan Microsoft AD yang AWS Dikelola untuk [Bagikan iklan Microsoft yang AWS Dikelola](#). AD Connector juga tidak sadar multi-VPC, yang berarti bahwa AWS aplikasi seperti [WorkSpaces](#) harus disediakan ke dalam VPC yang sama dengan AD Connector Anda.

Setelah diatur, AD Connector menawarkan manfaat sebagai berikut:

- Pengguna akhir dan administrator TI Anda dapat menggunakan kredensi perusahaan yang ada untuk masuk ke AWS aplikasi seperti WorkSpaces,, WorkDocs atau Amazon. WorkMail
- Anda dapat mengelola AWS sumber daya seperti EC2 instans Amazon atau bucket Amazon S3 melalui akses berbasis peran IAM ke file. Konsol Manajemen AWS
- Anda dapat secara konsisten menerapkan kebijakan keamanan yang ada (seperti kedaluwarsa kata sandi, riwayat kata sandi, dan penguncian akun) baik pengguna atau administrator TI mengakses sumber daya di infrastruktur lokal atau di Cloud. AWS
- Anda dapat menggunakan AD Connector untuk mengaktifkan otentikasi multi-faktor dengan mengintegrasikan dengan infrastruktur MFA berbasis Radius yang ada untuk memberikan lapisan keamanan tambahan saat pengguna mengakses aplikasi. AWS

Lanjutkan membaca topik di bagian ini untuk mempelajari cara menghubungkan ke direktori dan memaksimalkan fitur AD Connector.

Topik

- [Memulai dengan AD Connector](#)
- [Praktik terbaik untuk AD Connector](#)
- [Memelihara direktori AD Connector](#)
- [Mengamankan direktori AD Connector Anda](#)
- [Memantau direktori AD Connector Anda](#)
- [Akses ke AWS aplikasi dan layanan dari AD Connector](#)
- [Cara untuk bergabung dengan EC2 instans Amazon ke Direktori Aktif Anda](#)
- [Kuota AD Connector](#)
- [Memecahkan masalah AD Connector](#)

Memulai dengan AD Connector

Dengan AD Connector, Anda dapat terhubung Directory Service ke Active Directory perusahaan yang ada. Ketika terhubung ke direktori Anda yang sudah ada, semua data direktori Anda tetap pada pengendali domain Anda. Directory Service tidak mereplikasi data direktori Anda.

Topik

- [Prasyarat AD Connector](#)
- [Membuat AD Connector](#)
- [Apa yang dibuat dengan AD Connector Anda](#)

Prasyarat AD Connector

Untuk terhubung ke direktori Anda yang sudah ada dengan AD Connector, anda memerlukan hal berikut:

Amazon VPC

Siapkan VPC dengan hal berikut:

- Setidaknya dua subnet. Masing-masing subnet harus berada di Availability Zone yang berbeda dan harus dari jenis jaringan yang sama.

Anda dapat menggunakan IPv6 untuk VPC Anda. Untuk informasi selengkapnya, lihat [IPv6 dukungan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.

- VPC harus terhubung ke jaringan Anda yang sudah ada melalui koneksi jaringan pribadi virtual (VPN) atau Direct Connect.
- VPC harus memiliki penghunian perangkat keras default.

Directory Service menggunakan dua struktur VPC. Instans EC2 yang membentuk direktori Anda berjalan di luar AWS akun Anda, dan dikelola oleh AWS Mereka memiliki dua adaptor jaringan, ETH0 dan ETH1. ETH0 adalah adaptor pengelola, dan berada di luar akun Anda. ETH1 dibuat dalam akun Anda.

Rentang IP pengelola jaringan ETH0 direktori Anda dipilih secara terprogram untuk memastikan tidak bertentangan dengan VPC tempat direktori Anda di-deploy. Rentang IP ini dapat berupa salah satu pasangan berikut (karena Direktori berjalan di dua subnet):

- 10.0.1.0/24 & 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 & 192.168.2.0/24

Kami menghindari konflik dengan memeriksa oktet pertama dari ETH1 CIDR. Jika dimulai dengan 10, maka kami memilih VPC 192.168.0.0/16 dengan subnet 192.168.1.0/24 dan 192.168.2.0/24. Jika oktet pertama adalah yang lain selain 10, kami memilih VPC 10.0.0.0/16 dengan subnet 10.0.1.0/24 dan 10.0.2.0/24.

Algoritma pemilihan tidak mencakup rute pada VPC Anda. Oleh karena itu Anda dapat mengalami konflik IP perutean yang dihasilkan dari skenario ini.

Untuk informasi selengkapnya, lihat topik berikut dalam Panduan Pengguna Amazon VPC:

- [Apa itu Amazon VPC?](#)
- [Subnet di VPC Anda](#)
- [Menambahkan Gerbang Pribadi Virtual Perangkat Keras ke VPC Anda](#)

Untuk informasi selengkapnya AWS Direct Connect, lihat [Panduan AWS Direct Connect Pengguna](#).

Direktori Aktif yang Ada

Anda harus terhubung ke jaringan yang ada dengan domain Active Directory.

 Note

AD Connector tidak mendukung [Domain Label Tunggal](#).

Tingkat fungsional domain Active Directory ini harus Windows Server 2003 atau lebih tinggi. AD Connector juga mendukung menghubungkan ke domain yang di-host di instans Amazon EC2.

 Note

AD Connector tidak mendukung pengendali domain baca-saja (RODC) jika digunakan dalam kombinasi dengan fitur penggabungan domain Amazon EC2.

Akun layanan

Anda harus memiliki kredensial untuk akun layanan di direktori yang sudah ada yang telah didelegasikan hak istimewa berikut:

- Membaca pengguna dan grup - Diperlukan
- Bergabunglah dengan komputer ke domain - Diperlukan hanya saat menggunakan Seamless Domain Join dan WorkSpaces
- Buat objek komputer - Diperlukan hanya saat menggunakan Seamless Domain Join dan WorkSpaces
- Kata sandi akun layanan harus sesuai dengan persyaratan AWS kata sandi. AWS kata sandi harus:
 - Panjangnya antara 8 dan 128 karakter, inklusif.
 - Berisi setidaknya satu karakter dari tiga dari empat kategori berikut:
 - Huruf kecil (a-z)
 - Huruf besar (A-Z)
 - Angka (0-9)
 - Karakter non-alfanumerik (~!@#\$%^&* _-+=`|\\(){}[]:;'"<>,.?/)

Untuk informasi selengkapnya, lihat [Mendelegasikan hak istimewa ke akun layanan Anda](#).

 Note

AD Connector menggunakan Kerberos untuk autentikasi dan otorisasi aplikasi AWS. LDAP hanya digunakan untuk pencarian objek pengguna dan grup (operasi baca). Dengan transaksi LDAP, tidak ada yang dapat berubah dan kredensial tidak diteruskan dalam teks yang jelas. Otentikasi ditangani oleh layanan AWS internal, yang menggunakan tiket Kerberos untuk melakukan operasi LDAP sebagai pengguna.

Izin pengguna

Semua pengguna Direktori Aktif harus memiliki izin untuk membaca atribut mereka sendiri. Secara spesifik yaitu atribut berikut:

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

Secara default, pengguna Direktori Aktif harus memiliki izin untuk membaca atribut-atribut ini. Namun, Administrator dapat mengubah izin ini dari waktu ke waktu sehingga Anda mungkin ingin memverifikasi bahwa pengguna Anda memiliki izin baca ini sebelum menyiapkan AD Connector untuk pertama kalinya.

Alamat IP

Dapatkan alamat IP dari dua server DNS atau pengendali domain di direktori yang ada.

AD Connector memperoleh catatan `_ldap._tcp.<DnsDomainName>` dan `_kerberos._tcp.<DnsDomainName>` SRV dari server ini saat menghubungkan ke direktori Anda, sehingga server ini harus berisi catatan SRV ini. AD Connector mencoba untuk menemukan pengendali domain umum yang akan menyediakan layanan LDAP dan Kerberos, sehingga data SRV ini harus mencakup setidaknya satu pengendali domain umum. Untuk informasi selengkapnya tentang catatan SRV, buka [SRV Resource Records](#) di Microsoft. TechNet

Port untuk subnet

Agar AD Connector mengalihkan permintaan direktori ke pengontrol domain Active Directory yang ada, firewall untuk jaringan yang ada harus memiliki port berikut yang terbuka CIDRs untuk kedua subnet di VPC Amazon Anda.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Autentikasi Kerberos
- TCP/UDP 389 - LDAP

Ini adalah port minimum yang diperlukan sebelum AD Connector dapat terhubung ke direktori Anda. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

Jika Anda ingin menggunakan AD Connector dan Amazon WorkSpaces, atribut Nonaktifkan VLVSuport LDAP harus disetel ke 0 untuk pengontrol domain Anda. Ini adalah pengaturan default untuk pengontrol domain. AD Connector tidak akan dapat menanyakan pengguna di direktori jika atribut Nonaktifkan VLVSuport LDAP diaktifkan. Ini mencegah AD Connector bekerja dengan Amazon WorkSpaces.

Note

Jika server DNS atau server Pengontrol Domain untuk Domain Direktori Aktif Anda yang ada berada dalam VPC, grup keamanan yang terkait dengan server tersebut harus memiliki port di atas terbuka untuk kedua CIDRs subnet di VPC.

Untuk persyaratan port tambahan, lihat [Persyaratan Port AD dan AD DS](#) pada Microsoft dokumentasi.

Pra-Autentikasi Kerberos

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Untuk petunjuk detail tentang cara mengaktifkan pengaturan ini, lihat [Pastikan bahwa Kerberos pra-autentikasi diaktifkan](#). Untuk informasi umum tentang pengaturan ini, buka [Preauthentication](#) on. Microsoft TechNet

Jenis enkripsi

AD Connector mendukung jenis enkripsi berikut ini ketika melakukan autentikasi melalui Kerberos ke pengendali domain Direktori Aktif Anda:

- AES-256-HMAC

- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center prasyarat

Jika Anda berencana untuk menggunakan IAM Identity Center dengan AD Connector, Anda perlu memastikan bahwa berikut ini benar:

- AD Connector Anda disiapkan di akun manajemen AWS organisasi Anda.
- Instance Pusat Identitas IAM Anda berada di Wilayah yang sama tempat AD Connector Anda disiapkan.

Untuk informasi selengkapnya, lihat [prasyarat Pusat Identitas IAM](#) di Panduan Pengguna. AWS IAM Identity Center

Prasyarat autentikasi multi-faktor

Untuk mendukung autentikasi multi-faktor dengan direktori AD Connector, Anda memerlukan yang berikut ini:

- Server [Remote Authentication Dial-In User Service](#) (RADIUS) di jaringan Anda yang ada yang memiliki dua titik akhir klien. Titik akhir klien RADIUS memiliki persyaratan sebagai berikut:
 - Untuk membuat titik akhir, Anda memerlukan alamat IP server Directory Service . Alamat IP ini dapat diperoleh dari bidang Direktori Alamat IP detail direktori Anda.
 - Kedua titik akhir RADIUS harus menggunakan kode rahasia bersama yang sama.
- Jaringan Anda yang ada harus mengizinkan lalu lintas masuk melalui port server RADIUS default (1812) dari server. Directory Service
- Nama pengguna antara server RADIUS Anda dan direktori Anda harus identik.

Untuk informasi selengkapnya tentang menggunakan AD Connector dengan MFA, lihat [Mengaktifkan otentikasi multi-faktor untuk AD Connector](#).

Mendelegasikan hak istimewa ke akun layanan Anda

Untuk menghubungkan ke direktori Anda, Anda harus memiliki kredensial untuk akun layanan AD Connector di direktori Anda yang telah didelegasikan hak istimewa tertentu. Walaupun anggota grup Admin Domain memiliki hak istimewa yang cukup untuk menghubungkan ke direktori, sebagai praktik

terbaik, Anda harus menggunakan akun layanan yang hanya memiliki hak istimewa minimum yang diperlukan untuk menghubungkan ke direktori. Prosedur berikut menunjukkan cara membuat grup baru yang disebut **Connectors**, mendelegasikan hak istimewa yang diperlukan untuk terhubung Directory Service ke grup ini, dan kemudian menambahkan akun layanan baru ke grup ini.

Prosedur ini harus dilakukan pada mesin yang telah digabungkan ke direktori Anda dan memiliki MMC snap-in Pengguna dan Komputer Direktori Aktif terinstal. Anda juga harus masuk sebagai administrator domain.

Untuk mendelegasikan hak istimewa ke akun layanan Anda

1. Buka Pengguna dan Komputer Direktori Aktif dan pilih root domain Anda di pohon navigasi.
2. Dalam daftar di panel sebelah kiri, klik kanan Pengguna, pilih Baru, lalu pilih Grup.
3. Di kotak dialog Objek Baru - Grup, masukkan yang berikut ini dan klik OKE.

Bidang	Nilai/Pemilihan
Nama grup	Connectors
Ruang lingkup kelompok	Global
Jenis grup	Keamanan

4. Di pohon navigasi Active Directory User and Computers, pilih identifikasi Unit Organisasi (OU) tempat akun komputer akan dibuat. Dalam menu, pilih Tindakan, lalu Delegasikan Kontrol. Anda dapat memilih OU induk hingga domain saat izin disebarkan ke anak. OUs Jika AD Connector Anda terhubung ke Microsoft AD yang AWS Dikelola, Anda tidak akan memiliki akses ke kontrol delegasi di tingkat root domain. Dalam kasus ini, untuk mendelegasikan kontrol, pilih OU di bawah direktori Anda OU Anda tempat objek komputer Anda akan dibuat.
5. Pada halaman Wizard Delegasi Kontrol, klik Selanjutnya, lalu klik Tambahkan.
6. Di kotak dialog Pilih Pengguna, Komputer, atau Grup, masukkan **Connectors** dan klik OKE. Jika ditemukan lebih dari satu objek, pilih grup **Connectors** yang dibuat di atas. Klik Berikutnya.
7. Pada halaman Tugas untuk Didelegasikan, pilih Buat tugas kustom untuk didelegasikan, lalu pilih Selanjutnya.
8. Pilih Hanya objek berikut dalam folder, lalu pilih Objek komputer dan Objek pengguna.
9. Pilih Buat objek yang dipilih dalam folder ini dan Hapus objek yang dipilih dalam folder ini. Lalu pilih Selanjutnya.

Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

☐ This folder, existing objects in this folder, and creation of new objects in this folder

☒ Only the following objects in the folder:

- ☐ Site Settings objects
- ☐ Sites Container objects
- ☐ Subnet objects
- ☐ Subnets Container objects
- ☐ Trusted Domain objects
- ☒ User objects

☒ Create selected objects in this folder

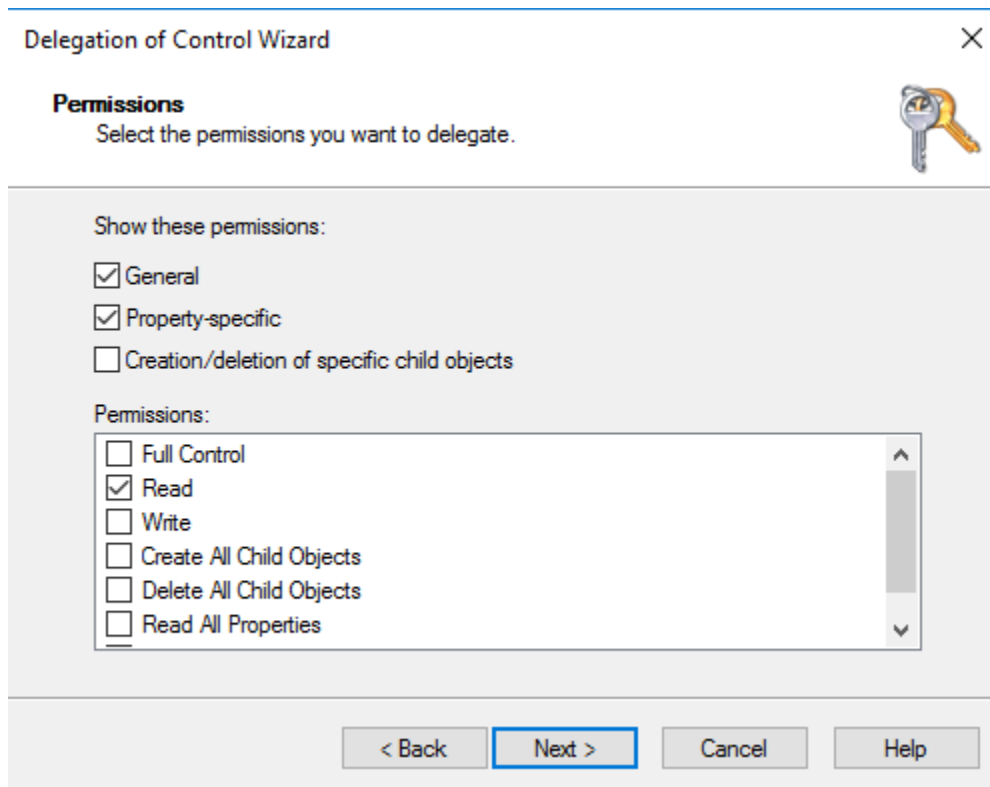
☒ Delete selected objects in this folder

< Back Next > Cancel Help

10. Pilih Baca, lalu pilih Selanjutnya.

Note

Jika Anda akan menggunakan Seamless Domain Join atau WorkSpaces, Anda juga harus mengaktifkan izin Tulis sehingga Active Directory dapat membuat objek komputer.



11. Verifikasi informasi pada halaman Wizard Menyelesaikan Delegasi Kontrol, dan klik Selesai.
12. Buat akun pengguna dengan kata sandi yang kuat dan tambahkan pengguna tersebut ke grup Connectors. Pengguna ini akan dikenal sebagai akun layanan AD Connector Anda dan karena sekarang menjadi anggota Connectors grup, sekarang memiliki hak istimewa yang cukup untuk terhubung Directory Service ke direktori.

Uji AD Connector Anda

Agar AD Connector dapat terhubung ke direktori yang ada, firewall untuk jaringan yang ada harus memiliki port tertentu yang terbuka CIDRs untuk kedua subnet di VPC. Untuk menguji apakah kondisi ini terpenuhi, lakukan langkah-langkah berikut:

Untuk menguji koneksi

1. Luncurkan instans Windows di VPC dan buat koneksi ke instans melalui RDP. Instans tersebut harus merupakan anggota domain Anda. Langkah-langkah yang tersisa dilakukan pada instans VPC ini.

2. Unduh dan unzip aplikasi [DirectoryServicePortTest](#) pengujian. Kode sumber dan file proyek Visual Studio disertakan sehingga Anda dapat memodifikasi aplikasi uji jika diinginkan.

 Note

Skrip ini tidak didukung pada Windows Server 2003 atau sistem operasi yang lebih tua.

3. Dari command prompt Windows, jalankan aplikasi uji DirectoryServicePortTest dengan opsi berikut:

 Note

Aplikasi DirectoryServicePortTest pengujian hanya dapat digunakan ketika tingkat fungsional domain dan hutan diatur ke Windows Server 2012 R2 dan di bawahnya.

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp  
"53,88,389" -udp "53,88,389"
```

<domain_name>

Nama domain yang memenuhi syarat. Ini digunakan untuk menguji tingkat fungsional hutan dan domain. Jika Anda mengecualikan nama domain, tingkat fungsional tidak akan diuji.

<server_IP_address>

Alamat IP dari pengendali domain di domain Anda. Port akan diuji terhadap alamat IP ini. Jika Anda mengecualikan alamat IP, port tidak akan diuji.

Aplikasi pengujian ini menentukan apakah port yang diperlukan terbuka dari VPC ke domain Anda, dan juga memverifikasi tingkat fungsional minimum hutan dan domain.

Output akan serupa dengan berikut ini.

```
Testing forest functional level.  
Forest Functional Level = Windows2008R2Forest : PASSED  
  
Testing domain functional level.  
Domain Functional Level = Windows2008R2Domain : PASSED
```


Testing required TCP ports to *<server_IP_address>*:

Checking TCP port 53: PASSED

Checking TCP port 88: PASSED

Checking TCP port 389: PASSED

Testing required UDP ports to *<server_IP_address>*:

Checking UDP port 53: PASSED

Checking UDP port 88: PASSED

Checking UDP port 389: PASSED

Berikut ini adalah kode sumber untuk aplikasi DirectoryServicePortTest.

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;

        private static string _domain = "";
        private static IPAddress _ipAddr = null;

        static void Main(string[] args)
        {
            if (ParseArgs(args))
```

```
{
    try
    {
        if (_domain.Length > 0)
        {
            try
            {
                TestForestFunctionalLevel();

                TestDomainFunctionalLevel();
            }
            catch (ActiveDirectoryObjectNotFoundException)
            {
                Console.WriteLine("The domain {0} could not be found.\n",
_domain);
            }
        }

        if (null != _ipAddr)
        {
            if (_tcpPorts.Count > 0)
            {
                TestTcpPorts(_tcpPorts);
            }

            if (_udpPorts.Count > 0)
            {
                TestUdpPorts(_udpPorts);
            }
        }
    }
    catch (AuthenticationException ex)
    {
        Console.WriteLine(ex.Message);
    }
}
else
{
    PrintUsage();
}

Console.Write("Press <enter> to continue.");
Console.ReadLine();
}
```

```
static void PrintUsage()
{
    string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
    Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
}

static bool ParseArgs(string[] args)
{
    bool fReturn = false;
    string ipAddress = "";

    try
    {
        _tcpPorts = new List<int>();
        _udpPorts = new List<int>();

        for (int i = 0; i < args.Length; i++)
        {
            string arg = args[i];

            if ("-tcp" == arg | "/tcp" == arg)
            {
                i++;
                string portList = args[i];
                _tcpPorts = ParsePortList(portList);
            }

            if ("-udp" == arg | "/udp" == arg)
            {
                i++;
                string portList = args[i];
                _udpPorts = ParsePortList(portList);
            }

            if ("-d" == arg | "/d" == arg)
            {
                i++;
                _domain = args[i];
            }
        }
    }
}
```

```
        if ("-ip" == arg | "/ip" == arg)
        {
            i++;
            ipAddress = args[i];
        }
    }
}
catch (ArgumentOutOfRangeException)
{
    return false;
}

if (_domain.Length > 0 || ipAddress.Length > 0)
{
    fReturn = true;
}

if (ipAddress.Length > 0)
{
    _ipAddr = IPAddress.Parse(ipAddress);
}

return fReturn;
}

static List<int> ParsePortList(string portList)
{
    List<int> ports = new List<int>();

    char[] separators = {',', ';', ':'};

    string[] portStrings = portList.Split(separators);
    foreach (string portString in portStrings)
    {
        try
        {
            ports.Add(Convert.ToInt32(portString));
        }
        catch (FormatException)
        {
        }
    }

    return ports;
}
```

```
}

static void TestForestFunctionalLevel()
{
    Console.WriteLine("Testing forest functional level.");

    DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
    Forest forestContext = Forest.GetForest(dirContext);

    Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

    if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
    {
        Console.WriteLine("PASSED");
    }
    else
    {
        Console.WriteLine("FAILED");
    }

    Console.WriteLine();
}

static void TestDomainFunctionalLevel()
{
    Console.WriteLine("Testing domain functional level.");

    DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
    Domain domainObject = Domain.GetDomain(dirContext);

    Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

    if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
    {
        Console.WriteLine("PASSED");
    }
    else
    {
        Console.WriteLine("FAILED");
    }
}
```

```
        Console.WriteLine();
    }

    static List<int> TestTcpPorts(List<int> portList)
    {
        Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

        List<int> failedPorts = new List<int>();

        foreach (int port in portList)
        {
            Console.Write("Checking TCP port {0}: ", port);

            TcpClient tcpClient = new TcpClient();

            try
            {
                tcpClient.Connect(_ipAddr, port);

                tcpClient.Close();
                Console.WriteLine("PASSED");
            }
            catch (SocketException)
            {
                failedPorts.Add(port);
                Console.WriteLine("FAILED");
            }
        }

        Console.WriteLine();

        return failedPorts;
    }

    static List<int> TestUdpPorts(List<int> portList)
    {
        Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

        List<int> failedPorts = new List<int>();

        foreach (int port in portList)
        {
            Console.Write("Checking UDP port {0}: ", port);
```

```
        UdpClient udpClient = new UdpClient();

        try
        {
            udpClient.Connect(_ipAddr, port);
            udpClient.Close();
            Console.WriteLine("PASSED");
        }
        catch (SocketException)
        {
            failedPorts.Add(port);
            Console.WriteLine("FAILED");
        }
    }

    Console.WriteLine();

    return failedPorts;
}
}
```

Membuat AD Connector

Untuk terhubung ke direktori Anda yang sudah ada dengan AD Connector, lakukan langkah-langkah berikut: Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikan prasyarat yang diidentifikasi dalam [Prasyarat AD Connector](#).

Note

Anda tidak dapat membuat AD Connector dengan template Cloud Formation.

Untuk menghubungkan dengan AD Connector

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori, lalu pilih Atur direktori.
2. Di halaman Pilih jenis direktori, pilih AD Connector, lalu pilih Selanjutnya.
3. Di halaman Masukkan informasi AD Connector, berikan informasi berikut:

Ukuran direktori

Pilih salah satu opsi ukuran Small atau Large. Untuk informasi selengkapnya tentang ukuran, lihat [AD Connector](#).

Deskripsi direktori

Deskripsi opsional untuk direktori.

4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.

VPC

VPC untuk direktori.

Subnet

Pilih subnet untuk pengendali domain. Kedua subnet harus berada di Zona Ketersediaan yang berbeda.

5. Di halaman Hubungkan ke AD, berikan informasi berikut:

Nama DNS direktori

Nama lengkap yang memenuhi syarat untuk direktori Anda, seperti `corp.example.com`.

Direktori nama NetBIOS

Nama pendek untuk direktori Anda, seperti CORP.

Alamat IP DNS

Alamat IP setidaknya satu server DNS di direktori yang ada. Server ini harus dapat diakses dari setiap subnet yang ditentukan pada langkah 4. Server ini dapat ditempatkan di luar AWS, selama ada konektivitas jaringan antara subnet yang ditentukan dan alamat IP server DNS.

Nama pengguna akun layanan

Nama pengguna dari pengguna di direktori yang ada. Untuk informasi selengkapnya tentang akun ini, lihat [Prasyarat AD Connector](#).

Kata sandi akun layanan

Kata sandi untuk akun pengguna yang ada. Kata sandi ini peka huruf besar/kecil dan panjangnya harus antara 8 dan 128 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:

- Huruf kecil (a-z)
- Huruf besar (A-Z)
- Angka (0-9)
- Karakter non-alfanumerik (~!@#\$%^&* _-+=`|(){}[]:;'"<>,.?/)

Konfirmasikan kata sandi

Ketik ulang kata sandi untuk akun pengguna yang sudah ada.

6. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Ini akan memerlukan beberapa menit sampai direktori dibuat. Setelah dibuat, nilai Status berubah ke Aktif.

Untuk informasi selengkapnya tentang apa yang dibuat dengan AD Connector, lihat [Apa yang dibuat dengan AD Connector Anda](#).

Apa yang dibuat dengan AD Connector Anda

Saat Anda membuat AD Connector, Directory Service secara otomatis membuat dan mengaitkan elastic network interface (ENI) dengan setiap instance AD Connector Anda. Masing-masing ENIs penting untuk konektivitas antara VPC dan Directory Service AD Connector Anda dan tidak boleh dihapus. Anda dapat mengidentifikasi semua antarmuka jaringan yang dicadangkan untuk digunakan Directory Service dengan deskripsi: "AWS menciptakan antarmuka jaringan untuk direktori-id direktori". Untuk informasi selengkapnya, lihat [Antarmuka Jaringan Elastis](#) di Panduan Pengguna Amazon EC2.

Note

Instans AD Connector di-deploy di dua Availability Zone di suatu Region secara default dan terhubung ke Amazon Virtual Private Cloud (VPC) Anda. Instans AD Connector yang gagal secara otomatis diganti di Availability Zone yang sama menggunakan alamat IP yang sama.

Saat Anda masuk ke AWS aplikasi atau layanan apa pun yang terintegrasi dengan AD Connector (AWS IAM Identity Center termasuk), aplikasi atau layanan akan meneruskan permintaan autentikasi Anda ke AD Connector yang kemudian meneruskan permintaan ke pengontrol domain di Active Directory yang dikelola sendiri untuk autentikasi. Jika Anda berhasil diautentikasi ke Active Directory yang dikelola sendiri, AD Connector kemudian mengembalikan token otentikasi ke aplikasi atau

layanan (mirip dengan token Kerberos). Pada titik ini, Anda sekarang dapat mengakses AWS aplikasi atau layanan.

Praktik terbaik untuk AD Connector

Berikut adalah beberapa saran dan panduan yang harus Anda pertimbangkan untuk menghindari masalah dan mendapatkan hasil maksimal dari AD Connector.

Menyiapkan: Prasyarat

Pertimbangkan panduan ini sebelum membuat direktori Anda.

Verifikasikan Anda memiliki jenis direktori yang tepat

Directory Service menyediakan berbagai cara untuk digunakan Microsoft Active Directory dengan AWS layanan lain. Anda dapat memilih directory service dengan fitur yang Anda butuhkan dengan biaya yang sesuai dengan anggaran Anda:

- AWS Directory Service untuk Microsoft Active Directory adalah pengelola yang kaya fitur yang Microsoft Active Directory dihosting di cloud. AWS AWS Microsoft AD yang dikelola adalah pilihan terbaik Anda jika Anda memiliki lebih dari 5.000 pengguna dan memerlukan hubungan kepercayaan yang disiapkan antara direktori yang AWS dihosting dan direktori lokal Anda.
- AD Connector cukup menghubungkan Active Directory lokal Anda yang sudah ada. AWS AD Connector adalah pilihan terbaik Anda saat Anda ingin menggunakan direktori on-premise Anda yang sudah ada dengan layanan AWS .
- Simple AD adalah direktori berskala rendah dan berbiaya rendah dengan kompatibilitas Active Directory dasar. Ini mendukung 5.000 atau lebih sedikit pengguna, aplikasi yang kompatibel dengan Samba 4, dan kompatibilitas LDAP untuk aplikasi sadar LDAP.

Untuk perbandingan Directory Service opsi yang lebih rinci, lihat [Mana yang harus dipilih](#).

Pastikan instans VPCs dan instans Anda dikonfigurasi dengan benar

Untuk terhubung ke, mengelola, dan menggunakan direktori Anda, Anda harus mengonfigurasi dengan benar VPCs bahwa direktori terkait. Lihat [Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS](#), [Prasyarat AD Connector](#), atau [Prasyarat Simple AD](#) untuk informasi tentang persyaratan keamanan dan jaringan VPC.

Jika Anda menambahkan instans ke domain Anda, pastikan bahwa Anda memiliki konektivitas dan akses jarak jauh ke instans Anda seperti yang dijelaskan di [Cara untuk bergabung dengan instans Amazon EC2 ke AWS Microsoft AD yang Dikelola](#).

Ketahui batasan Anda

Pelajari tentang berbagai batasan untuk jenis direktori spesifik Anda. Penyimpanan yang tersedia dan ukuran agregat objek Anda adalah satu-satunya keterbatasan terkait jumlah objek yang dapat Anda simpan dalam direktori Anda. Lihat [AWS Kuota Microsoft AD yang dikelola](#), [Kuota AD Connector](#), atau [Kuota Simple AD](#) untuk detail tentang direktori pilihan Anda.

Pahami konfigurasi grup AWS keamanan direktori Anda dan gunakan

AWS membuat [grup keamanan](#) dan melampirkannya ke [antarmuka jaringan elastis](#) direktori Anda yang dapat diakses dari dalam peered atau diubah ukurannya. [VPCs](#) AWS mengkonfigurasi grup keamanan untuk memblokir lalu lintas yang tidak perlu ke direktori dan memungkinkan lalu lintas yang diperlukan.

Memodifikasi grup keamanan direktori

Untuk mengubah keamanan direktori grup keamanan Anda, Anda dapat melakukannya. Hanya buat perubahan tersebut jika Anda sepenuhnya memahami cara kerja filter grup keamanan. Untuk informasi selengkapnya, lihat [Grup Keamanan Amazon EC2 untuk instans Linux](#) di Panduan Pengguna Amazon EC2. Perubahan yang tidak tepat dapat mengakibatkan hilangnya komunikasi ke komputer dan instance yang dituju. AWS merekomendasikan agar Anda tidak mencoba membuka port tambahan ke direktori Anda karena ini mengurangi keamanan direktori Anda. Harap tinjau dengan seksama [Model Tanggung Jawab Bersama AWS](#).

Warning

Secara teknis dimungkinkan bagi Anda untuk mengaitkan grup keamanan direktori dengan instans EC2 lain yang Anda buat. Namun, AWS merekomendasikan untuk tidak melakukan praktik ini. AWS mungkin memiliki alasan untuk memodifikasi grup keamanan tanpa pemberitahuan untuk mengatasi kebutuhan fungsional atau keamanan direktori terkelola. Perubahan tersebut mempengaruhi setiap instans yang Anda asosiasikan dengan grup keamanan direktori dan dapat mengganggu operasi instans terkait. Selain itu, mengaitkan grup keamanan direktori dengan instans EC2 Anda dapat menciptakan risiko keamanan potensial untuk instans EC2 Anda.

Mengkonfigurasi situs dan subnet on-premise dengan benar saat menggunakan AD Connector

Jika jaringan on-premise Anda memiliki situs Direktori Aktif yang ditetapkan, Anda harus memastikan subnet di VPC tempat AD Connector Anda berada didefinisikan di situs Direktori Aktif, dan bahwa tidak ada konflik antara subnet di VPC dan subnet di situs Anda yang lainnya.

Untuk menemukan pengendali domain, AD Connector menggunakan situs Direktori Aktif yang rentang alamat IP subnet nya dekat dengan yang ada di VPC yang berisi AD Connector. Jika Anda memiliki situs yang subnetnya memiliki rentang alamat IP yang sama seperti yang ada di VPC Anda, AD Connector akan menemukan pengendali domain di situs tersebut, yang mungkin tidak secara fisik dekat dengan Region Anda.

Memahami batasan nama pengguna untuk AWS aplikasi

Directory Service memberikan dukungan untuk sebagian besar format karakter yang dapat digunakan dalam pembangunan nama pengguna. Namun, ada batasan karakter yang diberlakukan pada nama pengguna yang akan digunakan untuk masuk ke AWS aplikasi, seperti, WorkDocs Amazon WorkSpaces WorkMail, atau Quick. Pembatasan ini mengharuskan karakter berikut tidak digunakan:

- Spasi
- Karakter multibyte
- !"#\$%&'()*+,-./:;<=>?@[\\]^_{|}~

Note

Simbol @ diperbolehkan selama itu mendahului akhiran UPN.

Memprogram aplikasi Anda

Sebelum memprogram aplikasi Anda, pertimbangkan hal berikut:

Muat tes sebelum diluncurkan ke produksi

Pastikan untuk melakukan pengujian laboratorium dengan aplikasi dan permintaan yang mewakili beban kerja produksi Anda untuk mengkonfirmasi bahwa direktori meningkatkan skala ke beban

aplikasi Anda. Jika Anda memerlukan kapasitas tambahan, sebarkan beban Anda di beberapa direktori AD Connector.

Menggunakan direktori Anda

Berikut adalah beberapa saran yang perlu diingat saat menggunakan direktori Anda.

Rotasi kredensial Admin secara teratur

Ubah kata sandi Admin akun layanan AD Connector Anda secara teratur, dan pastikan kata sandi konsisten dengan kebijakan kata sandi Direktori Aktif Anda yang sudah ada. Untuk petunjuk tentang cara mengubah kata sandi akun layanan, lihat [Memperbarui kredensi akun layanan AD Connector Anda di Konsol Manajemen AWS](#).

Gunakan AD Connector unik untuk setiap domain

AD Connector dan domain AD on-premise Anda memiliki hubungan 1-banding-1. Artinya, untuk setiap domain on-premise, termasuk domain anak di hutan AD yang ingin Anda autentikasi, Anda harus membuat AD Connector yang unik. Setiap AD Connector yang Anda buat harus menggunakan akun layanan yang berbeda, meskipun terhubung ke direktori yang sama.

Periksa kompatibilitas

Saat menggunakan AD Connector, Anda harus memastikan bahwa direktori lokal Anda dan tetap kompatibel dengannya Directory Service. Untuk informasi selengkapnya tentang tanggung jawab Anda, silakan lihat [model tanggung jawab bersama](#) kami.

Memelihara direktori AD Connector

Anda dapat menggunakan Konsol Manajemen AWS untuk mempertahankan AD Connector dan menyelesaikan tugas day-to-day administratif. Cara Anda dapat mempertahankan direktori Anda meliputi:

- [Lihat detail tentang AD Connector Anda](#).
- [Perbarui alamat DNS yang ditunjuk oleh AD Connector Anda](#).
- [Hapus AD Connector Anda](#) saat tidak diperlukan lagi.

Melihat informasi direktori AD Connector

Untuk melihat informasi direktori terperinci.

1. Di panel navigasi [Konsol AWS Directory Service](#), di bawah Direktori Aktif, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda. Informasi tentang direktori ditampilkan dalam halaman Detail direktori.

Untuk informasi selengkapnya tentang bidang Status, lihat [Memahami status direktori Anda](#).

Memperbarui jenis jaringan direktori

Anda dapat memperbarui jenis jaringan Directory Service direktori Anda dari IPv4 ke Dual-stack (IPv4 dan IPv6). Memperbarui jenis jaringan untuk menyertakan alamat IPv6 IP menyediakan ruang alamat yang lebih besar daripada IPv4. IPv4 dan IPv6 komunikasi independen satu sama lain.

Untuk detailnya, lihat [Bandingkan IPv4 dan IPv6](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Important

Ini adalah operasi satu arah yang tidak dapat dibalik. Uji di lingkungan non-produksi terlebih dahulu.

Prasyarat

Sebelum Anda memperbarui jenis jaringan direktori Anda, pastikan persyaratan berikut terpenuhi:

- VPC Anda harus dikonfigurasi dengan rentang IPv6 CIDR. Untuk detailnya, lihat [IPv6 dukungan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.
- Anda memiliki akses administratif ke Konsol Manajemen AWS.
- Direktori Anda harus dalam status Aktif.
- Anda memiliki izin IAM yang sesuai untuk mengubah Directory Service pengaturan.

Untuk memperbarui jenis jaringan direktori

Untuk memperbarui direktori Anda ke jaringan dual-stack

Note

Jika direktori Anda direplikasi di beberapa wilayah, lakukan pembaruan ini di setiap wilayah.

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih direktori target.
3. Buka tab Jaringan & Keamanan.
4. Pilih Tambahkan IPv6 dukungan. Opsi ini hanya tersedia untuk direktori IPv4 -only.
5. Tinjau informasi pembaruan dan detail harga.
6. Pilih Tambah untuk mengonfirmasi pembaruan.

Setelah memulai pembaruan, status direktori berubah menjadi Memperbarui selama proses pembaruan. Pembaruan biasanya membutuhkan waktu 15-30 menit untuk diselesaikan. Setelah selesai, status direktori kembali ke Aktif.

Memperbarui alamat DNS untuk AD Connector

Gunakan langkah-langkah berikut untuk memperbarui alamat DNS yang ditunjuk oleh AD Connector Anda.

Note

Jika Anda memiliki pembaruan yang sedang berlangsung, Anda harus menunggu sampai selesai sebelum mengirimkan pembaruan lain.

Jika Anda menggunakan WorkSpaces dengan AD Connector Anda, pastikan bahwa alamat DNS untuk Workspace Anda diperbarui juga. Untuk informasi selengkapnya, lihat [Memperbarui server DNS untuk WorkSpaces](#).

Untuk memperbarui pengaturan DNS Anda untuk AD Connector

1. Di panel navigasi [AWS Directory Service konsol](#), di bawah Active Directory, pilih Direktori.

2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & Keamanan.
4. Gulir ke bawah ke bagian Pengaturan DNS yang ada dan pilih Perbarui.
5. Di dialog Perbarui alamat DNS yang ada, ketik alamat IP DNS yang diperbarui, lalu pilih Perbarui.

Untuk informasi selengkapnya tentang pemecahan masalah AD Connector, lihat [Memecahkan Masalah AD Connector](#).

Menghapus AD Connector

Saat Konektor AD dihapus, direktori lokal Anda tetap utuh. Semua instans yang bergabung ke direktori juga tetap utuh dan tetap bergabung ke direktori on-premise Anda. Anda masih bisa menggunakan kredensial direktori Anda untuk masuk ke instans ini.

Untuk menghapus AD Connector

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori. Pastikan Anda berada di AWS Region tempat AD Connector digunakan. Untuk informasi selengkapnya, lihat [Memilih Wilayah](#).
2. Pastikan tidak ada AWS aplikasi yang diaktifkan untuk AD Connector yang ingin Anda hapus. AWS Aplikasi yang diaktifkan akan mencegah Anda menghapus AD Connector Anda.
 - a. Pada halaman Direktori, pilih ID direktori Anda.
 - b. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi. Di bagian AWS aplikasi & layanan, Anda melihat AWS aplikasi mana yang diaktifkan untuk AD Connector Anda.
 - Nonaktifkan Konsol Manajemen AWS akses. Untuk informasi selengkapnya, lihat [Menonaktifkan akses Konsol Manajemen AWS](#).
 - Untuk menonaktifkan Amazon WorkSpaces, Anda harus membatalkan pendaftaran layanan dari direktori di konsol. WorkSpaces Untuk informasi selengkapnya, lihat [Menghapus direktori](#) di Panduan WorkSpaces Administrasi Amazon.
 - Untuk menonaktifkan WorkDocs, Anda harus menghapus WorkDocs situs di WorkDocs konsol. Untuk informasi selengkapnya, lihat [Menghapus situs](#) di Panduan WorkDocs Administrasi Amazon.
 - Untuk menonaktifkan Amazon WorkMail, Anda harus menghapus WorkMail organisasi Amazon di WorkMail konsol Amazon. Untuk informasi selengkapnya, lihat [Menghapus organisasi](#) di Panduan WorkMail Administrator Amazon.

- Untuk menonaktifkan Amazon FSx untuk Windows File Server, Anda harus menghapus sistem FSx file Amazon dari domain. Untuk informasi selengkapnya, lihat [Bekerja dengan Active Directory FSx untuk Windows File Server](#) di Amazon FSx untuk Windows File Server User Guide.
- Untuk menonaktifkan Amazon Relational Database Service, Anda harus menghapus instans Amazon RDS dari domain. Untuk informasi selengkapnya, lihat [Mengelola instans DB dalam domain](#) dalam Panduan Pengguna Amazon RDS.
- Untuk menonaktifkan AWS Client VPN Layanan, Anda harus menghapus layanan direktori dari Endpoint Client VPN. Untuk informasi selengkapnya, lihat [Bekerja dengan Client VPN](#) di Panduan AWS Client VPN Administrator.
- Untuk menonaktifkan Amazon Connect, Anda harus menghapus Instans Amazon Connect. Untuk informasi selengkapnya, lihat [Menghapus instans Amazon Connect](#) di Panduan Administrasi Amazon Connect.
- Untuk menonaktifkan Amazon Quick, Anda harus berhenti berlangganan Amazon Quick. Untuk informasi selengkapnya, lihat [Menutup Amazon Quick akun Anda](#) di Panduan Pengguna Cepat Amazon.

 Note

Jika Anda menggunakan AWS IAM Identity Center dan sebelumnya telah menghubungkannya ke direktori Microsoft AD AWS Terkelola yang ingin Anda hapus, Anda harus terlebih dahulu mengubah sumber identitas sebelum dapat menghapusnya. Untuk informasi selengkapnya, lihat [Mengubah sumber identitas Anda](#) di Panduan Pengguna Pusat Identitas IAM.

3. Di panel navigasi, pilih Direktori.
4. Pilih hanya AD Connector yang akan dihapus dan klik Delete. Dibutuhkan beberapa menit agar AD Connector dihapus. Ketika AD Connector telah dihapus, itu dihapus dari daftar direktori Anda.

Mengamankan direktori AD Connector Anda

Anda dapat menggunakan fitur seperti otentikasi multi-faktor (MFA), Protokol Akses Direktori Ringan sisi klien melalui Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS),

dan untuk mengamankan AD Connector Anda. AWS Private Certificate Authority Cara Anda dapat mengamankan AD Connector Anda meliputi:

- Aktifkan MFA yang meningkatkan keamanan AD Connector Anda.
- Aktifkan Protokol Akses Direktori Ringan sisi klien melalui Secure Socket Layer (SSL) /Transport Layer Security (TLS) (LDAPS) sehingga komunikasi melalui LDAP dienkripsi dan meningkatkan keamanan.
- Aktifkan autentikasi Mutual Transport Layer Security (mTLS) berbasis sertifikat dengan kartu pintar yang memungkinkan pengguna mengautentikasi ke Amazon Web Services melalui Active Directory dan AD Connector Anda.
- Perbarui kredensial akun layanan AD Connector Anda.
- Siapkan AWS Private CA Konektor untuk AD sehingga Anda dapat menerbitkan dan mengelola sertifikat untuk AD Connector Anda.

Tugas untuk mengamankan AD Connector

- [Mengaktifkan otentikasi multi-faktor untuk AD Connector](#)
- [Mengaktifkan LDAPS Sisi Klien Menggunakan AD Connector](#)
- [Mengaktifkan otentikasi mTLS di AD Connector untuk digunakan dengan kartu pintar](#)
- [Memperbarui kredensi akun layanan AD Connector Anda di Konsol Manajemen AWS](#)
- [Siapkan AWS Private CA Konektor untuk AD](#)

Mengaktifkan otentikasi multi-faktor untuk AD Connector

Anda dapat mengaktifkan autentikasi multi-faktor untuk AD Connector jika Active Directory berjalan di lokasi atau di instans Amazon EC2. Untuk informasi selengkapnya tentang menggunakan otentikasi multi-faktor dengan Directory Service, lihat. [Prasyarat AD Connector](#)

Note

Autentikasi multi-faktor tidak tersedia untuk Simple AD. Namun, MFA dapat diaktifkan untuk direktori AWS Microsoft AD Terkelola Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan otentikasi multi-faktor untuk Microsoft AD yang Dikelola AWS](#).

Untuk mengaktifkan autentikasi multi-faktor untuk AD Connector

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori AD Connector Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian Autentikasi multi-faktor, pilih Tindakan, lalu pilih Aktifkan.
5. Pada halaman Aktifkan multi-factor authentication (MFA), berikan nilai berikut:

Label tampilan

Berikan nama label.

Nama DNS server RADIUS atau alamat IP

Alamat IP titik akhir server RADIUS, atau alamat IP penyeimbang beban server RADIUS. Anda dapat memasukkan beberapa alamat IP dengan memisahkannya dengan koma (misalnya, 192.0.0.0,192.0.0.12).

Note

RADIUS MFA hanya berlaku untuk mengautentikasi akses ke Konsol Manajemen AWS, atau ke aplikasi dan layanan Amazon Enterprise seperti, WorkSpaces Amazon Quick, atau Amazon Chime. Itu tidak menyediakan beban kerja MFA ke Windows yang berjalan pada instans EC2, atau untuk masuk ke instans EC2. Directory Service tidak mendukung Challenge/Response otentikasi RADIUS.

Pengguna harus memiliki kode MFA mereka pada saat mereka memasukkan nama pengguna dan kata sandi mereka. Atau, Anda harus menggunakan solusi yang melakukan MFA out-of-band seperti verifikasi teks SMS untuk pengguna. Dalam solusi out-of-band MFA, Anda harus memastikan bahwa Anda menetapkan nilai batas waktu RADIUS dengan tepat untuk solusi Anda. Saat menggunakan solusi out-of-band MFA, halaman masuk akan meminta pengguna untuk kode MFA. Dalam hal ini, praktik terbaik adalah bagi pengguna untuk memasukkan kata sandi mereka di bidang kata sandi dan bidang autentikasi multi-faktor (MFA).

Port

Port yang digunakan oleh server RADIUS Anda untuk komunikasi. Jaringan lokal Anda harus mengizinkan lalu lintas masuk melalui port server RADIUS default (UDP:1812) dari server.

Directory Service

Kode rahasia bersama

Kode rahasia bersama yang ditentukan ketika titik akhir RADIUS Anda dibuat.

Konfirmasikan kode rahasia bersama

Konfirmasi kode rahasia bersama untuk titik akhir RADIUS Anda.

Protokol

Pilih protokol yang ditentukan saat titik akhir RADIUS Anda dibuat.

Batas waktu server (dalam hitungan detik)

Jumlah waktu, dalam detik, untuk menunggu server RADIUS menanggapi. Ini harus berupa nilai antara 1 dan 50.

Permintaan Max RADIUS mencoba ulang

Berapa kali komunikasi dengan server RADIUS dicoba. Ini harus berupa nilai antara 0 dan 10.

Autentikasi multi-faktor tersedia ketika Status RADIUS berubah ke Diaktifkan.

6. Pilih Aktifkan.

Mengaktifkan LDAPS Sisi Klien Menggunakan AD Connector

Dukungan LDAPS sisi klien di AD Connector mengenkripsi komunikasi antara Microsoft Active Directory (AD) dan aplikasi. AWS Contoh aplikasi tersebut termasuk WorkSpaces,, Quick AWS IAM Identity Center, dan Amazon Chime. Enkripsi ini membantu Anda melindungi data identitas organisasi dengan lebih baik dan memenuhi persyaratan keamanan Anda.

Anda juga dapat membatalkan pendaftaran dan menonaktifkan LDAPS sisi klien.

Topik

- [Prasyarat](#)
- [Mengaktifkan LDAPS sisi klien](#)
- [Mengelola LDAPS sisi klien](#)

Prasyarat

Sebelum Anda mengaktifkan LDAPS sisi klien, Anda harus memenuhi persyaratan berikut.

Prasyarat:

- [Men-deploy sertifikat server di Direktori Aktif](#)
- [Persyaratan sertifikat CA](#)
- [Persyaratan jaringan](#)

Men-deploy sertifikat server di Direktori Aktif

Untuk mengaktifkan LDAPS sisi klien, Anda perlu untuk mendapatkan dan menginstal sertifikat server untuk setiap pengendali domain di Direktori Aktif. Sertifikat ini akan digunakan oleh layanan LDAP untuk mendengarkan dan secara otomatis menerima koneksi SSL dari klien LDAP. Anda dapat menggunakan sertifikat SSL yang dikeluarkan oleh deployment Active Directory Certificate Services (ADCS) atau dibeli dari penerbit komersial. Untuk informasi lebih lanjut tentang persyaratan sertifikat server Direktori Aktif, lihat [LDAP melalui Sertifikat SSL \(LDAPS\)](#) di situs web Microsoft.

Persyaratan sertifikat CA

Sertifikat otoritas sertifikat (CA), yang mewakili penerbit sertifikat server Anda, diperlukan untuk operasi LDAPS sisi klien. Sertifikat CA cocok dengan sertifikat server yang disajikan oleh pengendali domain Direktori Aktif Anda untuk mengenkripsi komunikasi LDAP. Perhatikan persyaratan sertifikat CA berikut:

- Untuk mendaftarkan sertifikat, harus lebih dari 90 hari dari kedaluwarsa.
- Sertifikat harus dalam format Privacy Enhanced Mail (PEM). Jika mengekspor sertifikat CA dari dalam Direktori Aktif, pilih base64 encoded X.509 (.CER) sebagai format file ekspor.
- Maksimum lima (5) sertifikat CA dapat disimpan per direktori AD Connector.
- Sertifikat yang menggunakan algoritma tanda tangan RSASSA-PSS tidak didukung.

Persyaratan jaringan

AWS lalu lintas aplikasi LDAP akan berjalan secara eksklusif pada port TCP 636, tanpa fallback ke port LDAP 389. Namun, komunikasi Windows LDAP yang mendukung replikasi, kepercayaan, dan banyak lagi akan terus menggunakan LDAP port 389 dengan keamanan native Windows. Konfigurasi grup AWS keamanan dan firewall jaringan untuk memungkinkan komunikasi TCP pada port 636 di AD Connector (outbound) dan Active Directory yang dikelola sendiri (inbound).

Mengaktifkan LDAPS sisi klien

Untuk mengaktifkan LDAPS sisi klien, Anda mengimpor sertifikat otoritas sertifikat (CA) ke AD Connector, dan kemudian mengaktifkan LDAPS di direktori Anda. Setelah mengaktifkan, semua lalu lintas LDAP antara AWS aplikasi dan Direktori Aktif yang dikelola sendiri akan mengalir dengan enkripsi saluran Secure Sockets Layer (SSL).

Anda dapat menggunakan dua metode yang berbeda untuk mengaktifkan LDAPS sisi klien untuk direktori Anda. Anda dapat menggunakan Konsol Manajemen AWS metode atau AWS CLI metode.

Mendaftarkan sertifikat di Directory Service

Gunakan salah satu metode berikut untuk mendaftarkan sertifikat Directory Service.

Metode 1: Untuk mendaftarkan sertifikat Anda di Directory Service (Konsol Manajemen AWS)

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih menu Tindakan, lalu pilih Mendaftarkan sertifikat.
5. Di kotak dialog Daftarkan sertifikat CA, pilih Telusuri, lalu pilih sertifikat dan pilih Buka.
6. Pilih Daftarkan sertifikat.

Metode 2: Untuk mendaftarkan sertifikat Anda di Directory Service (AWS CLI)

- Jalankan perintah berikut. Untuk data sertifikat, arahkan ke lokasi file sertifikat CA Anda. ID sertifikat akan diberikan dalam tanggapan.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data  
file://your_file_path
```

Memeriksa status pendaftaran

Untuk melihat status pendaftaran sertifikat atau daftar sertifikat terdaftar, gunakan salah satu metode berikut:

Metode 1: Untuk memeriksa status pendaftaran sertifikat di Directory Service (Konsol Manajemen AWS)

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Meninjau status pendaftaran sertifikat saat ini yang ditampilkan di bawah kolom Status pendaftaran. Ketika nilai status pendaftaran berubah menjadi Registered, sertifikat Anda telah berhasil didaftarkan.

Metode 2: Untuk memeriksa status pendaftaran sertifikat di Directory Service (AWS CLI)

- Jalankan perintah berikut. Jika nilai status mengembalikan Registered, sertifikat Anda telah berhasil didaftarkan.

```
aws ds list-certificates --directory-id your_directory_id
```

Mengaktifkan LDAPS sisi klien

Gunakan salah satu metode berikut untuk mengaktifkan LDAPS sisi klien. Directory Service

Note

Anda harus berhasil mendaftarkan setidaknya satu sertifikat sebelum Anda dapat mengaktifkan LDAPS sisi klien.

Metode 1: Untuk mengaktifkan LDAPS sisi klien di () Directory Service Konsol Manajemen AWS

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Pilih Aktifkan. Jika opsi ini tidak tersedia, verifikasi bahwa sertifikat yang valid telah berhasil terdaftar, dan kemudian coba lagi.
3. Di kotak dialog Aktifkan LDAPS sisi klien, pilih Aktifkan.

Metode 2: Untuk mengaktifkan LDAPS sisi klien di () Directory Service AWS CLI

- Jalankan perintah berikut.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Memeriksa status LDAPS

Gunakan salah satu metode berikut untuk memeriksa status LDAPS di. Directory Service

Metode 1: Untuk memeriksa status LDAPS di Directory Service ()Konsol Manajemen AWS

- Buka bagian LDAPS sisi klien pada halaman Detail direktori.
- Jika nilai status ditampilkan sebagai Diaktifkan, LDAPS telah berhasil dikonfigurasi.

Metode 2: Untuk memeriksa status LDAPS di Directory Service ()AWS CLI

- Jalankan perintah berikut. Jika nilai status mengembalikan Enabled, LDAPS telah berhasil dikonfigurasi.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

Untuk informasi selengkapnya tentang melihat sertifikat LDAPS sisi klien Anda, membatalkan pendaftaran atau menonaktifkan sertifikat LDAPS Anda, lihat. [Mengelola LDAPS sisi klien](#)

Mengelola LDAPS sisi klien

Gunakan perintah ini untuk mengelola konfigurasi LDAPS Anda.

Anda dapat menggunakan dua metode yang berbeda untuk mengelola pengaturan LDAPS sisi klien. Anda dapat menggunakan Konsol Manajemen AWS metode atau AWS CLI metode.

Melihat detail sertifikat

Gunakan salah satu metode berikut untuk melihat ketika sertifikat diatur untuk kedaluwarsa.

Metode 1: Untuk melihat detail sertifikat di Directory Service (Konsol Manajemen AWS)

- Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.

2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, di bawah Sertifikat CA, informasi tentang sertifikat akan ditampilkan.

Metode 2: Untuk melihat detail sertifikat di Directory Service (AWS CLI)

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Membatalkan pendaftaran sertifikat

Gunakan salah satu metode berikut untuk membatalkan pendaftaran sertifikat.

 Note

Jika hanya satu sertifikat yang terdaftar, Anda harus terlebih dahulu menonaktifkan LDAPS sebelum Anda dapat membatalkan pendaftaran sertifikat.

Metode 1: Untuk membatalkan pendaftaran sertifikat di () Directory Service Konsol Manajemen AWS

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih Tindakan, lalu pilih Membatalkan pendaftaran sertifikat.
5. Di kotak dialog Membatalkan pendaftaran sertifikat CA, pilih Batalkan pendaftaran.

Metode 2: Untuk membatalkan pendaftaran sertifikat di () Directory Service AWS CLI

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Menonaktifkan LDAPS sisi klien

Gunakan salah satu metode berikut untuk menonaktifkan LDAPS sisi klien.

Metode 1: Untuk menonaktifkan LDAPS sisi klien di () Directory Service Konsol Manajemen AWS

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih Nonaktifkan.
5. Di kotak dialog Nonaktifkan LDAPS sisi klien, pilih Nonaktifkan.

Metode 2: Untuk menonaktifkan LDAPS sisi klien di () Directory Service AWS CLI

- Jalankan perintah berikut.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Mengaktifkan otentikasi mTLS di AD Connector untuk digunakan dengan kartu pintar

Anda dapat menggunakan autentikasi mutual Transport Layer Security (mTLS) berbasis sertifikat dengan kartu pintar untuk mengautentikasi pengguna ke Amazon WorkSpaces melalui Active Directory (AD) dan AD Connector yang dikelola sendiri. Saat diaktifkan, pengguna memilih kartu pintar mereka di layar WorkSpaces login dan memasukkan PIN untuk mengautentikasi, alih-alih menggunakan nama pengguna dan kata sandi. Dari sana, desktop virtual Windows atau Linux menggunakan kartu pintar untuk mengautentikasi ke AD dari OS desktop asli.

Note

Otentikasi kartu pintar di AD Connector hanya tersedia di berikut ini Wilayah AWS, dan hanya dengan WorkSpaces. AWS Aplikasi lain tidak didukung saat ini.

- AS Timur (Virginia Utara)
- US West (Oregon)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- Eropa (Irlandia)
- AWS GovCloud (AS-Barat)
- AWS GovCloud (AS-Timur)

Anda juga dapat membatalkan pendaftaran dan menonaktifkan sertifikat.

Topik

- [Prasyarat](#)
- [Mengaktifkan autentikasi kartu pintar](#)
- [Mengelola pengaturan otentikasi kartu pintar](#)

Prasyarat

Untuk mengaktifkan autentikasi mutual Transport Layer Security (mTLS) berbasis sertifikat menggunakan kartu pintar untuk WorkSpaces klien Amazon, Anda memerlukan infrastruktur kartu pintar operasional yang terintegrasi dengan Active Directory yang dikelola sendiri. Untuk informasi selengkapnya tentang cara mengatur otentikasi kartu pintar dengan Amazon WorkSpaces dan Active Directory, lihat [Panduan WorkSpaces Administrasi Amazon](#).

Sebelum Anda mengaktifkan otentikasi kartu pintar WorkSpaces, harap tinjau prasyarat berikut:

- [Persyaratan sertifikat CA](#)
- [Persyaratan sertifikat pengguna](#)
- [Proses pengecekan pencabutan sertifikat](#)
- [Pertimbangan-pertimbangan](#)

Persyaratan sertifikat CA

AD Connector memerlukan sertifikat otoritas sertifikasi (CA), yang mewakili penerbit sertifikat pengguna Anda, untuk autentikasi kartu pintar. AD Connector mencocokkan sertifikat CA dengan

sertifikat yang ditampilkan oleh pengguna Anda dengan kartu pintar mereka. Perhatikan persyaratan sertifikat CA berikut:

- Sebelum Anda dapat mendaftarkan sertifikat CA, harus lebih dari 90 hari dari kedaluwarsa.
- Sertifikat CA harus dalam format Privacy-Enhanced Mail (PEM). Jika Anda mengekspor sertifikat CA dari dalam Direktori Aktif, pilih base64 encoded X.509 (.CER) sebagai format file ekspor.
- Semua sertifikat CA root dan perantara yang terangkai dari CA penerbit sampai sertifikat pengguna harus diunggah agar autentikasi kartu pintar berhasil.
- Maksimum 100 sertifikat CA dapat disimpan per direktori AD Connector
- AD Connector tidak mendukung algoritma tanda tangan RSASSA-PSS untuk sertifikat CA.
- Verifikasi Layanan Propagasi Sertifikat diatur ke Otomatis dan berjalan.

Persyaratan sertifikat pengguna

Berikut ini adalah beberapa persyaratan untuk sertifikat pengguna:

- Sertifikat kartu pintar pengguna memiliki Nama Alternatif Subjek (SAN) dari pengguna `userPrincipalName` (UPN).
- Sertifikat kartu pintar pengguna memiliki Penggunaan Kunci yang Ditingkatkan sebagai log-on kartu pintar (1.3.6.1.4.1.311.20.2.2) Otentikasi Klien (1.3.6.1.5.5.7.3.2).
- Informasi Protokol Status Sertifikat Online (OCSP) untuk sertifikat kartu pintar pengguna harus berupa Metode Akses = Protokol Status Sertifikat On-line (1.3.6.1.5.5.7.48.1) di Akses Informasi Otoritas.

Untuk informasi selengkapnya tentang AD Connector dan persyaratan autentikasi kartu pintar, lihat [Persyaratan](#) di Panduan WorkSpaces Administrasi Amazon. Untuk membantu mengatasi WorkSpaces masalah Amazon, seperti masuk ke, mengatur ulang kata sandi WorkSpaces, atau menyambungkan ke WorkSpaces, lihat [Memecahkan WorkSpaces masalah klien di](#) Panduan Pengguna Amazon. WorkSpaces

Proses pengecekan pencabutan sertifikat

Untuk melakukan autentikasi kartu pintar, AD Connector harus memeriksa status pencabutan sertifikat pengguna menggunakan Online Certificate Status Protocol (OCSP). Untuk melakukan pengecekan pencabutan sertifikat, URL penjawab OCSP harus dapat diakses internet. Jika

menggunakan nama DNS, URL penjawab OCSP harus menggunakan domain tingkat atas yang ditemukan di [Basis Data Zona Root Internet Assigned Numbers Authority \(IANA\)](#).

 Note

Direktori yang dibuat setelah 7 Oktober 2025, mengharuskan server OCSP yang digunakan untuk validasi SmartCard sertifikat dapat dirutekan melalui konfigurasi jaringan VPC Anda. Jika server OCSP Anda tidak dapat diakses melalui tabel perutean, grup keamanan, dan jaringan VPC Anda ACLs, SmartCard otentikasi akan gagal selama pemeriksaan pencabutan sertifikat. Untuk mengatasi masalah ini, pastikan bahwa:

- Perutean Jaringan: Tabel rute VPC Anda memungkinkan lalu lintas mencapai server OCSP Anda dari subnet tempat instance direktori AD Connector Anda digunakan.
- Grup Keamanan: Grup keamanan yang terkait dengan antarmuka jaringan direktori Anda mengizinkan lalu lintas keluar ke server OCSP Anda di port 80 (HTTP).
- Jaringan ACLs: Jaringan subnet Anda ACLs memungkinkan lalu lintas dua arah server OCSP to/from Anda.
- Internet Gateway/NAT: Jika server OCSP Anda menghadap ke internet, pastikan VPC Anda memiliki gateway internet atau konfigurasi gateway NAT yang sesuai untuk subnet direktori. Jika jenis jaringan Anda IPv4, Anda harus memiliki NAT dan gateway internet yang dikonfigurasi dengan VPC Anda.

Pemeriksaan pencabutan sertifikat AD Connector menggunakan proses berikut ini:

- AD Connector harus memeriksa ekstensi Authority Information Access (AIA) di sertifikat pengguna untuk URL penjawab OCSP, lalu AD Connector menggunakan URL tersebut untuk memeriksa pencabutan.
- Jika AD Connector tidak dapat menyelesaikan URL yang ditemukan di ekstensi AIA sertifikat pengguna, atau menemukan URL penjawab OCSP di sertifikat pengguna, AD Connector menggunakan URL OCSP opsional yang disediakan selama pendaftaran sertifikat CA root.

Jika URL di ekstensi AIA sertifikat pengguna terselesaikan tapi tidak responsif, maka autentikasi pengguna gagal.

- Jika URL penjawab OCSP yang disediakan selama pendaftaran sertifikat CA root tidak dapat diselesaikan, tidak responsif, atau tidak ada URL penjawab OCSP yang disediakan, autentikasi pengguna gagal.

- Server OCSP harus sesuai dengan [RFC 6960](#). Selain itu, server OCSP harus mendukung permintaan menggunakan metode GET untuk permintaan yang kurang dari atau sama dengan 255 byte secara total.

 Note

AD Connector memerlukan URL HTTP untuk URL penjawab OCSP.

Pertimbangan-pertimbangan

Sebelum mengaktifkan autentikasi kartu pintar di AD Connector, pertimbangkan item berikut ini:

- AD Connector menggunakan autentikasi Transport Layer Security berbasis sertifikat (mutual TLS) untuk mengautentikasi pengguna ke Direktori Aktif menggunakan sertifikat kartu pintar berbasis perangkat keras atau perangkat lunak. Hanya kartu akses umum (CAC) dan kartu verifikasi identitas pribadi (PIV) yang didukung saat ini. Jenis lain dari perangkat keras atau kartu pintar berbasis perangkat lunak mungkin berfungsi tetapi belum diuji untuk digunakan dengan Protokol Streaming. WorkSpaces
- Otentikasi kartu pintar menggantikan otentikasi nama pengguna dan kata sandi ke. WorkSpaces

Jika Anda memiliki AWS aplikasi lain yang dikonfigurasi di direktori AD Connector Anda dengan otentikasi kartu pintar diaktifkan, aplikasi tersebut masih menampilkan layar input nama pengguna dan kata sandi.

- Mengaktifkan autentikasi kartu pintar membatasi panjang sesi pengguna ke maksimum seumur hidup untuk tiket layanan Kerberos. Anda dapat mengkonfigurasi pengaturan ini menggunakan Kebijakan Grup, dan diatur ke 10 jam secara default. Untuk informasi lebih lanjut tentang pengaturan ini, lihat [Dokumentasi Microsoft](#).
- Jenis enkripsi Kerberos yang didukung oleh akun layanan AD Connector harus sesuai dengan setiap jenis enkripsi Kerberos yang didukung pengontrol domain.

Mengaktifkan autentikasi kartu pintar

Untuk mengaktifkan otentikasi kartu pintar WorkSpaces di AD Connector, pertama-tama Anda harus mengimpor sertifikat otoritas sertifikat (CA) ke AD Connector. Anda dapat mengimpor sertifikat CA ke AD Connector menggunakan AWS Directory Service konsol, [API](#), atau [CLI](#). Gunakan langkah-

langkah berikut untuk mengimpor sertifikat CA Anda dan selanjutnya mengaktifkan otentikasi kartu pintar.

Langkah-langkah

- [Mengaktifkan delegasi terbatas Kerberos untuk akun layanan AD Connector](#)
- [Mendaftarkan sertifikat CA di AD Connector](#)
- [Mengaktifkan otentikasi kartu pintar untuk AWS aplikasi dan layanan yang didukung](#)

Mengaktifkan delegasi terbatas Kerberos untuk akun layanan AD Connector

Untuk menggunakan otentikasi kartu pintar dengan AD Connector, Anda harus mengaktifkan Kerberos Constrained Delegation (KCD) untuk akun AD Connector Service ke layanan LDAP di direktori AD yang dikelola sendiri.

Kerberos Constrained Delegation adalah sebuah fitur di Windows Server. Fitur ini memungkinkan administrator untuk menentukan dan menegakkan batasan kepercayaan aplikasi dengan membatasi ruang lingkup di mana layanan aplikasi dapat bertindak atas nama pengguna. Untuk informasi selengkapnya, lihat [Delegasi yang dibatasi Kerberos](#).

Note

Kerberos Constrained Delegation (KCD) memerlukan bagian nama pengguna dari akun layanan AD Connector agar sesuai dengan Nama s pengguna yang sama. AMAccountName s dibatasi hingga 20 karakter. s AMAccount Name adalah atribut Microsoft Active Directory yang digunakan sebagai nama masuk untuk versi klien dan server Windows sebelumnya.

1. Gunakan SetSpn perintah untuk menetapkan Service Principal Name (SPN) untuk akun layanan AD Connector di AD yang dikelola sendiri. Hal ini mengizinkan akun layanan untuk konfigurasi delegasi.

SPN dapat berupa kombinasi layanan atau nama tetapi bukan duplikat SPN yang ada. -s memeriksa adanya duplikat.

```
setspn -s my/spn service_account
```

2. Di Pengguna dan Komputer AD, buka menu konteks (klik kanan) dan pilih akun layanan AD Connector dan pilih Properties.
3. Pilih tab Delegasi.
4. Pilih Percayai pengguna ini untuk delegasi ke layanan tertentu saja dan Gunakan opsi protokol otentikasi apa pun.
5. Pilih Tambahkan lalu Pengguna atau Komputer untuk menemukan pengendali domain.
6. Pilih OKE untuk menampilkan daftar layanan tersedia yang digunakan untuk delegasi.
7. Pilih jenis layanan Idap dan pilih OK.
8. Pilih OK lagi untuk menyimpan konfigurasi.
9. Ulangi proses ini untuk pengontrol domain lain di Direktori Aktif. Atau Anda dapat mengotomatiskan proses menggunakan PowerShell.

Mendaftarkan sertifikat CA di AD Connector

Gunakan salah satu metode berikut untuk mendaftarkan sertifikat CA untuk direktori AD Connector Anda.

Metode 1: Untuk mendaftarkan sertifikat CA Anda di AD Connector (Konsol Manajemen AWS)

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian Autentikasi kartu pintar, pilih Tindakan, lalu pilih Daftar sertifikat.
5. Dalam kotak dialog Daftarkan sertifikat, pilih Pilih file, lalu pilih sertifikat dan pilih Buka. Anda dapat memilih untuk melakukan pengecekan pencabutan sertifikat ini dengan memberikan URL responder Online Certificate Status Protocol (OCSP). Untuk informasi lebih lanjut tentang OCSP, lihat [Proses pengecekan pencabutan sertifikat](#).
6. Pilih Daftarkan sertifikat. Ketika Anda melihat status sertifikat berubah menjadi Terdaftar, proses pendaftaran telah selesai dengan sukses.

Metode 2: Untuk mendaftarkan sertifikat CA Anda di AD Connector (AWS CLI)

- Jalankan perintah berikut. Untuk data sertifikat, arahkan ke lokasi file sertifikat CA Anda. Untuk memberikan alamat penjawab OCSP sekunder, gunakan objek `ClientCertAuthSettings` opsional.


```
aws ds register-certificate --directory-id your_directory_id --certificate-  
data file://your_file_path --type ClientCertAuth --client-cert-auth-settings  
OCSPUrl=http://your_OCSP_address
```

Jika berhasil, respons memberikan ID sertifikat. Anda juga dapat memverifikasi sertifikat CA Anda terdaftar berhasil dengan menjalankan perintah CLI berikut:

```
aws ds list-certificates --directory-id your_directory_id
```

Jika nilai status mengembalikan Registered, Anda telah berhasil mendaftarkan sertifikat Anda.

Mengaktifkan otentikasi kartu pintar untuk AWS aplikasi dan layanan yang didukung

Gunakan salah satu metode berikut untuk mendaftarkan sertifikat CA untuk direktori AD Connector Anda.

Metode 1: Untuk mengaktifkan otentikasi kartu pintar di AD Connector ()Konsol Manajemen AWS

1. Arahkan ke bagian otentikasi kartu pintar di halaman Detail direktori, dan pilih Aktifkan. Jika opsi ini tidak tersedia, verifikasi bahwa sertifikat yang valid telah berhasil terdaftar, dan kemudian coba lagi.
2. Dalam kotak dialog Aktifkan otentikasi kartu pintar, pilih Aktifkan.

Metode 2: Untuk mengaktifkan otentikasi kartu pintar di AD Connector ()AWS CLI

- Jalankan perintah berikut.

```
aws ds enable-client-authentication --directory-id your_directory_id --type  
SmartCard
```

Jika berhasil, AD Connector akan mengembalikan respons HTTP 200 dengan tubuh HTTP kosong.

Untuk informasi selengkapnya tentang melihat sertifikat, membatalkan pendaftaran, atau menonaktifkan sertifikat Anda, lihat. [Mengelola pengaturan otentikasi kartu pintar](#)

Mengelola pengaturan otentikasi kartu pintar

Anda dapat menggunakan dua metode berbeda untuk mengelola pengaturan kartu pintar. Anda dapat menggunakan Konsol Manajemen AWS metode atau AWS CLI metode.

Topik

- [Melihat detail sertifikat](#)
- [Membatalkan pendaftaran sertifikat](#)
- [Nonaktifkan otentikasi kartu pintar](#)

Melihat detail sertifikat

Gunakan salah satu metode berikut untuk melihat ketika sertifikat diatur untuk kedaluwarsa.

Metode 1: Untuk melihat detail sertifikat di Directory Service (Konsol Manajemen AWS)

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori AD Connector Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian Autentikasi kartu pintar, di bawah sertifikat CA, pilih ID sertifikat untuk menampilkan detail tentang sertifikat tersebut.

Metode 2: Untuk melihat detail sertifikat di Directory Service (AWS CLI)

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Membatalkan pendaftaran sertifikat

Gunakan salah satu metode berikut untuk membatalkan pendaftaran sertifikat.

 Note

Jika hanya satu sertifikat yang terdaftar, Anda harus menonaktifkan otentikasi kartu pintar terlebih dahulu sebelum Anda dapat membatalkan pendaftaran sertifikat.

Metode 1: Untuk membatalkan pendaftaran sertifikat di () Directory Service Konsol Manajemen AWS

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori AD Connector Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian Autentikasi kartu pintar, di bawah sertifikat CA, pilih sertifikat yang ingin Anda deregister, pilih Tindakan, lalu pilih Deregister Certificate.

 Important

Pastikan sertifikat yang akan Anda deregister tidak aktif atau saat ini digunakan sebagai bagian dari rantai sertifikat CA untuk otentikasi kartu pintar.

5. Di kotak dialog Membatalkan pendaftaran sertifikat CA, pilih Batalkan pendaftaran.

Metode 2: Untuk membatalkan pendaftaran sertifikat di () Directory Service AWS CLI

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Nonaktifkan otentikasi kartu pintar

Gunakan salah satu metode berikut untuk menonaktifkan otentikasi kartu pintar.

Metode 1: Untuk menonaktifkan otentikasi kartu pintar di Directory Service ()Konsol Manajemen AWS

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih tautan ID direktori untuk direktori AD Connector Anda.

3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian otentikasi kartu pintar, pilih Nonaktifkan.
5. Dalam kotak dialog Nonaktifkan otentikasi kartu pintar, pilih Nonaktifkan.

Metode 2: Untuk menonaktifkan otentikasi kartu pintar di Directory Service ()AWS CLI

- Jalankan perintah berikut.

```
aws ds disable-client-authentication --directory-id your_directory_id --type SmartCard
```

Memperbarui kredensi akun layanan AD Connector Anda di Konsol Manajemen AWS

Kredensi AD Connector yang Anda berikan Directory Service mewakili akun layanan yang digunakan untuk mengakses direktori lokal yang ada. Anda dapat mengubah kredensi akun layanan Directory Service dengan melakukan langkah-langkah berikut.

Note

Jika AWS IAM Identity Center diaktifkan untuk direktori, Directory Service harus mentransfer nama utama layanan (SPN) dari akun layanan saat ini ke akun layanan baru. Jika akun layanan saat ini tidak memiliki izin untuk menghapus SPN atau akun layanan baru tidak memiliki izin untuk menambahkan SPN, Anda akan diminta kredensial akun direktori yang memiliki izin untuk melakukan kedua tindakan tersebut. Kredensial ini hanya digunakan untuk mentransfer SPN dan tidak disimpan oleh layanan.

Untuk memperbarui kredensi akun layanan AD Connector Anda di Directory Service

1. Di panel navigasi [AWS Directory Service konsol](#), di bawah Active Directory, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, gulir ke bawah ke bagian Kredensial akun Layanan.
4. Di bagian Kredensial akun layanan, pilih Perbarui.
5. Di kotak dialog Perbarui kredensi akun layanan, ketik nama pengguna dan kata sandi akun layanan. Masukkan kembali kata sandi untuk mengonfirmasinya dan kemudian pilih Perbarui.

Siapkan AWS Private CA Konektor untuk AD

Anda dapat mengintegrasikan Active Directory yang dikelola sendiri dengan AWS Private Certificate Authority menggunakan AD Connector untuk menerbitkan dan mengelola sertifikat bagi pengguna, grup, dan mesin yang bergabung dengan domain AD. AWS Private CA Connector for AD menyediakan penggantian drop-in yang dikelola AWS Private CA sepenuhnya untuk perusahaan yang dikelola sendiri CAs tanpa mengharuskan Anda untuk menyebarkan, menambal, atau memperbarui agen lokal atau server proxy.

Anda dapat mengatur integrasi ini melalui Directory Service konsol, AWS Private CA Konektor untuk konsol AD, atau dengan memanggil [CreateTemplateAPI](#). Untuk menggunakan AWS Private CA Konektor untuk konsol Active Directory, lihat [AWS Private CA Konektor untuk Direktori Aktif](#). Bagian berikut menjelaskan cara mengatur integrasi ini dari Directory Service konsol.

Prasyarat

Untuk petunjuk penyiapan, lihat [Mengatur Konektor untuk AD](#) di Panduan Pengguna AWS Private CA Konektor untuk AD.

Menyiapkan AWS Private CA Konektor untuk AD

Untuk membuat konektor CA Pribadi untuk Active Directory

1. Masuk ke Konsol Manajemen AWS dan buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah tab Manajemen Aplikasi dan bagian AWS aplikasi & layanan, pilih AWS Private CA Konektor untuk AD.
4. Pada halaman Create Private CA certificate for Active Directory, selesaikan langkah-langkah untuk membuat konektor Private CA for Active Directory.

Untuk informasi selengkapnya, lihat [Membuat konektor](#).

Lihat AWS Private CA Konektor Anda untuk AD

Untuk melihat detail konektor CA Pribadi

1. Masuk ke Konsol Manajemen AWS dan buka Directory Service konsol di <https://console.aws.amazon.com/directoryservicev2/>.

2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah tab Manajemen Aplikasi dan bagian AWS aplikasi & layanan, lihat konektor CA Pribadi Anda dan CA Pribadi terkait. Bidang berikut menampilkan:
 - a. AWS Private CA Connector ID — Pengidentifikasi unik untuk AWS Private CA konektor. Pilih untuk melihat halaman detail.
 - b. AWS Private CA subjek — Informasi mengenai nama yang dibedakan untuk CA. Pilih untuk melihat halaman detail.
 - c. Status - Hasil pemeriksaan status untuk AWS Private CA Konektor dan AWS Private CA:
 - Aktif — Kedua cek lulus
 - 1/2 pemeriksaan gagal - Satu pemeriksaan gagal
 - Gagal - Kedua pemeriksaan gagal

Untuk detail status yang gagal, arahkan kursor ke hyperlink untuk melihat pemeriksaan mana yang gagal.

- d. Status Pendaftaran Sertifikat DC - Pemeriksaan status untuk status sertifikat pengontrol domain:
 - Diaktifkan - Pendaftaran sertifikat diaktifkan
 - Dinonaktifkan - Pendaftaran sertifikat dinonaktifkan
- e. Tanggal dibuat — Saat AWS Private CA Konektor dibuat.

Untuk informasi selengkapnya, lihat [Lihat detail konektor](#).

Verifikasi penerbitan sertifikat ke pengguna AD

Selesaikan langkah-langkah berikut untuk mengonfirmasi bahwa AWS Private CA menerbitkan sertifikat ke Active Directory yang dikelola sendiri:

- Mulai ulang pengontrol domain lokal Anda.
- Lihat sertifikat Anda dengan Microsoft Management Console. Untuk informasi lebih lanjut, lihat [Microsoft dokumentasi](#).

Memantau direktori AD Connector Anda

Anda bisa mendapatkan hasil maksimal dari AD Connector Anda dengan mempelajari lebih lanjut tentang status AD Connector yang berbeda dan apa artinya untuk AD Connector Anda. Anda juga dapat menggunakan Amazon Simple Notification Service untuk menerima pemberitahuan mengenai status AD Connector Anda.

Tugas untuk memantau AD Connector:

- [Memahami status direktori Anda](#)
- [Mengaktifkan pemberitahuan status direktori AD Connector dengan Amazon SNS](#)

Memahami status direktori Anda

Berikut ini adalah berbagai status untuk direktori.

Aktif

Direktori beroperasi secara normal. Tidak ada masalah yang terdeteksi oleh Directory Service untuk direktori Anda.

Creating

Direktori saat ini sedang dibuat. Pembuatan direktori biasanya memakan waktu antara 20 sampai 45 menit tetapi dapat bervariasi tergantung pada beban sistem.

Dihapus

Direktori telah dihapus. Semua sumber daya untuk direktori telah dirilis. Setelah direktori memasuki keadaan ini, direktori tidak dapat dipulihkan.

Deleting

Direktori saat ini sedang dihapus. Direktori akan tetap dalam keadaan ini sampai benar-benar dihapus. Setelah direktori memasuki keadaan ini, operasi hapus tidak dapat dibatalkan, dan direktori tidak dapat dipulihkan.

Gagal

Direktori tidak dapat dibuat. Harap hapus direktori ini. Jika masalah ini berlanjut, hubungi [Pusat AWS Dukungan](#).

Terganggu

Direktori berjalan dalam keadaan terdegradasi. Satu atau lebih masalah telah terdeteksi, dan tidak semua operasi direktori dapat bekerja pada kapasitas operasional penuh. Terdapat banyak potensi alasan untuk keadaan direktori seperti ini. Ini termasuk aktivitas pemeliharaan operasional normal seperti patching atau rotasi EC2 instance, hot spotting sementara oleh aplikasi di salah satu pengontrol domain Anda, atau perubahan yang Anda buat pada jaringan Anda yang secara tidak sengaja mengganggu komunikasi direktori. Untuk informasi selengkapnya, lihat salah satu dari [Pemecahan Masalah AWS Microsoft AD yang Dikelola](#), [Memecahkan masalah AD Connector](#), [Pemecahan masalah Simple AD](#). Untuk masalah terkait pemeliharaan normal, AWS selesaikan masalah ini dalam waktu 40 menit. Jika setelah meninjau topik pemecahan masalah, direktori Anda dalam keadaan Terganggu lebih dari 40 menit, kami merekomendasikan Anda untuk menghubungi [Pusat AWS Dukungan](#).

Important

Jangan memulihkan snapshot ketika direktori dalam keadaan Terganggu. Sangatlah jarang pemulihan snapshot diperlukan untuk mengatasi gangguan. Untuk informasi selengkapnya, lihat [Memulihkan iklan Microsoft AWS Terkelola Anda dengan snapshot](#).

Tidak bisa dioperasikan

Direktori tidak berfungsi. Semua titik akhir direktori telah melaporkan masalah.

Diminta

Permintaan untuk membuat direktori Anda sedang tertunda.

Mengaktifkan pemberitahuan status direktori AD Connector dengan Amazon SNS

Menggunakan Amazon Simple Notification Service (Amazon SNS), Anda dapat menerima pesan email atau teks (SMS) saat status direktori Anda berubah. Anda akan diberitahu jika direktori Anda berubah dari status Aktif ke status [Terganggu atau Tidak dapat dioperasikan](#). Anda juga menerima notifikasi ketika direktori kembali ke status Aktif.

Cara kerjanya

Amazon SNS menggunakan “topik” untuk mengumpulkan dan mendistribusikan pesan. Setiap topik memiliki satu atau lebih pelanggan yang menerima pesan yang telah diterbitkan untuk topik tersebut. Dengan menggunakan langkah-langkah di bawah ini, Anda dapat menambahkan Directory Service sebagai penerbit ke topik Amazon SNS. Saat Directory Service mendeteksi perubahan dalam status direktori Anda, ia menerbitkan pesan ke topik tersebut, yang kemudian dikirim ke pelanggan topik tersebut.

Anda dapat mengaitkan beberapa direktori sebagai penerbit ke satu topik. Anda juga dapat menambahkan pesan status direktori ke topik yang sebelumnya Anda buat di Amazon SNS. Anda memiliki kendali terperinci atas siapa yang dapat menerbitkan dan berlangganan topik. Untuk informasi lengkap tentang Amazon SNS, lihat [Apa yang Dimaksud dengan Amazon SNS?](#).

Untuk mengaktifkan olahpesan SNS untuk direktori Anda

1. Masuk ke Konsol Manajemen AWS dan buka [Directory Service konsol](#).
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih Tindakan, dan kemudian pilih Buat notifikasi.
5. Pada halaman Buat notifikasi, pilih Pilih jenis notifikasi, lalu pilih Buat notifikasi baru. Atau, jika Anda sudah memiliki topik SNS yang ada, Anda dapat memilih Mengasosiasikan topik SNS yang ada untuk mengirim pesan status dari direktori ini ke topik tersebut.

Note

Jika Anda memilih Buat notifikasi baru tetapi kemudian menggunakan nama topik yang sama untuk topik SNS yang sudah ada, Amazon SNS tidak membuat topik baru, tetapi hanya menambahkan informasi langganan baru ke topik yang ada.

Jika Anda memilih Mengasosiasikan topik SNS yang ada, Anda hanya akan dapat memilih topik SNS yang ada di Region yang sama dengan direktori.

6. Pilih Jenis penerima dan masukkan informasi kontak Penerima. Jika Anda memasukkan nomor telepon untuk SMS, gunakan angka saja. Jangan menyertakan tanda hubung, spasi, atau tanda kurung.

7. (Opsional) Berikan nama untuk topik Anda dan nama tampilan SNS. Nama tampilan adalah nama pendek hingga 10 karakter yang disertakan dalam semua pesan SMS dari topik ini. Bila menggunakan opsi SMS, nama tampilan diperlukan.

 Note

Jika Anda masuk menggunakan pengguna IAM atau peran yang hanya memiliki kebijakan [DirectoryServiceFullAccess](#) terkelola, nama topik Anda harus dimulai dengan "DirectoryMonitoring". Jika Anda ingin menyesuaikan nama topik Anda lebih lanjut, Anda memerlukan hak istimewa tambahan untuk SNS.

8. Pilih Buat.

[Jika Anda ingin menunjuk pelanggan SNS tambahan, seperti alamat email tambahan, antrian Amazon SQS AWS Lambda atau, Anda dapat melakukan ini dari konsol Amazon SNS.](#)

Untuk menghapus pesan status direktori dari topik

1. Masuk ke Konsol Manajemen AWS dan buka [Directory Service konsol](#).
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih nama topik SNS dalam daftar, pilih Tindakan, dan kemudian pilih Hapus.
5. Pilih Hapus.

Ini akan menghapus direktori Anda sebagai penerbit untuk topik SNS yang dipilih. Jika Anda ingin menghapus seluruh topik, Anda dapat melakukan ini dari konsol [Amazon SNS](#).

 Note

Sebelum menghapus topik Amazon SNS menggunakan konsol SNS, Anda harus memastikan bahwa direktori tidak mengirim pesan status untuk topik tersebut.

Jika Anda menghapus topik Amazon SNS menggunakan konsol SNS, perubahan ini tidak akan segera tercermin dalam konsol Directory Service. Anda hanya akan diberitahu pada saat direktori menerbitkan notifikasi untuk topik yang dihapus, dalam hal ini Anda akan melihat status diperbarui pada tab Pemantauan direktori yang menunjukkan topik tidak dapat ditemukan.

Oleh karena itu, untuk menghindari kehilangan pesan status direktori penting, sebelum menghapus topik apa pun yang menerima pesan dari Directory Service, kaitkan direktori Anda dengan topik Amazon SNS yang berbeda.

Akses ke AWS aplikasi dan layanan dari AD Connector

Anda dapat mengizinkan AD Connector mengakses AWS aplikasi dan layanan untuk Active Directory yang terhubung. Beberapa AWS aplikasi dan layanan yang didukung meliputi:

- Amazon Chime
- Amazon WorkSpaces
- Pusat Identitas IAM
- Konsol Manajemen AWS

Tidak ada aplikasi pihak ketiga yang bekerja dengan AD Connector.

Tugas untuk mengakses AWS aplikasi dan layanan dari AD Connector

- [Kebijakan kompatibilitas aplikasi untuk AD Connector](#)
- [Mengaktifkan akses ke AWS aplikasi dan layanan dari AD Connector](#)

Kebijakan kompatibilitas aplikasi untuk AD Connector

Sebagai alternatif dari AWS Directory Service untuk Microsoft Active Directory ([AWS Microsoft AD yang dikelola](#)), AD Connector adalah proxy Active Directory untuk aplikasi dan layanan yang AWS dibuat saja. Anda mengkonfigurasi proksi untuk menggunakan domain Direktori Aktif yang ditentukan. Bila aplikasi harus mencari pengguna atau grup di Direktori Aktif, AD Connector akan memproksikan permintaan ke direktori. Demikian pula ketika pengguna masuk ke aplikasi, AD Connector memproksikan permintaan autentikasi ke direktori. Tidak ada aplikasi pihak ketiga yang bekerja dengan AD Connector.

Berikut ini adalah daftar AWS aplikasi dan layanan yang kompatibel:

- Amazon Chime - Untuk instruksi detail, lihat [Menghubungkan ke Direktori Aktif Anda](#).
- Amazon Connect - Untuk informasi selengkapnya, lihat [Cara kerja Amazon Connect](#).

- Amazon EC2 untuk Windows atau Linux — Anda dapat menggunakan fitur gabungan domain Active Directory yang mulus dari Amazon EC2 Windows atau Linux untuk menggabungkan instans Anda ke Active Directory yang dikelola sendiri (lokal). Setelah bergabung, instans berkomunikasi langsung dengan Direktori Aktif Anda dan melewati AD Connector. Untuk informasi selengkapnya, lihat [Cara untuk bergabung dengan EC2 instans Amazon ke Direktori Aktif Anda](#).
- Konsol Manajemen AWS — Anda dapat menggunakan AD Connector untuk mengautentikasi Konsol Manajemen AWS pengguna dengan kredensi Active Directory mereka tanpa menyiapkan infrastruktur SAFL. Untuk informasi selengkapnya, lihat [Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola](#).
- Cepat - Untuk informasi selengkapnya, lihat [Mengelola akun pengguna di Quick Enterprise Edition](#).
- AWS IAM Identity Center - Untuk petunjuk terperinci, lihat [Connect IAM Identity Center ke Active Directory lokal](#).
- AWS Transfer Family - Untuk petunjuk terperinci, lihat [Bekerja dengan Microsoft Directory Service Active Directory](#).
- AWS Client VPN - Untuk petunjuk terperinci, lihat [Otentikasi dan otorisasi klien](#).
- WorkDocs - Untuk petunjuk terperinci, lihat [Menghubungkan ke direktori lokal Anda dengan AD Connector](#).
- Amazon WorkMail - Untuk petunjuk terperinci, lihat [Mengintegrasikan Amazon WorkMail dengan direktori yang ada \(penyiapan standar\)](#).
- WorkSpaces - Untuk petunjuk terperinci, lihat [Meluncurkan WorkSpace menggunakan AD Connector](#).

Note

Amazon RDS hanya kompatibel dengan Microsoft AD AWS Terkelola, dan tidak kompatibel dengan AD Connector. Untuk informasi selengkapnya, lihat bagian iklan Microsoft yang AWS dikelola di [Directory Service FAQ](#) halaman.

Mengaktifkan akses ke AWS aplikasi dan layanan dari AD Connector

Pengguna dapat mengotorisasi AD Connector untuk memberikan AWS aplikasi dan layanan, seperti Amazon WorkSpaces, akses ke Active Directory Anda. AWS Aplikasi dan layanan berikut dapat diaktifkan atau dinonaktifkan untuk bekerja dengan AD Connector.

AWS aplikasi/layanan	Informasi selengkapnya...
Amazon Chime	Untuk informasi selengkapnya, lihat Menghubungkan ke Direktori Aktif .
Amazon Connect	Untuk informasi selengkapnya, lihat Panduan Administrasi Amazon Connect .
Amazon WorkDocs	Untuk informasi selengkapnya, lihat Memulai dengan Amazon WorkDocs .
Amazon WorkMail	Untuk informasi selengkapnya, lihat Membuat organisasi .
Amazon WorkSpaces	Anda dapat membuat Simple AD, AWS Managed Microsoft AD, atau AD Connector langsung dari WorkSpaces. Cukup luncurkan Pengaturan Advanced saat membuat Workspace Anda. Untuk informasi selengkapnya, lihat Panduan WorkSpaces Administrasi Amazon.
AWS Client VPN	Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Client VPN .
AWS IAM Identity Center	Untuk informasi selengkapnya, lihat Panduan Pengguna AWS IAM Identity Center .
Konsol Manajemen AWS	Untuk informasi selengkapnya, lihat Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola .
AWS Transfer Family	Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Transfer Family .

Setelah diaktifkan, Anda mengelola akses ke direktori Anda di konsol dari aplikasi atau layanan yang ingin Anda berikan akses ke direktori Anda. Untuk menemukan tautan AWS aplikasi dan layanan yang dijelaskan di atas di Directory Service konsol, lakukan langkah-langkah berikut.

Untuk menampilkan aplikasi dan layanan untuk direktori

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Tinjau daftar di bawah bagian aplikasi & layanan AWS .

Untuk informasi selengkapnya tentang cara mengotorisasi atau membatalkan otorisasi AWS aplikasi dan layanan yang digunakan Directory Service, lihat. [Otorisasi untuk AWS aplikasi dan layanan menggunakan Directory Service](#)

Cara untuk bergabung dengan EC2 instans Amazon ke Direktori Aktif Anda

AD Connector adalah gateway direktori yang dapat digunakan untuk mengarahkan permintaan direktori ke Microsoft Active Directory lokal tanpa menyimpan informasi apa pun di cloud. Berikut informasi selengkapnya tentang bagaimana Anda dapat bergabung dengan Amazon EC2 ke domain Direktori Aktif:

- Anda dapat menggabungkan EC2 instans Amazon dengan mulus ke domain Active Directory saat instans diluncurkan. Untuk informasi selengkapnya tentang menggabungkan instans EC2 Windows ke Microsoft AD yang AWS Dikelola, lihat [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#).
- Jika Anda perlu menggabungkan EC2 instance secara manual ke domain Active Directory, Anda harus meluncurkan instance di grup atau subnet yang tepat AWS Region dan keamanan, lalu bergabung dengan instance tersebut ke domain Active Directory.
- Untuk dapat terhubung dari jarak jauh ke instans ini, Anda harus memiliki konektivitas IP ke instans dari jaringan di mana Anda menghubungkannya dari. Dalam kebanyakan kasus, ini mengharuskan gateway internet dilampirkan ke VPC Amazon Anda dan instans tersebut memiliki alamat IP publik. Untuk informasi selengkapnya tentang menghubungkan ke internet menggunakan gateway internet lihat [Connect to the internet menggunakan gateway internet](#) di Panduan Pengguna Amazon VPC.

 Note

Setelah Anda menggabungkan instans ke Active Directory (lokal) yang dikelola sendiri, instans akan berkomunikasi langsung dengan Active Directory dan melewati AD Connector.

Kuota AD Connector

Berikut ini adalah Kuota default untuk AD Connector. Kecuali dinyatakan lain, masing-masing kuota adalah per Region.

Kuota AD Connector

Sumber daya	Kuota default
Direktori AD Connector	10
Jumlah maksimum dari sertifikat otoritas sertifikasi (CA) terdaftar per direktori	5

Memecahkan masalah AD Connector

Berikut ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temui saat membuat atau menggunakan AD Connector.

Topik

- [Masalah pembuatan](#)
- [Masalah konektivitas](#)
- [Masalah otentikasi](#)
- [Masalah pemeliharaan](#)
- [Saya tidak dapat menghapus AD Connector](#)
- [Alat umum untuk menyelidiki emiten AD Connector](#)

Masalah pembuatan

Berikut ini adalah masalah pembuatan yang umum untuk AD Connector

- [Saya menerima kesalahan “AZ Dibatasi” saat saya membuat direktori](#)
- [Saya menerima kesalahan “Masalah konektivitas terdeteksi” ketika saya mencoba membuat AD Connector](#)

Saya menerima kesalahan “AZ Dibatasi” saat saya membuat direktori

Beberapa AWS akun yang dibuat sebelum 2012 mungkin memiliki akses ke Availability Zones di Wilayah AS Timur (Virginia N.), AS Barat (California N.), atau Asia Pasifik (Tokyo) yang tidak mendukung Directory Service direktori. Jika Anda menerima kesalahan seperti ini saat membuat Active Directory, pilih subnet di Availability Zone yang berbeda dan coba buat direktori lagi.

Saya menerima kesalahan “Masalah konektivitas terdeteksi” ketika saya mencoba membuat AD Connector

Jika Anda menerima kesalahan “Masalah konektivitas terdeteksi” saat mencoba membuat Konektor AD, kesalahan mungkin karena ketersediaan port atau kompleksitas kata sandi AD Connector. Anda dapat menguji koneksi Konektor AD untuk melihat apakah port berikut tersedia:

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

Untuk menguji koneksi Anda, lihat [Uji AD Connector Anda](#). Tes koneksi harus dilakukan pada instance yang digabungkan ke kedua subnet yang terkait dengan alamat IP Konektor AD.

Jika tes koneksi berhasil dan instance bergabung dengan domain, periksa kata sandi Konektor AD Anda. AD Connector harus memenuhi persyaratan kompleksitas AWS kata sandi. Untuk informasi selengkapnya, lihat Akun layanan di [Prasyarat AD Connector](#).

Jika AD Connector Anda tidak memenuhi persyaratan ini, buat ulang AD Connector Anda dengan kata sandi yang sesuai dengan persyaratan ini.

Saya menerima “Kesalahan layanan internal telah ditemukan saat menghubungkan direktori. Silakan coba lagi operasinya.” kesalahan saat saya membuat AD Connector

Kesalahan ini biasanya terjadi ketika AD Connector gagal membuat dan tidak dapat terhubung ke pengontrol domain yang valid untuk domain Direktori Aktif yang dikelola sendiri.

Note

Sebagai [praktik terbaik](#), jika jaringan yang dikelola sendiri memiliki Situs Direktori Aktif yang ditentukan, Anda harus memastikan hal-hal berikut:

- Subnet VPC tempat AD Connector Anda berada ditentukan di Situs Direktori Aktif.
- Tidak ada konflik antara subnet VPC Anda dan subnet di situs Anda yang lain.

AD Connector menggunakan Situs Direktori Aktif yang rentang alamat IP subnetnya dekat dengan VPC yang berisi AD Connector untuk menemukan pengontrol domain AD Anda. Jika Anda memiliki situs yang subnetnya memiliki rentang alamat IP yang sama dengan yang ada di VPC Anda, AD Connector akan menemukan pengontrol domain di situs tersebut. Pengontrol domain mungkin secara fisik tidak dekat dengan Wilayah tempat Konektor AD Anda berada.

- Ketidakkonsistenan dalam catatan DNS SRV (Catatan ini menggunakan sintaks berikut: `_ldap._tcp.<DnsDomainName>` dan `_kerberos._tcp.<DnsDomainName>`) yang dibuat dalam domain Active Directory yang dikelola pelanggan. Ini dapat terjadi ketika AD Connector tidak dapat menemukan dan terhubung ke pengontrol domain yang valid berdasarkan catatan SRV ini.
- Masalah jaringan antara AD Connector dan AD yang dikelola pelanggan seperti perangkat firewall.

Anda dapat menggunakan [pengambilan paket jaringan](#) pada pengontrol domain, server DNS, dan log aliran VPC dari antarmuka jaringan direktori untuk menyelidiki masalah ini. Hubungi [AWS Dukungan](#) untuk bantuan lebih lanjut.

Masalah konektivitas

Berikut ini adalah masalah konektivitas umum untuk AD Connector

- [Saya menerima kesalahan "Masalah hubungan terdeteksi" ketika mencoba menghubungkan ke direktori on-premise saya](#)

- [Saya menerima error “DNS tidak tersedia” ketika mencoba menghubungkan ke direktori on-premise saya](#)
- [Saya menerima error “catatan SRV” ketika mencoba menghubungkan ke direktori on-premise saya](#)

Saya menerima kesalahan "Masalah hubungan terdeteksi" ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan galat yang mirip dengan berikut ini saat menyambung ke direktori lokal Anda: Masalah konektivitas terdeteksi: LDAP tidak tersedia (port TCP 389) untuk IP: *<IP address>* Kerberos/authentication tidak tersedia (port TCP 88) untuk IP: *<IP address>* Pastikan port yang terdaftar tersedia dan coba lagi operasi.

AD Connector harus dapat berkomunikasi dengan pengendali domain on-premise Anda melalui TCP dan UDP melewati port-port berikut. Verifikasi bahwa grup keamanan dan firewall on-premise mengizinkan komunikasi TCP dan UDP melewati port-port ini. Untuk informasi selengkapnya, lihat [Prasyarat AD Connector](#).

- 88 (Kerberos)
- 389 (LDAP)

Anda mungkin memerlukan TCP/UDP port tambahan tergantung pada kebutuhan Anda. Lihat daftar berikut untuk beberapa port ini. Untuk informasi selengkapnya tentang port yang digunakan oleh Active Directory, lihat [Cara mengonfigurasi firewall untuk domain Active Directory dan trust dalam Microsoft dokumentasi](#).

- 135 (Pemetaan Titik Akhir RPC)
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

Saya menerima error “DNS tidak tersedia” ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan error yang serupa dengan yang berikut ini saat menghubungkan ke direktori on-premise Anda:

DNS unavailable (TCP port 53) for IP: *<DNS IP address>*

AD Connector harus dapat berkomunikasi dengan server DNS on-premise Anda melalui TCP dan UDP melewati port 53. Verifikasi bahwa grup keamanan dan firewall on-premise mengizinkan komunikasi TCP dan UDP melewati port ini. Untuk informasi selengkapnya, lihat [Prasyarat AD Connector](#).

Saya menerima error “catatan SRV” ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan error yang serupa dengan satu atau beberapa berikut ini saat menghubungkan ke direktori on-premise Anda:

SRV record for LDAP does not exist for IP: *<DNS IP address>* SRV record for Kerberos does not exist for IP: *<DNS IP address>*

AD Connector perlu memperoleh catatan SRV `_ldap._tcp.<DnsDomainName>` dan `_kerberos._tcp.<DnsDomainName>` saat menghubungkan ke direktori Anda. Anda akan mendapatkan error ini jika layanan tidak dapat memperoleh catatan ini dari server DNS yang Anda tentukan saat menghubungkan ke direktori Anda. Untuk informasi selengkapnya mengenai catatan SRV ini, lihat [SRV record requirements](#).

Masalah otentikasi

Berikut adalah beberapa masalah otentikasi umum dengan AD Connector:

- [Saya menerima kesalahan “Validasi Sertifikat gagal” ketika saya mencoba masuk Amazon WorkSpaces dengan kartu pintar](#)
- [Saya menerima error “Kredensial Tidak Valid” saat akun layanan yang digunakan oleh AD Connector mencoba untuk mengautentikasi](#)
- [Saya menerima kesalahan “Tidak Dapat Mengautentikasi” saat menggunakan AWS aplikasi untuk mencari pengguna atau grup](#)
- [Saya menerima kesalahan tentang kredensial direktori saya ketika saya mencoba memperbarui akun layanan AD Connector](#)
- [Beberapa pengguna saya tidak dapat mengautentikasi dengan direktori saya](#)

Saya menerima kesalahan “Validasi Sertifikat gagal” ketika saya mencoba masuk Amazon WorkSpaces dengan kartu pintar

Anda menerima pesan galat yang mirip dengan berikut ini ketika Anda mencoba masuk ke kartu pintar Anda WorkSpaces : ERROR: Validasi Sertifikat gagal. Silakan coba lagi dengan me-restart browser atau aplikasi Anda dan pastikan Anda memilih sertifikat yang benar. Kesalahan terjadi jika sertifikat kartu pintar tidak disimpan dengan benar pada klien yang menggunakan sertifikat. Untuk informasi selengkapnya tentang AD Connector dan persyaratan kartu pintar, lihat [Prasyarat](#).

Gunakan prosedur berikut untuk memecahkan masalah kemampuan kartu pintar untuk menyimpan sertifikat di toko sertifikat pengguna:

1. Pada perangkat yang mengalami kesulitan mengakses sertifikat, akses Microsoft Management Console (MMC).

Important

Sebelum bergerak maju, buat salinan sertifikat kartu pintar.

2. Arahkan ke toko sertifikat di MMC. Hapus sertifikat kartu pintar pengguna dari toko sertifikat. Untuk informasi selengkapnya tentang melihat penyimpanan sertifikat di MMC, lihat [Cara: Melihat sertifikat dengan snap-in MMC dalam](#) dokumentasi. Microsoft
3. Lepaskan kartu pintar.
4. Masukkan kembali kartu pintar sehingga dapat mengisi kembali sertifikat kartu pintar di toko sertifikat pengguna.

Warning

Jika kartu pintar tidak mengisi kembali sertifikat ke toko pengguna maka tidak dapat digunakan untuk otentikasi kartu WorkSpaces pintar.

Akun Layanan Konektor AD harus memiliki yang berikut:

- my/spnditambahkan ke Nama Prinsip Layanan
- Delegasikan untuk layanan LDAP

Setelah sertifikat diisi kembali pada kartu pintar, pengontrol domain on-premise harus diperiksa untuk menentukan apakah mereka diblokir dari pemetaan Nama Utama Pengguna (UPN) untuk Nama Alternatif Subjek. Untuk informasi selengkapnya tentang perubahan ini, lihat [Cara menonaktifkan Nama Alternatif Subjek untuk pemetaan UPN dalam Microsoft dokumentasi](#).

Gunakan prosedur berikut untuk memeriksa kunci registri pengontrol domain Anda:

- Di Editor Registri, arahkan ke kunci sarang berikut

HKEY_LOCAL_MACHINE\ SISTEM\ Layanan\ Kdc\ CurrentControlSet UseSubjectAltName

- Periksa nilai: UseSubjectAltName
 - i. Jika nilainya disetel ke 0, maka pemetaan Nama Alternatif Subjek dinonaktifkan dan Anda harus secara eksplisit memetakan sertifikat yang diberikan hanya ke 1 pengguna. Jika sertifikat dipetakan ke beberapa pengguna dan nilai ini adalah 0, login dengan sertifikat itu akan gagal.
 - ii. Jika nilainya tidak disetel atau disetel ke 1, Anda harus secara eksplisit memetakan sertifikat yang diberikan hanya ke 1 pengguna atau menggunakan bidang Nama Alternatif Subjek untuk login.
 - A. Jika bidang Nama Alternatif Subjek ada pada sertifikat, itu akan diprioritaskan.
 - B. Jika bidang Nama Alternatif Subjek tidak ada pada sertifikat dan sertifikat secara eksplisit dipetakan ke lebih dari satu pengguna, login dengan sertifikat itu akan gagal.

Note

Jika kunci registri diatur pada Pengontrol Domain on-premise maka AD Connector tidak akan dapat menemukan pengguna di Active Directory dan menghasilkan pesan kesalahan di atas.

Sertifikat Otoritas Sertifikat (CA) harus diunggah ke sertifikat kartu pintar AD Connector. Sertifikat harus berisi informasi OCSP. Berikut daftar persyaratan tambahan untuk CA:

- Sertifikat harus berada di Otoritas Root Terpercaya dari Pengontrol Domain, Server Otoritas Sertifikat, dan WorkSpaces.

- Sertifikat Offline dan Root CA tidak akan berisi informasi OSCP. Sertifikat ini berisi informasi tentang pencabutan mereka.
- Jika Anda menggunakan sertifikat CA pihak ketiga untuk otentikasi kartu pintar, maka CA dan sertifikat perantara harus dipublikasikan ke NTAAuth toko Active Directory. Mereka harus diinstal di otoritas root tepercaya untuk semua pengontrol domain, server otoritas sertifikat, dan WorkSpaces.
- Anda dapat menggunakan perintah ikuti untuk mempublikasikan sertifikat ke NTAAuth toko Active Directory:

```
certutil -dspublish -f Third_Party_CA.cer NTAAuthCA
```

Untuk informasi selengkapnya tentang menerbitkan sertifikat ke NTAAuth toko, lihat [Mengimpor sertifikat CA yang diterbitkan ke NTAAuth toko Enterprise di](#) Access Amazon WorkSpaces dengan Panduan Instalasi Kartu Akses Umum.

Anda dapat memeriksa untuk melihat apakah sertifikat pengguna atau sertifikat rantai CA diverifikasi oleh OCSP dengan mengikuti prosedur ini:

1. Ekspor sertifikat kartu pintar ke lokasi di mesin lokal seperti drive C:.
2. Buka prompt Baris Perintah dan arahkan ke lokasi penyimpanan sertifikat kartu pintar yang diekspor.
3. Masukkan perintah berikut:

```
certutil -URL Certificate_name.cer
```

4. Jendela pop-up akan muncul mengikuti perintah. Pilih opsi OCSP di sudut kanan dan pilih Ambil. Status harus kembali seperti yang diverifikasi.

Untuk informasi lebih lanjut tentang perintah certutil, lihat [certutil](#) dalam dokumentasi Microsoft

Saya menerima error “Kredensial Tidak Valid” saat akun layanan yang digunakan oleh AD Connector mencoba untuk mengautentikasi

Hal ini dapat terjadi jika hard drive pada pengendali domain Anda kehabisan ruang. Pastikan bahwa hard drive pengendali domain Anda tidak penuh.

Saya menerima “Kesalahan telah terjadi” atau “Kesalahan tak terduga” ketika saya mencoba memperbarui akun layanan AD Connector

Kesalahan atau gejala berikut terjadi saat mencari pengguna di Aplikasi AWS Perusahaan seperti [Amazon WorkSpaces Console Launch Wizard](#):

- Telah Terjadi Kesalahan. Jika Anda terus mengalami masalah, hubungi AWS Dukungan Tim di forum komunitas dan melalui Dukungan AWS Premium.
- Telah Terjadi Kesalahan. Direktori Anda membutuhkan pembaruan kredensi. Harap perbarui kredensial direktori.

Jika Anda mencoba memperbarui kredensial akun layanan AD Connector di AD Connector, Anda mungkin menerima pesan galat berikut:

- Kesalahan tak terduga. Terjadi kesalahan tak terduga.
- Terjadi kesalahan. Ada kesalahan dengan account/password kombinasi layanan. Silakan coba lagi.

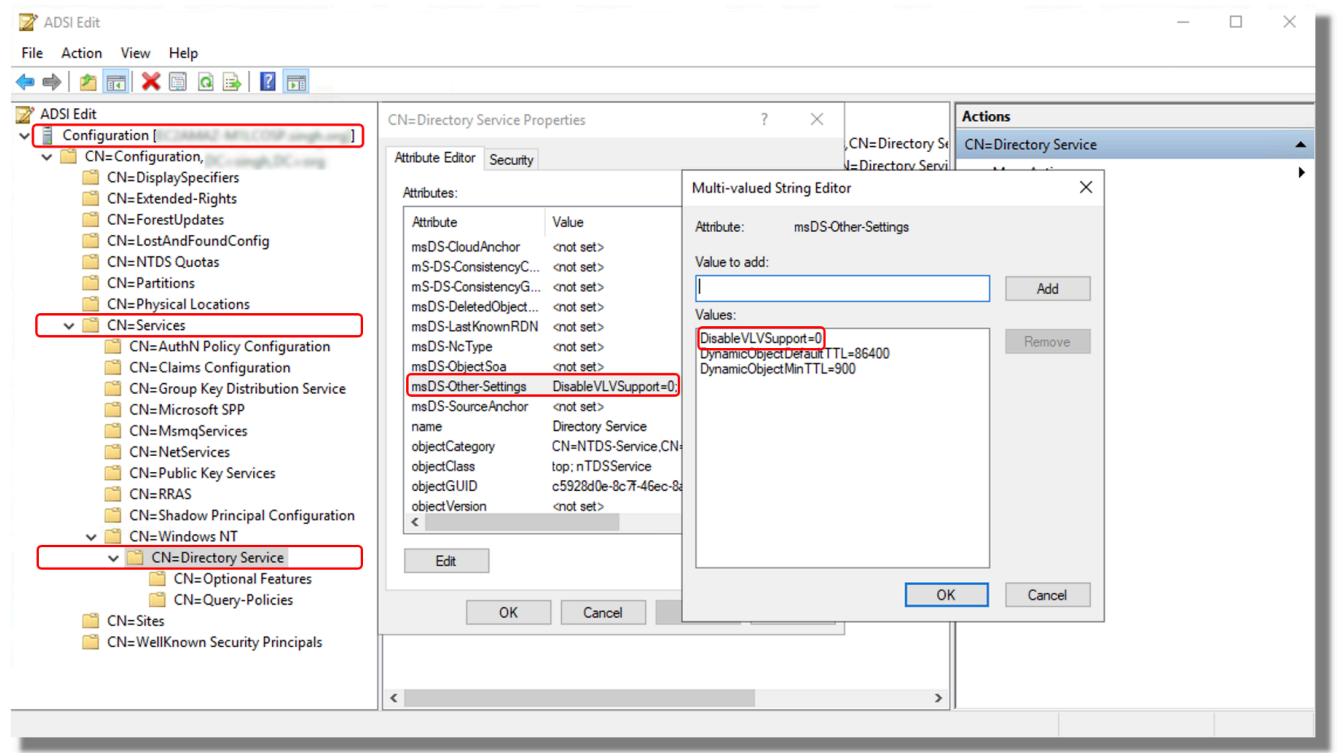
Akun layanan direktori AD Connector berada di Active Directory yang dikelola pelanggan. Akun digunakan sebagai identitas untuk melakukan kueri dan operasi pada domain Active Directory yang dikelola pelanggan melalui AD Connector atas nama Aplikasi AWS Perusahaan. AD Connector menggunakan Kerberos dan LDAP untuk melakukan operasi ini.

Daftar berikut menjelaskan apa arti pesan kesalahan ini:

- Mungkin ada masalah dengan sinkronisasi waktu dan Kerberos. AD Connector mengirimkan permintaan otentikasi Kerberos ke Active Directory. Permintaan ini sensitif terhadap waktu dan jika permintaan ditunda, mereka akan gagal. Pastikan tidak ada masalah sinkronisasi waktu antara pengontrol domain yang dikelola pelanggan. Untuk mengatasi masalah ini, lihat [Rekomendasi - Mengonfigurasi Root PDC dengan Sumber Waktu Otoritatif dan Hindari Kemiringan Waktu Luas](#) dalam dokumentasi. Microsoft Untuk informasi selengkapnya tentang layanan waktu dan sinkronisasi, lihat berikut ini:
 - [Bagaimana Layanan Windows Waktu Bekerja](#)
 - [Toleransi maksimum untuk sinkronisasi jam komputer](#)
 - [Windows Alat dan pengaturan layanan waktu](#)

- [Perangkat jaringan perantara, dengan pembatasan MTU jaringan, seperti konfigurasi perangkat keras Firewall atau VPN, antara AD Connector dan pengontrol domain yang dikelola pelanggan, dapat menyebabkan kesalahan ini karena fragmentasi jaringan.](#)
- Untuk memverifikasi pembatasan MTU, Anda dapat melakukan [pengujian Ping](#) antara pengontrol domain terkelola pelanggan dan instans Amazon EC2 yang diluncurkan di salah satu subnet direktori yang terhubung melalui AD Connector. Ukuran bingkai tidak boleh lebih besar dari ukuran default 1500 Bytes
- Tes ping akan membantu Anda memahami apakah ukuran bingkai lebih dari 1500 byte (juga dikenal sebagai bingkai Jumbo) dan mereka dapat mencapai AD Connector VPC dan subnet tanpa perlu fragmentasi. Verifikasi lebih lanjut dengan tim jaringan Anda dan pastikan bahwa bingkai Jumbo diizinkan di perangkat jaringan perantara.
- Anda mungkin menghadapi masalah ini, jika [LDAPS sisi klien diaktifkan di](#) AD Connector, dan sertifikat kedaluwarsa. Pastikan sertifikat sisi server dan sertifikat CA valid, belum kedaluwarsa, dan memenuhi persyaratan sesuai [LDAPsdokumentasi](#).
- Jika [Virtual List View Support](#) dinonaktifkan di domain Active Directory yang dikelola pelanggan, maka AWS Aplikasi tidak akan dapat mencari pengguna karena AD Connector menggunakan pencarian VLV dalam kueri LDAP. Dukungan Tampilan Daftar Virtual dinonaktifkan ketika Nonaktifkan VLVSupport diatur ke nilai bukan nol. Pastikan [Dukungan Virtual List View \(VLV\)](#) diaktifkan di Active Directory menggunakan langkah-langkah berikut:
 1. Masuk ke Pengontrol Domain sebagai pemilik peran master skema menggunakan akun dengan kredensial Admin Skema.
 2. Pilih Mulai dan kemudian Jalankan, dan masukkan **Adsiedit.msc**.
 3. Di alat Edit ADSI, Connect to Configuration Partition, dan perluas node Configuration [DomainController].
 4. Perluas CN = konfigurasi, DC DomainName = wadah.
 5. Perluas objek CN=Services.
 6. Perluas objek CN = Windows NT.
 7. Pilih objek CN=Directory Service. Pilih Properti.
 8. Dalam daftar Atribut, pilih MSDS-Other-Settings. Pilih Edit.
 9. Dalam daftar Nilai, pilih contoh Nonaktifkan VLVSupport = x di mana x tidak sama dengan 0, dan pilih Hapus.
 10. Setelah menghapus, masukkan **DisableVLVSupport=0**. Pilih Tambahkan.

11. Pilih OK. Anda dapat menutup alat Edit ADSI. Gambar berikut menunjukkan kotak dialog Editor String Multi-nilai di jendela Edit ADSI:



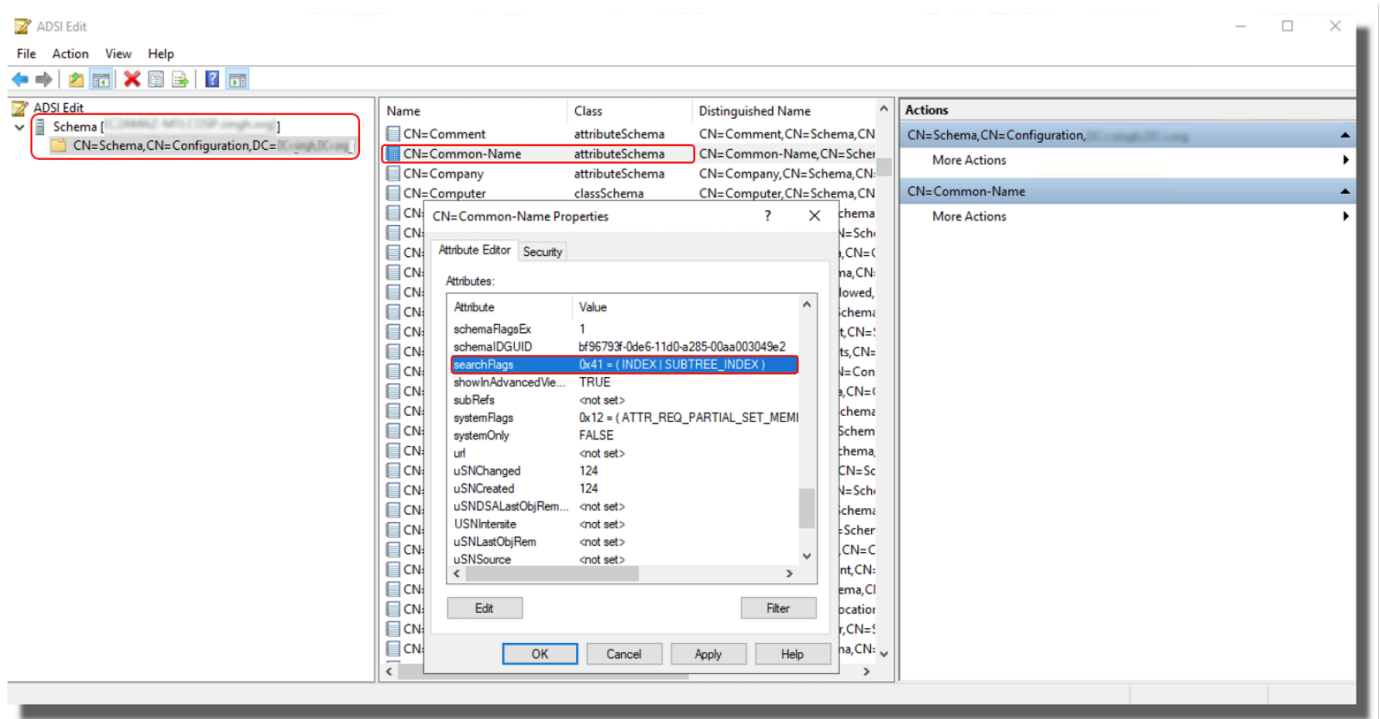
Note

Dalam infrastruktur Active Directory besar dengan lebih dari 100.000 pengguna, Anda mungkin hanya dapat mencari pengguna tertentu. Namun, jika Anda mencoba mencantumkan semua pengguna (Misalnya, Tampilkan Semua Pengguna di WorkSpaces Launch Wizard) sekaligus, itu mungkin mengakibatkan kesalahan yang sama meskipun Dukungan VLV diaktifkan. AD Connector mengharuskan hasil diurutkan untuk atribut "CN" menggunakan Subtree Index. Indeks Subtree adalah jenis indeks yang mempersiapkan pengontrol domain untuk melakukan operasi pencarian Virtual List View (LDAP) yang memungkinkan AD Connector menyelesaikan pencarian yang diurutkan. Indeks ini meningkatkan pencarian VLV dan mencegah penggunaan tabel database sementara yang disebut. [MaxTempTableSize](#) Ukuran tabel ini dapat bervariasi, tetapi secara default jumlah maksimum entri adalah 10000 (MaxTempTableSize pengaturan Kebijakan Kueri Default). Meningkatkan kurang efisien daripada menggunakan Pengindeksan Subtree. MaxTempTableSize Untuk menghindari kesalahan ini di lingkungan AD yang besar, disarankan untuk menggunakan Subtree Indexing.

Anda dapat mengaktifkan indeks Subtree dengan memodifikasi atribut [searchflags](#) pada definisi atribut, dalam skema Active Directory, dengan nilai 65 (0x41), menggunakan langkah-langkah berikut: ADSEdit

1. Masuk ke Pengontrol Domain sebagai pemilik peran master skema menggunakan akun dengan kredensial Admin Skema.
2. Pilih Mulai dan Jalankan, masukkan **Adsiedit.msc**.
3. Di alat Edit ADSI, sambungkan ke Partisi Skema.
4. Perluas CN = skema, CN = konfigurasi, DC = wadah. DomainName
5. Temukan atribut "Common-Name" dan klik kanan dan pilih Properties.
6. Temukan atribut searchFlags dan ubah nilainya **65 (0x41)** untuk mengaktifkan SubTree pengindeksan bersama dengan Indeks normal.

Gambar berikut menunjukkan CN = Common-name properties kotak dialog di jendela Edit ADSI:



7. Pilih OK. Anda dapat menutup alat Edit ADSI.
8. Untuk konfirmasi, Anda harus dapat melihat ID peristiwa 1137 (Sumber: Direktori Aktif_DomainServices), yang menunjukkan bahwa AD telah berhasil membuat indeks baru untuk atribut yang ditentukan.

Untuk informasi lebih lanjut, lihat [Microsoftdokumentasi](#).

Saya menerima kesalahan “Tidak Dapat Mengautentikasi” saat menggunakan AWS aplikasi untuk mencari pengguna atau grup

Anda mungkin mengalami kesalahan saat mencari pengguna atau masuk ke AWS aplikasi, seperti WorkSpaces atau Quick, bahkan saat status AD Connector aktif. Jika kata sandi akun layanan AD Connector telah diubah atau kedaluwarsa, AD Connector tidak dapat lagi menanyakan domain Active Directory. Hubungi Administrator AD Anda dan verifikasi hal-hal berikut:

- Periksa kata sandi akun layanan AD Connector belum kedaluwarsa
- Memeriksa akun layanan AD Connector tidak memiliki opsi Pengguna harus mengubah kata sandi saat login berikutnya diaktifkan.
- Periksa akun layanan AD Connector tidak terkunci.
- Jika Anda tidak yakin apakah kata sandi telah kedaluwarsa atau diubah, Anda dapat mengatur ulang kata sandi akun layanan dan juga [memperbarui](#) kata sandi yang sama di AD Connector.

Saya menerima kesalahan tentang kredensial direktori saya ketika saya mencoba memperbarui akun layanan AD Connector

Anda menerima pesan galat yang mirip dengan satu atau beberapa hal berikut saat mencoba memperbarui akun layanan AD Connector:

Pesan: Telah Terjadi Kesalahan Direktori Anda membutuhkan pembaruan kredensial. Harap perbarui kredensial direktori. Terjadi Kesalahan Direktori Anda memerlukan pembaruan kredensial. Harap perbarui kredensial direktori berikut Perbarui Kredensial Akun Layanan AD Connector Anda
Pesan: Terjadi Kesalahan Permintaan Anda bermasalah. Silakan lihat detail berikut. Ada kesalahan dengan kombinasi akun layanan/kata sandi

Mungkin ada masalah dengan sinkronisasi waktu dan Kerberos. AD Connector mengirimkan permintaan otentikasi Kerberos ke Active Directory. Permintaan ini sensitif terhadap waktu dan jika permintaan ditunda, mereka akan gagal. Untuk mengatasi masalah ini, lihat [Rekomendasi - Mengonfigurasi Root PDC dengan Sumber Waktu Otoritatif dan Hindari Kemiringan Waktu Luas](#) dalam dokumentasi. Microsoft Untuk informasi lebih lanjut tentang layanan waktu dan sinkronisasi, lihat di bawah ini:

- [Bagaimana Layanan Windows Waktu Bekerja](#)
- [Toleransi maksimum untuk sinkronisasi jam komputer](#)
- [Windows Alat dan pengaturan layanan waktu](#)

Beberapa pengguna saya tidak dapat mengautentikasi dengan direktori saya

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Ini adalah pengaturan default untuk akun pengguna baru, tetapi tidak boleh diubah. Untuk informasi selengkapnya tentang pengaturan ini, buka [Preauthentication](#) on. Microsoft TechNet

Masalah pemeliharaan

Berikut ini adalah masalah perawatan umum untuk AD Connector

- Direktori saya terjebak dalam status “Diminta”
- Gabungan domain yang mulus untuk instans Amazon EC2 berhenti berfungsi

Direktori saya terjebak dalam status “Diminta”

Jika Anda memiliki direktori yang telah berada dalam status “Diminta” selama lebih dari lima menit, coba hapus direktori dan buat ulang. Jika masalah ini berlanjut, hubungi [AWS Dukungan](#).

Gabungan domain yang mulus untuk instans Amazon EC2 berhenti berfungsi

Jika penggabungan domain yang mulus untuk instans EC2 bekerja dan kemudian berhenti saat AD Connector aktif, kredensial untuk akun layanan AD Connector Anda mungkin telah kedaluwarsa. Kredensial yang kedaluwarsa dapat mencegah AD Connector membuat objek komputer di Direktori Aktif Anda.

Untuk mengatasi masalah ini, perbarui kata sandi akun layanan dalam urutan berikut sehingga kata sandi cocok:

1. Perbarui kata sandi untuk akun layanan di Direktori Aktif Anda.
2. Perbarui kata sandi untuk akun layanan di AD Connector Anda di Directory Service. Untuk informasi selengkapnya, lihat [Memperbarui kredensi akun layanan AD Connector Anda di Konsol Manajemen AWS](#).

Important

Memperbarui kata sandi hanya di Directory Service tidak mendorong perubahan kata sandi ke Active Directory lokal yang ada sehingga penting untuk melakukannya dalam urutan yang ditunjukkan pada prosedur sebelumnya.

Saya tidak dapat menghapus AD Connector

Jika AD Connector beralih ke status tidak dapat dioperasikan, Anda tidak lagi memiliki akses ke pengontrol domain. Kami memblokir penghapusan AD Connector ketika masih ada aplikasi yang terhubung dengannya karena salah satu aplikasi tersebut mungkin masih menggunakan direktori. Untuk daftar aplikasi yang perlu Anda nonaktifkan untuk menghapus AD Connector Anda, lihat [Menghapus AD Connector](#). Jika Anda masih tidak dapat menghapus AD Connector, Anda dapat meminta bantuan melalui [AWS Dukungan](#).

Alat umum untuk menyelidiki emiten AD Connector

Alat-alat berikut dapat digunakan untuk memecahkan masalah berbagai masalah AD Connector yang terkait dengan pembuatan, otentikasi, dan konektivitas:

DirectoryServicePortTest alat

Alat [DirectoryServicePortTest](#) pengujian dapat membantu saat memecahkan masalah konektivitas antara AD Connector dan Active Directory atau server DNS yang dikelola pelanggan. Untuk informasi selengkapnya tentang cara menggunakan alat ini, lihat [Uji AD Connector Anda](#).

Alat penangkap paket

Anda dapat menggunakan utilitas pengambilan Windows paket bawaan ([netsh](#)) untuk menyelidiki dan memecahkan masalah jaringan potensial atau masalah komunikasi Direktori Aktif (ldap dan kerberos). Untuk informasi selengkapnya, lihat [Mengambil Jejak Jaringan tanpa menginstal apa pun](#).

Log Alur VPC

Untuk lebih memahami permintaan apa yang diterima dan dikirim dari AD Connector, Anda dapat mengonfigurasi [log aliran VPC](#) untuk antarmuka jaringan direktori. Anda dapat mengidentifikasi semua antarmuka jaringan yang dicadangkan untuk digunakan Directory Service dengan deskripsi: `AWS created network interface for directory your-directory-id`.

Kasus penggunaan sederhana adalah selama pembuatan AD Connector dengan domain Active Directory yang dikelola pelanggan dengan sejumlah besar pengontrol domain. Anda dapat menggunakan log aliran VPC dan memfilter oleh port Kerberos (88) untuk mengetahui pengontrol domain apa di Direktori Aktif yang dikelola pelanggan yang dihubungi untuk otentikasi.

Simple AD

Simple AD adalah direktori terkelola mandiri yang didukung oleh Samba 4 Active Directory Compatible Server. Ini tersedia dalam dua ukuran.

- Kecil - Mendukung hingga 500 pengguna (sekitar 2.000 objek termasuk pengguna, grup, dan komputer).
- Large - Mendukung hingga 5.000 pengguna (sekitar 20.000 objek termasuk pengguna, grup, dan komputer).

Simple AD menyediakan subset fitur yang ditawarkan oleh Microsoft AD yang AWS Dikelola, termasuk kemampuan untuk mengelola akun pengguna dan keanggotaan grup, membuat dan menerapkan kebijakan grup, terhubung dengan aman ke EC2 instans Amazon, dan menyediakan sistem masuk tunggal (SSO) berbasis Kerberos. Namun, perhatikan bahwa Simple AD tidak mendukung fitur seperti otentikasi multi-faktor (MFA), hubungan kepercayaan dengan domain lain, Pusat Administrasi Direktori Aktif, PowerShell dukungan, tempat daur ulang Direktori Aktif, akun layanan terkelola grup, dan ekstensi skema untuk aplikasi POSIX dan Microsoft.

Simple AD menawarkan banyak keuntungan:

- Simple AD memudahkan [pengelolaan EC2 instans amazon yang menjalankan Linux dan Windows](#) dan menyebarkan aplikasi Windows di AWS Cloud.
- Kebanyakan aplikasi dan alat-alat yang Anda gunakan hari ini yang memerlukan dukungan Microsoft Active Directory dapat digunakan dengan Simple AD.
- Akun pengguna di Simple AD memungkinkan akses ke AWS aplikasi seperti WorkSpaces, WorkDocs, atau Amazon WorkMail.
- Anda dapat mengelola AWS sumber daya melalui akses berbasis peran IAM ke. Konsol Manajemen AWS
- Snapshot otomatis harian memungkinkan point-in-time pemulihan.

Simple AD tidak mendukung berikut ini:

- WorkSpaces Aplikasi Amazon
- Amazon Chime
- Amazon FSx

- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- AWS IAM Identity Center
- Hubungan Kepercayaan dengan domain lain
- Pusat Administrasi Direktori Aktif
- PowerShell
- Keranjang sampah Direktori Aktif
- Akun layanan yang dikelola grup
- Ekstensi skema untuk aplikasi POSIX dan Microsoft

Lanjutkan membaca topik di bagian ini untuk mempelajari cara membuat Simple AD Anda sendiri.

Topik

- [Memulai dengan Simple AD](#)
- [Praktik terbaik untuk Simple AD](#)
- [Memelihara direktori Simple AD](#)
- [Amankan direktori Simple AD Anda](#)
- [Memantau direktori Simple AD](#)
- [Akses ke AWS aplikasi dan layanan dari Simple AD](#)
- [Cara untuk bergabung dengan instans Amazon EC2 ke Simple AD Anda](#)
- [Manajemen pengguna dan grup di Simple AD](#)
- [Kuota Simple AD](#)
- [Pemecahan masalah Simple AD](#)

Memulai dengan Simple AD

Simple AD membuat direktori berbasis Samba yang dikelola sepenuhnya di cloud. AWS Saat Anda membuat direktori dengan Simple AD, Directory Service buat dua pengontrol domain dan server DNS atas nama Anda. Pengontrol domain dibuat dalam subnet yang berbeda di VPC Amazon, redundansi ini membantu memastikan bahwa direktori Anda tetap dapat diakses bahkan jika terjadi kegagalan.

Topik

- [Prasyarat Simple AD](#)
- [Buat Simple AD Anda](#)
- [Apa yang dibuat dengan Simple AD Anda](#)

Prasyarat Simple AD

Untuk membuat Simple AD Active Directory, Anda memerlukan VPC Amazon dengan yang berikut ini:

- VPC harus memiliki penghunian perangkat keras default.

Anda dapat menggunakan IPv6 untuk VPC Anda. Untuk informasi selengkapnya, lihat [IPv6 dukungan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.

- Setidaknya dua subnet dalam dua Availability Zone yang berbeda dan harus dari jenis jaringan yang sama. Subnet harus berada dalam rentang Classless Inter-Domain Routing (CIDR) yang sama. Jika Anda ingin memperpanjang atau mengubah ukuran VPC untuk direktori Anda, maka pastikan untuk memilih kedua subnet pengendali domain untuk rentang VPC CIDR yang diperpanjang. Saat Anda membuat Simple AD, Directory Service buat dua pengontrol domain dan server DNS atas nama Anda.
- Untuk informasi selengkapnya tentang rentang CIDR, lihat [pengalaman IP untuk subnet Anda VPCs dan subnet di Panduan](#) Pengguna Amazon VPC.
- Jika Anda memerlukan dukungan LDAPS dengan Simple AD, kami sarankan Anda mengonfigurasinya menggunakan Network Load Balancer yang terhubung ke port 389. Model ini memungkinkan Anda untuk menggunakan sertifikat yang kuat untuk hubungan LDAPS, menyederhanakan akses ke LDAPS melalui alamat IP NLB tunggal, dan memiliki kegagalan otomatis melalui NLB. Simple AD tidak mendukung penggunaan sertifikat yang ditandatangani sendiri pada port 636. Untuk informasi selengkapnya tentang cara mengkonfigurasi LDAPS dengan Simple AD, lihat [Cara mengkonfigurasi titik akhir LDAPS untuk Simple AD](#) di Blog Keamanan AWS.
- Jenis enkripsi berikut harus diaktifkan dalam direktori:
 - RC4_HMAC_MD5
 - AES128_HMAC_SHA1
 - AES256_HMAC_SHA1
 - Jenis enkripsi masa depan

 Note

Menonaktifkan jenis enkripsi ini dapat menyebabkan masalah komunikasi dengan RSAT (Remote Server Administration Tools) dan mempengaruhi ketersediaan atau direktori Anda.

- Untuk informasi lebih lanjut, lihat [Apa itu Amazon VPC?](#) di Panduan Pengguna Amazon VPC.

Directory Service menggunakan dua struktur VPC. Instans EC2 yang membentuk direktori Anda berjalan di luar AWS akun Anda, dan dikelola oleh AWS Mereka memiliki dua adaptor jaringan, ETH0 dan ETH1. ETH0 adalah adaptor pengelola, dan berada di luar akun Anda. ETH1 dibuat dalam akun Anda.

Rentang IP pengelola jaringan ETH0 direktori Anda dipilih secara terprogram untuk memastikan tidak bertentangan dengan VPC tempat direktori Anda di-deploy. Rentang IP ini dapat berupa salah satu pasangan berikut (karena Direktori berjalan di dua subnet):

- 10.0.1.0/24 & 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 & 192.168.2.0/24

Kami menghindari konflik dengan memeriksa oktet pertama dari ETH1 CIDR. Jika dimulai dengan 10, maka kami memilih VPC 192.168.0.0/16 dengan subnet 192.168.1.0/24 dan 192.168.2.0/24. Jika oktet pertama adalah yang lain selain 10, kami memilih VPC 10.0.0.0/16 dengan subnet 10.0.1.0/24 dan 10.0.2.0/24.

Algoritma pemilihan tidak mencakup rute pada VPC Anda. Oleh karena itu Anda dapat mengalami konflik IP perutean yang dihasilkan dari skenario ini.

 Important

Jika salah satu prasyarat Simple AD diubah setelah Simple AD Anda dibuat, Simple AD Anda dapat menjadi Terganggu. Untuk mengatasi status Gangguan Iklan Sederhana Anda, Anda harus menghubungi [AWS Dukungan](#).

Buat Simple AD Anda

Prosedur ini memandu Anda melalui semua langkah yang diperlukan untuk membuat Simple AD. Ini dimaksudkan untuk membantu Anda memulai dengan Simple AD dengan cepat dan mudah, tetapi tidak dimaksudkan untuk digunakan dalam lingkungan produksi skala besar.

Langkah-langkah

- [Prasyarat](#)
- [Membuat dan mengonfigurasi VPC Amazon Anda untuk Simple AD Anda](#)
- [Membuat Simple AD Anda](#)

Prasyarat

Prosedur ini mengasumsikan hal berikut:

- Anda memiliki yang aktif Akun AWS.
- Akun Anda belum mencapai batas Amazon VPCs untuk Wilayah tempat Anda ingin menggunakan Simple AD. Untuk informasi selengkapnya tentang VPC, lihat [Apa itu Amazon VPC?](#) dan [Subnet di VPC Anda di](#) Panduan Pengguna Amazon VPC.
- Anda tidak memiliki VPC yang ada di Wilayah dengan CIDR sebesar. 10.0.0.0/16
- Anda berada di Wilayah di mana Simple AD tersedia. Untuk informasi selengkapnya, lihat [Ketersediaan wilayah untuk Directory Service](#).

Untuk informasi selengkapnya, lihat [Prasyarat Simple AD](#).

Membuat dan mengonfigurasi VPC Amazon Anda untuk Simple AD Anda

Pertama, Anda akan membuat dan mengonfigurasi VPC Amazon untuk digunakan dengan Simple AD Anda. Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikan [Prasyarat](#).

VPC yang akan Anda buat akan memiliki dua subnet publik. Directory Service membutuhkan dua subnet di VPC Anda, dan setiap subnet harus berada di Availability Zone yang berbeda.

Buat VPC

1. Buka konsol Amazon VPC di. <https://console.aws.amazon.com/vpc/>
2. Di Dasbor VPC, pilih Buat VPC.

3. Di bawah pengaturan VPC, pilih VPC dan lainnya.
4. Lengkapi bidang-bidang ini sebagai berikut:
 - Tetap Dipilih secara otomatis di bawah Generasi otomatis tag nama. Ubah proyek menjadi ADS VPC.
 - Blok IPv4 CIDR seharusnya. 10.0.0.0/16
 - Simpan opsi blok Tidak ada IPv6 CIDR yang dipilih.
 - Penyewaan harus tetap Default.
 - Pilih 2 untuk Jumlah Availability Zones (AZs).
 - Pilih 2 untuk Jumlah subnet publik. Jumlah subnet pribadi dapat diubah menjadi 0.
 - Pilih Sesuaikan blok CIDR subnet untuk mengonfigurasi rentang alamat IP subnet publik. Blok CIDR subnet publik harus 10.0.0.0/20 dan. 10.0.16.0/20
5. Pilih Buat VPC. Ini akan memerlukan beberapa menit sampai VPC dibuat.

Membuat Simple AD Anda

Untuk membuat Simple AD baru, lakukan langkah-langkah berikut. Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikan hal-hal berikut di [Prasyarat](#) dan [Membuat dan mengonfigurasi VPC Amazon Anda untuk Simple AD Anda](#).

Buat Iklan Sederhana

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori, lalu pilih Atur direktori.
2. Di halaman Pilih jenis direktori, pilih Simple AD, lalu pilih Selanjutnya.
3. Di halaman Masukkan informasi direktori, berikan informasi berikut:

Ukuran direktori

Pilih salah satu opsi ukuran Small atau Large. Untuk informasi selengkapnya tentang ukuran, lihat [Simple AD](#).

Nama organisasi

Sebuah nama organisasi yang unik untuk direktori Anda yang akan digunakan untuk mendaftarkan perangkat klien.

Bidang ini hanya tersedia jika Anda membuat direktori sebagai bagian dari peluncuran WorkSpaces.

Nama DNS direktori

Nama berkualifikasi penuh untuk direktori, seperti `corp.example.com`.

Direktori nama NetBIOS

Nama singkat untuk direktori, seperti `CORP`.

Kata sandi administrator

Kata sandi untuk administrator direktori. Proses pembuatan direktori menciptakan akun administrator dengan nama pengguna `Administrator` dan kata sandi ini.

Kata sandi administrator direktori peka akan huruf besar kecil dan harus terdiri dari 8 sampai 64 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:

- Huruf kecil (a-z)
- Huruf besar (A-Z)
- Angka (0-9)
- Karakter non-alfanumerik (~!@#\$%^&* _-+=`|()\{}[]:;'"<>,.?/)

Konfirmasikan kata sandi

Ketik ulang kata sandi administrator.

Important

Pastikan untuk menyimpan kata sandi ini. Directory Service tidak menyimpan kata sandi ini, dan tidak dapat diambil. Namun, Anda dapat mengatur ulang kata sandi dari Directory Service konsol atau dengan menggunakan [ResetUserPasswordAPI](#).

Deskripsi direktori

Deskripsi opsional untuk direktori.

4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.

VPC

VPC untuk direktori.

Subnet

Pilih subnet untuk pengendali domain. Kedua subnet harus berada di Zona Ketersediaan yang berbeda.

5. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Ini akan memerlukan beberapa menit sampai direktori dibuat. Setelah dibuat, nilai Status berubah ke Aktif.

Untuk informasi selengkapnya tentang apa yang dibuat dengan Simple AD Anda, lihat [Apa yang dibuat dengan Simple AD Anda](#).

Apa yang dibuat dengan Simple AD Anda

Saat Anda membuat Direktori Aktif dengan Simple AD, Directory Service lakukan tugas-tugas berikut atas nama Anda:

- Mengatur direktori berbasis Samba dalam VPC.
- Membuat akun administrator direktori dengan nama pengguna Administrator dan kata sandi yang ditentukan. Anda menggunakan akun ini untuk mengelola direktori.

Important

Pastikan untuk menyimpan kata sandi ini. Directory Service tidak menyimpan kata sandi ini, dan tidak dapat diambil. Namun, Anda dapat mengatur ulang kata sandi dari Directory Service konsol atau dengan menggunakan [ResetUserPasswordAPI](#).

- Membuat grup keamanan untuk pengontrol direktori.
- Membuat akun dengan nama AWSAdminD-**xxxxxxxx** yang memiliki hak istimewa admin domain. Akun ini digunakan oleh Directory Service untuk melakukan operasi otomatis untuk operasi pemeliharaan direktori, seperti mengambil snapshot direktori dan transfer peran FSMO. Kredensial untuk akun ini disimpan dengan aman oleh Directory Service.
- Secara otomatis membuat dan mengasosiasikan antarmuka jaringan elastis (ENI) dengan masing-masing pengendali domain Anda. Masing-masing ENIs penting untuk konektivitas antara VPC dan pengontrol Directory Service domain Anda dan tidak boleh dihapus. Anda dapat mengidentifikasi semua antarmuka jaringan yang dicadangkan untuk digunakan Directory Service dengan deskripsi: "AWS menciptakan antarmuka jaringan untuk direktori-id direktori". Untuk informasi selengkapnya, lihat [Antarmuka Jaringan Elastis](#) di Panduan EC2 Pengguna Amazon. Server DNS default dari

Direktori Aktif Microsoft AD yang AWS Dikelola adalah server DNS VPC di Classless Inter-Domain Routing (CIDR) +2. Untuk informasi selengkapnya, lihat [Server DNS](#) Amazon di Panduan Pengguna Amazon VPC.

 Note

Pengendali domain di-deploy di dua Availability Zone di suatu Region secara default dan terhubung ke Amazon Virtual Private Cloud (VPC) Anda. Backup secara otomatis diambil sekali per hari, dan volume Amazon Elastic Block Store (EBS) dienkripsi untuk memastikan bahwa data diamankan saat istirahat. Pengendali domain yang gagal secara otomatis diganti di Availability Zone yang sama menggunakan alamat IP yang sama, dan pemulihan bencana penuh dapat dilakukan dengan menggunakan backup terbaru.

Praktik terbaik untuk Simple AD

Berikut adalah beberapa saran dan panduan yang harus Anda pertimbangkan untuk menghindari masalah dan mendapatkan hasil maksimal dari Simple AD.

Menyiapkan: Prasyarat

Pertimbangkan panduan ini sebelum membuat direktori Anda.

Verifikasikan Anda memiliki jenis direktori yang tepat

Directory Service menyediakan berbagai cara untuk digunakan Microsoft Active Directory dengan AWS layanan lain. Anda dapat memilih directory service dengan fitur yang Anda butuhkan dengan biaya yang sesuai dengan anggaran Anda:

- AWS Directory Service untuk Microsoft Active Directory adalah pengelola kaya fitur yang Microsoft Active Directory dihosting di cloud. AWS AWS Microsoft AD yang dikelola adalah pilihan terbaik Anda jika Anda memiliki lebih dari 5.000 pengguna dan memerlukan hubungan kepercayaan yang disiapkan antara direktori yang AWS dihosting dan direktori lokal Anda.
- AD Connector cukup menghubungkan Active Directory lokal Anda yang ada. AWS AD Connector adalah pilihan terbaik Anda saat Anda ingin menggunakan direktori on-premise Anda yang sudah ada dengan layanan AWS .

- Simple AD adalah direktori berskala rendah dan berbiaya rendah dengan kompatibilitas Active Directory dasar. Ini mendukung 5.000 atau lebih sedikit pengguna, aplikasi yang kompatibel dengan Samba 4, dan kompatibilitas LDAP untuk aplikasi sadar LDAP.

Untuk perbandingan Directory Service opsi yang lebih rinci, lihat [Mana yang harus dipilih](#).

Pastikan instans VPCs dan instans Anda dikonfigurasi dengan benar

Untuk terhubung ke, mengelola, dan menggunakan direktori Anda, Anda harus mengonfigurasi dengan benar VPCs bahwa direktori terkait. Lihat [Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS](#), [Prasyarat AD Connector](#), atau [Prasyarat Simple AD](#) untuk informasi tentang persyaratan keamanan dan jaringan VPC.

Jika Anda menambahkan instans ke domain Anda, pastikan bahwa Anda memiliki konektivitas dan akses jarak jauh ke instans Anda seperti yang dijelaskan di [Cara untuk bergabung dengan instans Amazon EC2 ke AWS Microsoft AD yang Dikelola](#).

Ketahui batasan Anda

Pelajari tentang berbagai batasan untuk jenis direktori spesifik Anda. Penyimpanan yang tersedia dan ukuran agregat objek Anda adalah satu-satunya keterbatasan terkait jumlah objek yang dapat Anda simpan dalam direktori Anda. Lihat [AWS Kuota Microsoft AD yang dikelola](#), [Kuota AD Connector](#), atau [Kuota Simple AD](#) untuk detail tentang direktori pilihan Anda.

Pahami konfigurasi dan gunakan grup AWS keamanan direktori Anda

AWS membuat [grup keamanan](#) dan melampirkannya ke [antarmuka jaringan elastis](#) pengontrol domain direktori Anda. AWS mengkonfigurasi grup keamanan untuk memblokir lalu lintas yang tidak perlu ke direktori dan memungkinkan lalu lintas yang diperlukan.

Memodifikasi grup keamanan direktori

Anda dapat memodifikasi grup keamanan untuk direktori Anda, tetapi hanya melakukannya jika Anda sepenuhnya memahami pemfilteran grup keamanan. Untuk informasi selengkapnya, lihat [Grup Keamanan Amazon EC2 untuk instans Linux](#) di Panduan Pengguna Amazon EC2. Perubahan yang tidak tepat dapat mengganggu komunikasi dengan komputer dan instans yang dituju. AWS merekomendasikan untuk tidak membuka port tambahan ke direktori Anda karena ini mengurangi keamanan. Tinjau [Model Tanggung Jawab AWS Bersama](#) sebelum melakukan perubahan.

 Warning

Secara teknis dimungkinkan bagi Anda untuk mengaitkan grup keamanan direktori dengan instans EC2 lain yang Anda buat. Namun, AWS merekomendasikan untuk tidak melakukan praktik ini. AWS mungkin memiliki alasan untuk memodifikasi grup keamanan tanpa pemberitahuan untuk mengatasi kebutuhan fungsional atau keamanan direktori terkelola. Perubahan tersebut mempengaruhi setiap instans yang Anda asosiasikan dengan grup keamanan direktori dan dapat mengganggu operasi instans terkait. Selain itu, mengaitkan grup keamanan direktori dengan instans EC2 Anda dapat menciptakan risiko keamanan potensial untuk instans EC2 Anda.

Gunakan Microsoft AD yang AWS Dikelola jika diperlukan kepercayaan

Simple AD tidak mendukung hubungan kepercayaan. Jika Anda perlu membangun kepercayaan antara Directory Service direktori Anda dan direktori lain, Anda harus menggunakan AWS Directory Service untuk Microsoft Active Directory.

Pengaturan: Membuat direktori Anda

Berikut adalah beberapa saran untuk dipertimbangkan saat Anda membuat direktori Anda.

Ingat ID dan kata sandi administrator Anda

Saat mengatur direktori Anda, Anda memberikan kata sandi untuk akun administrator. ID akun tersebut adalah Administrator untuk Simple AD. Ingat kata sandi yang Anda buat untuk akun ini; jika tidak, Anda tidak akan dapat menambahkan objek ke direktori Anda.

Memahami batasan nama pengguna untuk AWS aplikasi

Directory Service memberikan dukungan untuk sebagian besar format karakter yang dapat digunakan dalam pembangunan nama pengguna. Namun, ada batasan karakter yang diberlakukan pada nama pengguna yang akan digunakan untuk masuk ke AWS aplikasi, seperti, WorkDocs Amazon WorkSpaces WorkMail, atau Quick. Pembatasan ini mengharuskan karakter berikut tidak digunakan:

- Spasi
- Karakter multibyte
- !"#\$%&'()*+,-./:;<=>?@[\\]^`{|}~

 Note

Simbol @ diperbolehkan selama itu mendahului akhiran UPN.

Memprogram aplikasi Anda

Sebelum memprogram aplikasi Anda, pertimbangkan hal berikut:

Menggunakan layanan locator Windows DC

Saat mengembangkan aplikasi, gunakan layanan pencari lokasi Windows DC atau gunakan layanan Dynamic DNS (DDNS) dari AWS Microsoft AD yang Dikelola untuk menemukan pengontrol domain (). DCs Jangan hard code aplikasi dengan alamat DC. Layanan locator DC membantu memastikan beban direktori didistribusikan dan memungkinkan Anda untuk mengambil keuntungan dari penskalaan horizontal dengan menambahkan pengendali domain untuk deployment Anda. Jika Anda mengikat aplikasi Anda ke DC tetap dan DC mengalami penambalan atau pemulihan, aplikasi Anda akan kehilangan akses ke DC alih-alih menggunakan salah satu yang tersisa. DCs Selain itu, hard coding DC dapat mengakibatkan hot spotting pada DC tunggal. Pada kasus yang parah, hot spotting dapat menyebabkan DC Anda menjadi tidak responsif. Kasus seperti itu juga dapat menyebabkan otomatisasi AWS direktori menandai direktori sebagai terganggu dan dapat memicu proses pemulihan yang menggantikan DC yang tidak responsif.

Muat tes sebelum diluncurkan ke produksi

Pastikan untuk melakukan pengujian laboratorium dengan aplikasi dan permintaan yang mewakili beban kerja produksi Anda untuk mengonfirmasi bahwa direktori menskalakan ke beban aplikasi Anda. Jika Anda memerlukan kapasitas tambahan, Anda harus menggunakan Directory Service Microsoft Active Directory, yang memungkinkan Anda menambahkan pengontrol domain untuk kinerja tinggi. Untuk informasi selengkapnya, lihat [Menerapkan pengontrol domain tambahan untuk AWS Microsoft AD yang Dikelola](#).

Gunakan kueri LDAP yang efisien

Kueri LDAP luas ke pengendali domain pada ribuan objek dapat mengkonsumsi siklus CPU yang signifikan dalam DC tunggal, mengakibatkan hot spotting. Hal ini dapat mempengaruhi aplikasi yang berbagi DC yang sama selama kueri.

Memelihara direktori Simple AD

Anda dapat menggunakan Konsol Manajemen AWS untuk mempertahankan Simple AD Anda dan menyelesaikan tugas day-to-day administratif. Cara Anda dapat mempertahankan Simple AD Anda meliputi:

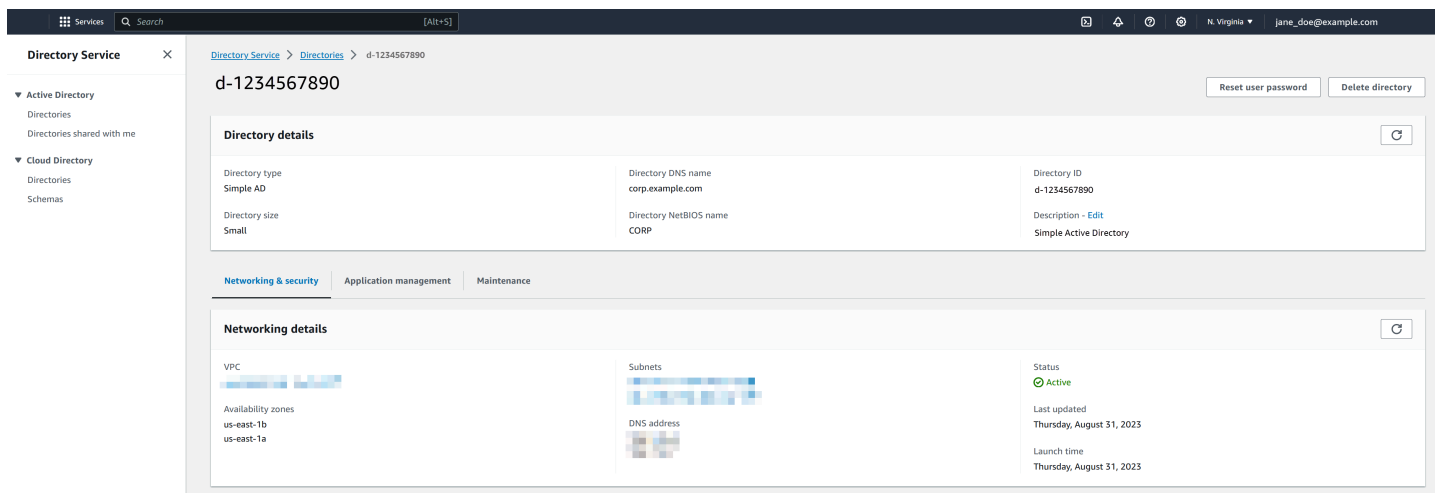
- [Lihat detail tentang Simple AD Anda](#) seperti nama DNS, ID Direktori, dan status direktori.
- [Perbarui alamat DNS untuk Simple AD Anda](#).
- [Kembalikan Simple AD Anda dengan snapshot](#). Anda juga dapat membuat snapshot dan menghapus snapshot.
- [Hapus Simple AD Anda](#) saat tidak lagi diperlukan.

Melihat informasi direktori Simple AD

Untuk melihat informasi direktori terperinci.

1. Di panel navigasi [Konsol AWS Directory Service](#), di bawah Direktori Aktif, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda. Informasi tentang direktori ditampilkan dalam halaman Detail direktori.

Untuk informasi selengkapnya tentang bidang Status, lihat [Memahami status direktori Simple AD Anda](#).



Memperbarui jenis jaringan direktori

Anda dapat memperbarui jenis jaringan Directory Service direktori Anda dari IPv4 ke Dual-stack (IPv4 dan IPv6). Memperbarui jenis jaringan untuk menyertakan alamat IPv6 IP menyediakan ruang alamat yang lebih besar daripada IPv4. IPv4 dan IPv6 komunikasi independen satu sama lain.

Untuk detailnya, lihat [Bandingkan IPv4 dan IPv6](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Important

Ini adalah operasi satu arah yang tidak dapat dibalik. Uji di lingkungan non-produksi terlebih dahulu.

Prasyarat

Sebelum memperbarui jenis jaringan direktori Anda, pastikan persyaratan berikut terpenuhi:

- VPC Anda harus dikonfigurasi dengan rentang IPv6 CIDR. Untuk detailnya, lihat [IPv6 dukungan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.
- Anda memiliki akses administratif ke Konsol Manajemen AWS.
- Direktori Anda harus dalam status Aktif.
- Anda memiliki izin IAM yang sesuai untuk mengubah Directory Service pengaturan.

Untuk memperbarui jenis jaringan direktori

Untuk memperbarui direktori Anda ke jaringan dual-stack

Note

Jika direktori Anda direplikasi di beberapa wilayah, lakukan pembaruan ini di setiap wilayah.

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pilih direktori target.
3. Buka tab Jaringan & Keamanan.

4. Pilih Tambahkan IPv6 dukungan. Opsi ini hanya tersedia untuk direktori IPv4 -only.

IPv6 hanya direktori yang tidak didukung.

5. Tinjau informasi pembaruan dan detail harga.
6. Pilih Tambah untuk mengonfirmasi pembaruan.

Setelah memulai pembaruan, status direktori berubah menjadi Memperbarui selama proses pembaruan. Pembaruan biasanya membutuhkan waktu 15-30 menit untuk diselesaikan. Setelah selesai, status direktori kembali ke Aktif.

Mengkonfigurasi server DNS untuk Simple AD

Anda dapat mengonfigurasi DNS untuk Simple AD dengan dua cara tergantung pada arsitektur dan persyaratan jaringan Anda.

Menggunakan Simple AD sebagai DNS Utama

Konfigurasi komputer klien Anda untuk menggunakan alamat IP server DNS Simple AD sebagai resolver DNS utama mereka. Simple AD meneruskan permintaan DNS ke alamat IP server DNS yang disediakan Amazon untuk VPC Amazon Anda. Server DNS ini akan menyelesaikan nama yang dikonfigurasi di zona host pribadi Amazon Route 53 Anda. Dengan mengarahkan komputer on-premise ke Simple AD Anda, Anda sekarang dapat menyelesaikan permintaan DNS ke zona yang dihosting pribadi. Untuk informasi selengkapnya tentang Route 53, lihat [Apa itu Route 53](#).

Selama pembuatan Simple AD, layanan melakukan uji jangkauan ke amazon.com untuk menentukan resolver DNS mana yang akan digunakan:

- Resolver DNS VPC Pelanggan (ETH1) - Dipilih saat amazon.com dapat dijangkau dari resolver VPC pelanggan. Opsi ini memungkinkan Route 53 zona host pribadi dan aturan firewall Resolver.
- Amazon Internal Resolver (ETH0) - Dipilih ketika amazon.com tidak dapat dijangkau dari pelanggan VPC DNS Resolver (). ETH1 Integrasi Route 53, zona yang dihosting pribadi, dan aturan firewall Resolver tidak akan berfungsi dengan opsi ini.

Important

Pemilihan DNS resolver terjadi secara otomatis selama pembuatan Simple AD dan tidak dapat dimodifikasi sesudahnya. Kami menyarankan Anda memastikan amazon.com dapat

diselesaikan di VPC Anda sebelum membuat Simple AD untuk mengaktifkan integrasi Route 53.

Menggunakan Route 53 sebagai DNS Utama

Anda juga dapat menggunakan Route 53 sebagai layanan DNS utama Anda:

- Konfigurasi komputer klien Anda untuk menggunakan alamat IP Route 53 Resolver sebagai resolver DNS utama mereka
- Buat aturan Resolver Route 53 untuk meneruskan hanya kueri nama domain (FQDN) domain yang memenuhi syarat secara kondisional ke Simple AD
- Pendekatan ini mempertahankan Route 53 sebagai sumber DNS otoritatif, dengan Simple AD hanya menangani kueri khusus domain

Perhatikan bahwa untuk mengaktifkan Simple AD untuk menanggapi permintaan DNS eksternal, access control list (ACL) jaringan untuk VPC yang berisi Simple AD Anda harus dikonfigurasi untuk mengizinkan lalu lintas dari luar VPC.

- Jika Anda tidak menggunakan Route 53 zona yang di-hosting pribadi, permintaan DNS Anda akan diteruskan ke server DNS publik.
- Jika Anda menggunakan server DNS khusus yang berada di luar VPC Anda dan ingin menggunakan DNS pribadi, Anda harus mengkonfigurasi ulang untuk menggunakan server DNS khusus pada EC2 instance dalam VPC Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang di-hosting pribadi](#).
- Jika Anda ingin Simple AD untuk menyelesaikan nama menggunakan kedua server DNS dalam VPC Anda dan server DNS pribadi di luar VPC Anda, Anda dapat melakukannya menggunakan set opsi DHCP. Untuk contoh terperinci, lihat [artikel ini](#).
- [Mengintegrasikan resolusi Directory Service' DNS s Anda](#) dengan. Amazon Route 53 Resolver

Note

Pembaruan dinamis DNS tidak didukung di domain Simple AD. Sebagai gantinya Anda dapat membuat perubahan secara langsung dengan menghubungkan ke direktori Anda menggunakan Pengelola DNS pada instans yang digabungkan ke domain Anda.

Memulihkan Simple AD Anda dengan snapshot

AWS Directory Service menyediakan kemampuan untuk mengambil snapshot manual data untuk direktori Simple AD Anda. Snapshot ini dapat digunakan untuk melakukan point-in-time pemulihan untuk direktori Anda. Anda tidak dapat mengambil snapshot dari direktori AD Connector.

Topik

- [Membuat snapshot dari direktori Anda](#)
- [Memulihkan direktori Anda dari snapshot](#)
- [Menghapus snapshot](#)

Membuat snapshot dari direktori Anda

Snapshot dapat digunakan untuk memulihkan direktori Anda ke apa itu pada titik waktu yang snapshot diambil. Untuk membuat snapshot manual dari direktori Anda, lakukan langkah-langkah berikut.

Note

Anda dibatasi hingga 5 snapshot manual untuk setiap direktori. Jika Anda telah mencapai batas ini, Anda harus menghapus salah satu snapshot manual yang ada sebelum Anda dapat membuat yang lain.

Untuk membuat snapshot manual

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih Tindakan, dan kemudian pilih Membuat snapshot.
5. Pada kotak dialog Membuat snapshot direktori, berikan nama untuk snapshot, jika diinginkan. Ketika siap, pilih Buat.

Tergantung pada ukuran direktori Anda, mungkin diperlukan beberapa menit untuk membuat snapshot. Ketika snapshot siap, nilai Status akan berubah menjadi Completed.

Memulihkan direktori Anda dari snapshot

Memulihkan direktori dari snapshot setara dengan memindahkan direktori kembali ke waktu dulu. Direktori snapshot unik untuk direktori tempat mereka dibuat. Snapshot hanya dapat dipulihkan ke direktori dari mana ia dibuat. Selain itu, usia maksimum yang didukung dari snapshot manual adalah 180 hari. Untuk informasi selengkapnya, lihat [Masa simpan yang berguna dari backup keadaan sistem Direktori Aktif](#) di situs web Microsoft.

Warning

Kami rekomendasikan Anda menghubungi [Pusat AWS Dukungan](#) sebelum pemulihan snapshot apa pun; kami mungkin dapat membantu Anda menghindari kebutuhan untuk melakukan pemulihan snapshot. Setiap pemulihan dari snapshot dapat mengakibatkan kehilangan data karena mereka adalah titik waktu. Penting Anda memahami bahwa semua server DNS DCs dan yang terkait dengan direktori akan offline sampai operasi pemulihan selesai.

Untuk memulihkan direktori Anda dari snapshot, lakukan langkah-langkah berikut.

Untuk memulihkan direktori dari snapshot

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih snapshot dalam daftar, pilih Tindakan, dan kemudian pilih Memulihkan snapshot.
5. Tinjau informasi di kotak dialog Memulihkan snapshot direktori, dan pilih Pemulihan.

Untuk direktori Simple AD, diperlukan beberapa menit untuk direktori dipulihkan. Ketika berhasil dipulihkan, nilai Status direktori berubah menjadi *Active*. Setiap perubahan yang dibuat ke direktori setelah tanggal snapshot akan ditimpa.

Menghapus snapshot

Untuk menghapus snapshot

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.

2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih Tindakan, dan kemudian pilih Hapus snapshot.
5. Verifikasi bahwa Anda ingin menghapus snapshot tersebut, lalu pilih Hapus.

Menghapus Simple AD

Ketika Simple AD dihapus, semua data direktori dan snapshot dihapus dan tidak dapat dipulihkan. Setelah direktori dihapus, semua instans yang bergabung ke direktori tetap utuh. Anda tidak dapat, bagaimanapun, menggunakan kredensial direktori Anda untuk masuk ke instans ini. Anda harus log in ke instans ini dengan akun pengguna yang lokal untuk instans.

Ketika direktori Microsoft AD, Simple AD, atau hybrid AWS terkelola dihapus, semua data direktori dan snapshot dihapus dan tidak dapat dipulihkan. Setelah direktori dihapus, semua instans yang bergabung ke direktori tetap utuh. Anda tidak dapat, bagaimanapun, menggunakan kredensial direktori Anda untuk masuk ke instans ini. Anda harus log in ke instans ini dengan akun pengguna yang lokal untuk instans.

Saat Konektor AD dihapus, direktori lokal Anda tetap utuh. Semua instans yang bergabung ke direktori juga tetap utuh dan tetap bergabung ke direktori on-premise Anda. Anda masih bisa menggunakan kredensial direktori Anda untuk masuk ke instans ini.

Untuk menghapus direktori

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori. Pastikan Anda berada di AWS Region tempat Active Directory Anda digunakan. Untuk informasi selengkapnya, lihat [Memilih Wilayah](#).
2. Pastikan tidak ada AWS aplikasi yang diaktifkan untuk direktori yang ingin Anda hapus. AWS Aplikasi yang diaktifkan akan mencegah Anda menghapus iklan Microsoft AWS Terkelola atau Simple AD Anda.
 - a. Pada halaman Direktori, pilih ID direktori Anda.
 - b. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi. Di bagian AWS aplikasi & layanan, Anda melihat AWS aplikasi mana yang diaktifkan untuk direktori Anda.
 - Nonaktifkan Konsol Manajemen AWS akses. Untuk informasi selengkapnya, lihat [Menonaktifkan akses Konsol Manajemen AWS](#).

- Untuk menonaktifkan Amazon WorkSpaces, Anda harus membatalkan pendaftaran layanan dari direktori di konsol. WorkSpaces Untuk informasi selengkapnya, lihat [Menghapus direktori](#) di Panduan WorkSpaces Administrasi Amazon.
- Untuk menonaktifkan WorkDocs, Anda harus menghapus WorkDocs situs di WorkDocs konsol. Untuk informasi selengkapnya, lihat [Menghapus situs](#) di Panduan WorkDocs Administrasi Amazon.
- Untuk menonaktifkan Amazon WorkMail, Anda harus menghapus WorkMail organisasi Amazon di WorkMail konsol Amazon. Untuk informasi selengkapnya, lihat [Menghapus organisasi](#) di Panduan WorkMail Administrator Amazon.
- Untuk menonaktifkan Amazon FSx untuk Windows File Server, Anda harus menghapus sistem FSx file Amazon dari domain. Untuk informasi selengkapnya, lihat [Bekerja dengan Active Directory FSx untuk Windows File Server](#) di Amazon FSx untuk Windows File Server User Guide.
- Untuk menonaktifkan Amazon Relational Database Service, Anda harus menghapus instans Amazon RDS dari domain. Untuk informasi selengkapnya, lihat [Mengelola instans DB dalam domain](#) dalam Panduan Pengguna Amazon RDS.
- Untuk menonaktifkan AWS Client VPN Layanan, Anda harus menghapus layanan direktori dari Endpoint Client VPN. Untuk informasi selengkapnya, lihat [Bekerja dengan Client VPN](#) di Panduan AWS Client VPN Administrator.
- Untuk menonaktifkan Amazon Connect, Anda harus menghapus Instans Amazon Connect. Untuk informasi selengkapnya, lihat [Menghapus instans Amazon Connect](#) di Panduan Administrasi Amazon Connect.
- Untuk menonaktifkan Amazon Quick, Anda harus berhenti berlangganan Amazon Quick. Untuk informasi selengkapnya, lihat [Menutup Amazon Quick akun Anda](#) di Panduan Pengguna Cepat Amazon.

 Note

Jika Anda menggunakan AWS IAM Identity Center dan sebelumnya telah menghubungkannya ke direktori Microsoft AD AWS Terkelola yang ingin Anda hapus, Anda harus terlebih dahulu mengubah sumber identitas sebelum dapat menghapusnya. Untuk informasi selengkapnya, lihat [Mengubah sumber identitas Anda](#) di Panduan Pengguna Pusat Identitas IAM.

3. Di panel navigasi, pilih Direktori.

4. Pilih hanya direktori yang akan dihapus dan klik Hapus. Ini akan memerlukan beberapa menit agar direktori dihapus. Ketika direktori telah dihapus, itu akan dihapus dari daftar direktori Anda.

Amankan direktori Simple AD Anda

Bagian ini menjelaskan pertimbangan untuk mengamankan lingkungan Simple AD Anda.

Topik

- [Cara mengatur ulang kata sandi akun krbtgt AD Sederhana](#)

Cara mengatur ulang kata sandi akun krbtgt AD Sederhana

Akun krbtgt memainkan peran penting dalam pertukaran tiket Kerberos. Akun krbtgt adalah akun khusus yang digunakan untuk enkripsi tiket pemberian tiket Kerberos (TGT), dan memainkan peran penting dalam keamanan protokol otentikasi Kerberos. Di Samba AD, krbtgt direpresentasikan sebagai akun pengguna (dinonaktifkan). Kata sandi untuk akun ini dibuat secara acak pada saat domain disediakan. Akses ke rahasia ini dapat mengakibatkan kompromi domain total yang tidak terdeteksi karena tiket Kerberos baru dapat dicetak tanpa audit. Untuk informasi selengkapnya, lihat [dokumentasi Samba](#).

Disarankan untuk mengubah kata sandi ini secara teratur setiap 90 hari. Anda dapat mengatur ulang kata sandi akun krbtgt dari Windows instans Amazon EC2 yang digabungkan ke Simple AD Anda.

Note

AWS Simple AD didukung oleh Samba-ad. Samba-ad tidak menyimpan hash N-1 untuk akun krbtgt. Oleh karena itu, ketika kata sandi akun krbtgt diatur ulang, klien Kerberos akan diminta untuk menegosiasikan Tiket Pemberian Tiket (TGT) baru selama permintaan Tiket Layanan (ST) berikutnya. Untuk meminimalkan potensi gangguan layanan, Anda harus menjadwalkan pengaturan ulang kata sandi akun krbtgt di luar jam kerja. Pendekatan ini mengurangi dampak pada operasi yang sedang berlangsung dan memastikan kelancaran kesinambungan otentikasi.

Prosedur berikut menunjukkan bagaimana Anda dapat mengatur ulang kata sandi akun krbtgt dari instans Amazon EC2. Windows

Prasyarat

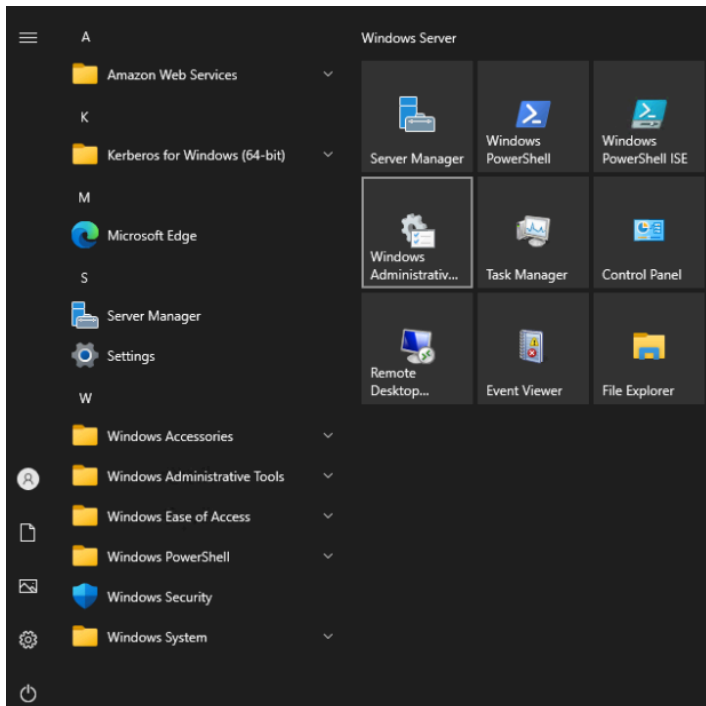
- Sebelum Anda dapat memulai prosedur ini, selesaikan yang berikut ini:
 - Anda memiliki domain yang bergabung dengan instans EC2 ke direktori Simple AD Anda.
 - Untuk informasi selengkapnya tentang cara menggabungkan Windows instans EC2 ke Simple AD, lihat [the section called “Bergabung dengan instance Windows”](#).
 - Anda memiliki kredensial administrator direktori Simple AD. Anda akan masuk sebagai administrator direktori Simple AD untuk prosedur ini.

Note

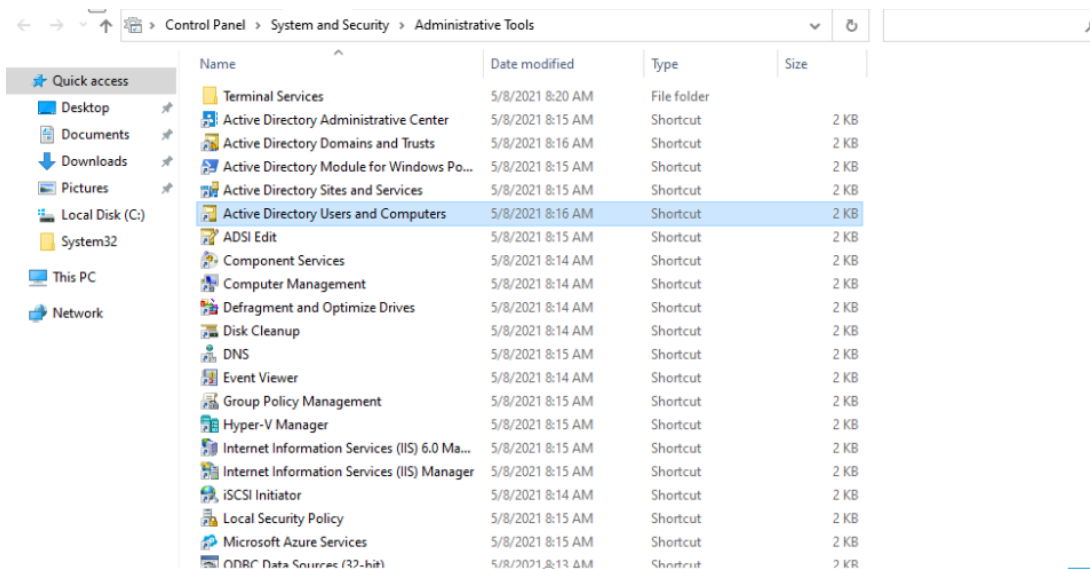
Beberapa Layanan AWS seperti Amazon WorkDocs dan Amazon WorkSpaces, akan membuat Simple AD atas nama Anda.

Reset Simple AD kata sandi akun krbtgt

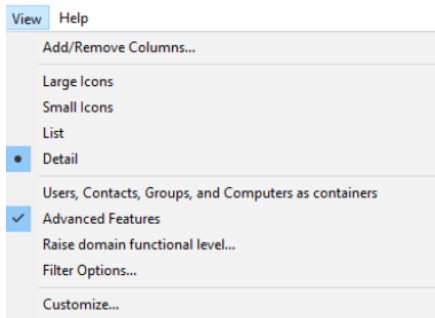
1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Di konsol Amazon EC2, pilih Instans dan pilih instance Server. Windows Kemudian pilih Connect.
3. Di halaman Connect to instance, pilih klien RDP.
4. Di kotak dialog Keamanan Windows, salin kredensial administrator lokal Anda untuk komputer Windows Server untuk masuk. Nama pengguna dapat dalam format berikut: NetBIOS-Name \administrator atau DNS-Name \administrator. Misalnya, corp\administrator akan menjadi nama pengguna jika Anda mengikuti prosedur di [the section called “Buat Simple AD Anda”](#).
5. Setelah masuk ke komputer Windows Server, buka Windows Administrative Tools dari menu Start dengan memilih folder Windows Administrative Tools.



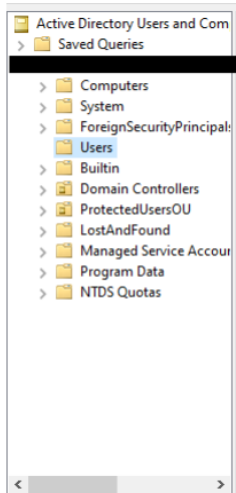
6. Di dashboard Windows Administrative Tools, buka Active Directory Users and Computers dengan memilih Active Directory User and Computers.



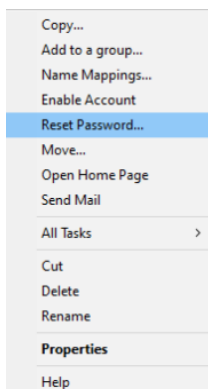
7. Di jendela Active Directory Users and Computers, pilih View dan kemudian pilih Enable Advanced Features.



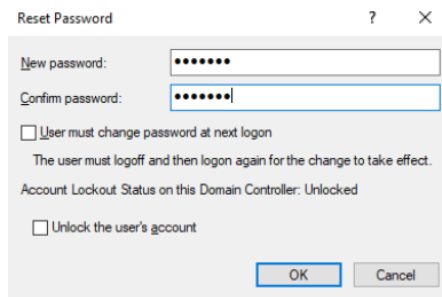
8. Di jendela Active Directory Users and Computers, pilih Users dari panel kiri.



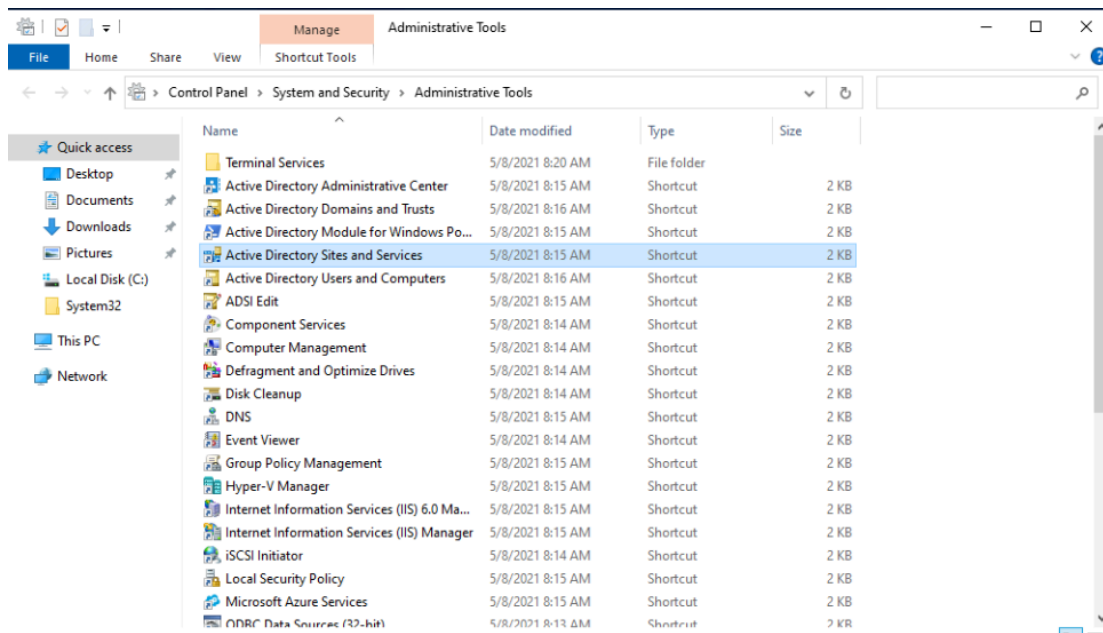
9. Temukan pengguna bernama krbtgt, klik kanan padanya dan pilih Reset Password.



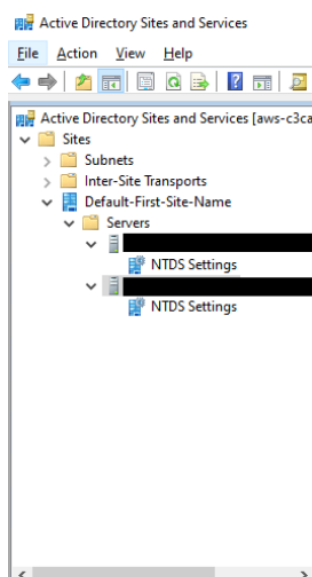
10. Di jendela baru, masukkan kata sandi baru, masukkan lagi, lalu pilih OK untuk mengatur ulang kata sandi akun krbtgt.



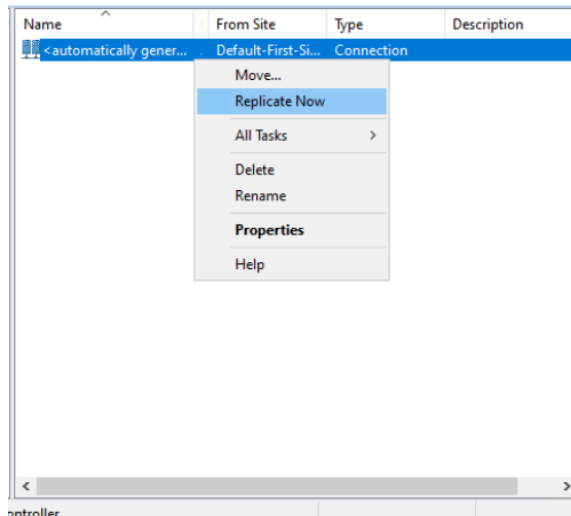
11. Di dasbor Alat Windows Administratif, pilih Situs dan Layanan Direktori Aktif.



12. Di jendela Active Directory Sites and Services, perluas Situs, Default-First-Site-Name, dan Server.



13. Di jendela Pengaturan NTDS, klik kanan pada server dan pilih Replicate Now.



14. Ulangi langkah 13 - 14 untuk server Anda yang lain.

Memantau direktori Simple AD

Anda bisa mendapatkan hasil maksimal dari Simple AD Anda dengan mempelajari lebih lanjut tentang berbagai status Simple AD dan apa artinya untuk Simple AD Anda. Anda juga dapat menggunakan AWS layanan seperti Amazon Simple Notification Service untuk memantau Simple AD Anda. Amazon Simple Notification Service dapat mengirimkan pemberitahuan status direktori Simple AD Anda.

Tugas untuk memantau Simple AD Anda

- [Memahami status direktori Simple AD Anda](#)
- [Mengaktifkan pemberitahuan status direktori Simple AD dengan Amazon Simple Notification Service](#)

Memahami status direktori Simple AD Anda

Berikut ini adalah berbagai status untuk direktori.

Aktif

Direktori beroperasi secara normal. Tidak ada masalah yang terdeteksi oleh Directory Service untuk direktori Anda.

Creating

Direktori saat ini sedang dibuat. Pembuatan direktori biasanya memakan waktu antara 20 sampai 45 menit tetapi dapat bervariasi tergantung pada beban sistem.

Dihapus

Direktori telah dihapus. Semua sumber daya untuk direktori telah dirilis. Setelah direktori memasuki keadaan ini, direktori tidak dapat dipulihkan.

Deleting

Direktori saat ini sedang dihapus. Direktori akan tetap dalam keadaan ini sampai benar-benar dihapus. Setelah direktori memasuki keadaan ini, operasi hapus tidak dapat dibatalkan, dan direktori tidak dapat dipulihkan.

Gagal

Direktori tidak dapat dibuat. Harap hapus direktori ini. Jika masalah ini berlanjut, hubungi [Pusat AWS Dukungan](#).

Terganggu

Direktori berjalan dalam keadaan terdegradasi. Satu atau lebih masalah telah terdeteksi, dan tidak semua operasi direktori dapat bekerja pada kapasitas operasional penuh. Terdapat banyak potensi alasan untuk keadaan direktori seperti ini. Ini termasuk aktivitas pemeliharaan operasional normal seperti patching atau rotasi instans EC2, hot spotting sementara oleh aplikasi pada salah satu pengendali domain Anda, atau perubahan yang Anda buat ke jaringan Anda yang secara tidak sengaja mengganggu komunikasi direktori. Direktori Anda dapat memiliki status terganggu jika Anda mengubah pengaturan yang diuraikan. [Prasyarat Simple AD](#) Untuk informasi selengkapnya, lihat salah satu dari [Pemecahan Masalah AWS Microsoft AD yang Dikelola](#), [Memecahkan masalah AD Connector](#), [Pemecahan masalah Simple AD](#). Untuk masalah terkait pemeliharaan normal, AWS selesaikan masalah ini dalam waktu 40 menit. Jika setelah meninjau topik pemecahan masalah, direktori Anda dalam keadaan Terganggu lebih dari 40 menit, kami merekomendasikan Anda untuk menghubungi [Pusat AWS Dukungan](#).

Important

Jangan memulihkan snapshot ketika direktori dalam keadaan Terganggu. Sangatlah jarang pemulihan snapshot diperlukan untuk mengatasi gangguan. Untuk informasi selengkapnya, lihat [Memulihkan iklan Microsoft AWS Terkelola Anda dengan snapshot](#).

Tidak bisa dioperasikan

Direktori tidak berfungsi. Semua titik akhir direktori telah melaporkan masalah.

Diminta

Permintaan untuk membuat direktori Anda sedang tertunda.

RestoreFailed

Memulihkan direktori dari snapshot gagal. Silakan coba lagi operasi pemulihan. Jika ini berlanjut, cobalah snapshot yang berbeda, atau hubungi [AWS Dukungan Pusat](#).

Memulihkan

Direktori saat ini sedang dipulihkan dari snapshot otomatis atau manual. Memulihkan dari snapshot biasanya memakan waktu beberapa menit, tergantung pada ukuran data direktori dalam snapshot.

Lihat informasi yang lebih lengkap di [Memecahkan masalah Pesan status direktori Simple AD](#).

Mengaktifkan pemberitahuan status direktori Simple AD dengan Amazon Simple Notification Service

Menggunakan Amazon Simple Notification Service (Amazon SNS), Anda dapat menerima pesan email atau teks (SMS) saat status direktori Anda berubah. Anda akan diberitahu jika direktori Anda berubah dari status Aktif ke status [Terganggu atau Tidak dapat dioperasikan](#). Anda juga menerima notifikasi ketika direktori kembali ke status Aktif.

Cara kerjanya

Amazon SNS menggunakan “topik” untuk mengumpulkan dan mendistribusikan pesan. Setiap topik memiliki satu atau lebih pelanggan yang menerima pesan yang telah diterbitkan untuk topik tersebut. Dengan menggunakan langkah-langkah di bawah ini, Anda dapat menambahkan Directory Service sebagai penerbit ke topik Amazon SNS. Saat Directory Service mendeteksi perubahan dalam status direktori Anda, ia menerbitkan pesan ke topik tersebut, yang kemudian dikirim ke pelanggan topik tersebut.

Anda dapat mengaitkan beberapa direktori sebagai penerbit ke satu topik. Anda juga dapat menambahkan pesan status direktori ke topik yang sebelumnya Anda buat di Amazon SNS. Anda memiliki kendali terperinci atas siapa yang dapat menerbitkan dan berlangganan topik. Untuk informasi lengkap tentang Amazon SNS, lihat [Apa yang Dimaksud dengan Amazon SNS?](#).

Untuk mengaktifkan olahpesan SNS untuk direktori Anda

1. Masuk ke Konsol Manajemen AWS dan buka [Directory Service konsol](#).
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih Tindakan, dan kemudian pilih Buat notifikasi.
5. Pada halaman Buat notifikasi, pilih Pilih jenis notifikasi, lalu pilih Buat notifikasi baru. Atau, jika Anda sudah memiliki topik SNS yang ada, Anda dapat memilih Mengasosiasikan topik SNS yang ada untuk mengirim pesan status dari direktori ini ke topik tersebut.

Note

Jika Anda memilih Buat notifikasi baru tetapi kemudian menggunakan nama topik yang sama untuk topik SNS yang sudah ada, Amazon SNS tidak membuat topik baru, tetapi hanya menambahkan informasi langganan baru ke topik yang ada.

Jika Anda memilih Mengasosiasikan topik SNS yang ada, Anda hanya akan dapat memilih topik SNS yang ada di Region yang sama dengan direktori.

6. Pilih Jenis penerima dan masukkan informasi kontak Penerima. Jika Anda memasukkan nomor telepon untuk SMS, gunakan angka saja. Jangan menyertakan tanda hubung, spasi, atau tanda kurung.
7. (Opsional) Berikan nama untuk topik Anda dan nama tampilan SNS. Nama tampilan adalah nama pendek hingga 10 karakter yang disertakan dalam semua pesan SMS dari topik ini. Bila menggunakan opsi SMS, nama tampilan diperlukan.

Note

Jika Anda masuk menggunakan pengguna IAM atau peran yang hanya memiliki kebijakan [DirectoryServiceFullAccess](#)terkelola, nama topik Anda harus dimulai dengan "DirectoryMonitoring". Jika Anda ingin menyesuaikan nama topik Anda lebih lanjut, Anda memerlukan hak istimewa tambahan untuk SNS.

8. Pilih Buat.

[Jika Anda ingin menunjuk pelanggan SNS tambahan, seperti alamat email tambahan, antrian Amazon SQS AWS Lambda atau, Anda dapat melakukan ini dari konsol Amazon SNS.](#)

Untuk menghapus pesan status direktori dari topik

1. Masuk ke Konsol Manajemen AWS dan buka [Directory Service konsol](#).
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih nama topik SNS dalam daftar, pilih Tindakan, dan kemudian pilih Hapus.
5. Pilih Hapus.

Ini akan menghapus direktori Anda sebagai penerbit untuk topik SNS yang dipilih. Jika Anda ingin menghapus seluruh topik, Anda dapat melakukan ini dari konsol [Amazon SNS](#).

 Note

Sebelum menghapus topik Amazon SNS menggunakan konsol SNS, Anda harus memastikan bahwa direktori tidak mengirim pesan status untuk topik tersebut.

Jika Anda menghapus topik Amazon SNS menggunakan konsol SNS, perubahan ini tidak akan segera tercermin dalam konsol Directory Service. Anda hanya akan diberitahu pada saat direktori menerbitkan notifikasi untuk topik yang dihapus, dalam hal ini Anda akan melihat status diperbarui pada tab Pemantauan direktori yang menunjukkan topik tidak dapat ditemukan.

Oleh karena itu, untuk menghindari kehilangan pesan status direktori penting, sebelum menghapus topik apa pun yang menerima pesan dari Directory Service, kaitkan direktori Anda dengan topik Amazon SNS yang berbeda.

Akses ke AWS aplikasi dan layanan dari Simple AD

Anda dapat memberikan akses ke pengguna Simple AD Anda untuk mengakses AWS aplikasi dan layanan. Beberapa AWS aplikasi dan layanan ini meliputi:

- Amazon WorkDocs
- Konsol Manajemen AWS
- Amazon WorkSpaces

Anda juga dapat menggunakan akses URLs dan sistem masuk tunggal dengan Simple AD Anda.

Topik

- [Kebijakan kompatibilitas aplikasi untuk Simple AD](#)
- [Mengaktifkan akses ke AWS aplikasi dan layanan untuk Simple AD Anda](#)
- [Mengaktifkan akses ke kredensial Konsol Manajemen AWS dengan Simple AD](#)
- [Membuat URL akses untuk Simple AD](#)
- [Mengaktifkan single sign-on](#)

Kebijakan kompatibilitas aplikasi untuk Simple AD

Simple AD merupakan implementasi dari Samba yang menyediakan banyak fitur dasar Direktori Aktif. Karena besarnya off-the-shelf aplikasi kustom dan komersial yang menggunakan Active Directory, AWS tidak dan tidak dapat melakukan verifikasi formal atau luas kompatibilitas aplikasi pihak ketiga dengan Simple AD. Meskipun AWS bekerja dengan pelanggan dalam upaya untuk mengatasi tantangan instalasi aplikasi potensial yang mungkin mereka hadapi, kami tidak dapat menjamin bahwa aplikasi apa pun atau akan terus kompatibel dengan Simple AD.

Aplikasi pihak ketiga berikut ini kompatibel dengan Simple AD:

- Microsoft Internet Information Services (IIS) pada platform berikut:
 - Windows Server 2003 R2
 - Windows Server 2008 R1
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
- Microsoft SQL Server:
 - SQL Server 2005 R2 (edisi Ekspres, Web, dan Standar)
 - SQL Server 2008 R2 (edisi Ekspres, Web, dan Standar)
 - SQL Server 2012 (edisi Ekspres, Web, dan Standar)
 - SQL Server 2014 (edisi Ekspres, Web, dan Standar)
- Microsoft SharePoint:
 - SharePoint Yayasan 2010
 - SharePoint Perusahaan 2010
 - SharePoint 2013 Perusahaan

Pelanggan dapat memilih untuk menggunakan AWS Directory Service untuk Microsoft Active Directory ([AWS Microsoft AD yang dikelola](#)) untuk tingkat kompatibilitas yang lebih tinggi berdasarkan Active Directory yang sebenarnya.

Mengaktifkan akses ke AWS aplikasi dan layanan untuk Simple AD Anda

Pengguna dapat mengotorisasi Simple AD untuk memberikan AWS aplikasi dan layanan, seperti Amazon WorkSpaces, akses ke Active Directory Anda. AWS Aplikasi dan layanan berikut dapat diaktifkan atau dinonaktifkan untuk bekerja dengan Simple AD.

AWS aplikasi/layanan	Informasi selengkapnya...
Amazon WorkDocs	Untuk informasi selengkapnya, lihat Panduan WorkDocs Administrasi Amazon
Amazon WorkMail	Untuk informasi selengkapnya, lihat Panduan WorkMail Administrator Amazon .
Amazon WorkSpaces	Anda dapat membuat Simple AD, AWS Managed Microsoft AD, atau AD Connector langsung dari WorkSpaces. Cukup luncurkan Pengaturan Advanced saat membuat Workspace Anda. Untuk informasi selengkapnya, lihat Panduan WorkSpaces Administrasi Amazon.
Konsol Manajemen AWS	Untuk informasi selengkapnya, lihat Mengaktifkan Konsol Manajemen AWS akses dengan kredensi Microsoft AD yang AWS Dikelola .

Setelah diaktifkan, Anda mengelola akses ke direktori Anda di konsol dari aplikasi atau layanan yang ingin Anda berikan akses ke direktori Anda. Untuk menemukan tautan AWS aplikasi dan layanan yang dijelaskan di atas di Directory Service konsol, lakukan langkah-langkah berikut.

Untuk menampilkan aplikasi dan layanan untuk direktori

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.

2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Tinjau daftar di bawah bagian aplikasi & layanan AWS .

Untuk informasi selengkapnya tentang cara mengotorisasi atau membatalkan otorisasi AWS aplikasi dan layanan yang digunakan Directory Service, lihat. [Otorisasi untuk AWS aplikasi dan layanan menggunakan Directory Service](#)

Mengaktifkan akses ke kredensial Konsol Manajemen AWS dengan Simple AD

Directory Service memungkinkan Anda untuk memberikan anggota direktori Anda akses ke Konsol Manajemen AWS. Secara default, anggota direktori Anda tidak memiliki akses ke AWS sumber daya apa pun. Anda menetapkan peran IAM ke anggota direktori Anda untuk memberi mereka akses ke berbagai AWS layanan dan sumber daya. IAM role menentukan layanan, sumber daya, dan tingkat akses yang dimiliki anggota direktori Anda.

Sebelum Anda dapat memberikan akses konsol ke anggota direktori Anda, direktori Anda harus memiliki URL akses. Untuk informasi selengkapnya tentang cara melihat detail direktori dan mendapatkan URL akses Anda, lihat [Melihat informasi direktori Microsoft AD yang AWS Dikelola](#). Untuk informasi selengkapnya tentang cara membuat URL akses, lihat [Membuat URL akses untuk Microsoft AD yang AWS Dikelola](#).

Untuk informasi selengkapnya tentang cara membuat dan menetapkan IAM role untuk anggota direktori Anda, lihat [Memberikan pengguna dan grup Microsoft AD AWS Terkelola akses ke AWS sumber daya dengan peran IAM](#).

Topik

- [Mengaktifkan akses Konsol Manajemen AWS](#)
- [Menonaktifkan akses Konsol Manajemen AWS](#)
- [Mengatur panjang sesi login](#)

Artikel Blog AWS Keamanan Terkait

- [Cara Mengakses Konsol Manajemen AWS Iklan Microsoft yang AWS Dikelola dan Kredensial Lokal Anda](#)

AWS re:Post Artikel Terkait

- [Bagaimana cara memberikan akses ke untuk pengguna Active Directory lokal? Konsol Manajemen AWS](#)

Mengaktifkan akses Konsol Manajemen AWS

Secara default, akses konsol tidak diaktifkan untuk direktori apapun. Untuk mengaktifkan akses konsol untuk pengguna dan grup direktori Anda, lakukan langkah-langkah berikut:

Untuk mengaktifkan akses konsol

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bawah bagian Konsol Manajemen AWS, pilih Aktifkan. Akses konsol sekarang diaktifkan untuk direktori Anda.

Important

Sebelum pengguna dapat masuk ke konsol dengan URL akses Anda, Anda harus terlebih dahulu menambahkan pengguna Anda ke peran IAM. Untuk informasi umum tentang menetapkan pengguna ke IAM role, lihat [Menetapkan pengguna atau grup ke peran IAM yang ada](#). Setelah IAM role telah ditetapkan, pengguna kemudian dapat mengakses konsol tersebut menggunakan URL akses Anda. Misalnya, jika URL akses direktori Anda adalah example-corp.awsapps.com, URL untuk mengakses konsol adalah. <https://example-corp.awsapps.com/console/>

Menonaktifkan akses Konsol Manajemen AWS

Untuk menonaktifkan akses konsol untuk pengguna dan grup direktori Anda, lakukan langkah-langkah berikut:

Untuk menonaktifkan akses konsol

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.

3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bawah bagian Konsol Manajemen AWS, pilih Menonaktifkan. Akses konsol sekarang dinonaktifkan untuk direktori Anda.
5. Jika setiap IAM role telah ditetapkan untuk pengguna atau grup dalam direktori, tombol Nonaktifkan mungkin tidak tersedia. Dalam kasus ini, Anda harus menghapus semua penetapan IAM role untuk direktori sebelum melanjutkan, termasuk tugas untuk pengguna atau grup dalam direktori Anda yang telah dihapus, yang akan ditampilkan sebagai Pengguna Dihapus atau Grup Dihapus.

Setelah semua penetapan IAM role dihapus, ulangi langkah-langkah di atas.

Mengatur panjang sesi login

Secara default, pengguna memiliki waktu 1 jam untuk menggunakan sesi mereka setelah berhasil masuk ke konsol tersebut sebelum mereka keluar. Setelah itu, pengguna harus masuk lagi untuk memulai sesi 1 jam berikutnya sebelum keluar lagi. Anda dapat menggunakan prosedur berikut untuk mengubah lama waktu hingga 12 jam per sesi.

Untuk mengatur lamanya sesi masuk

1. Pada panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bawah bagian Aplikasi & layanan AWS, pilih Konsol Manajemen AWS.
5. Di kotak dialog Kelola Akses ke AWS Sumber Daya, pilih Lanjutkan.
6. Di halaman Menetapkan pengguna dan grup ke IAM role, di bawah Atur lamanya sesi masuk, edit nilai bernomor, dan kemudian pilih Simpan.

Membuat URL akses untuk Simple AD

URL akses digunakan dengan AWS aplikasi dan layanan, seperti Amazon WorkDocs, untuk mencapai halaman login yang terkait dengan direktori Anda. URL harus unik secara global. Anda dapat membuat URL akses untuk direktori Anda dengan melakukan langkah-langkah berikut.

 Warning

Setelah Anda membuat URL akses aplikasi untuk direktori ini, itu tidak dapat diubah. Setelah URL akses dibuat, tidak dapat digunakan oleh orang lain. Jika Anda menghapus direktori Anda, URL akses juga dihapus dan kemudian dapat digunakan oleh akun lain.

Untuk membuat URL akses

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bagian URL akses aplikasi, jika URL akses belum ditetapkan ke direktori, tombol Buat ditampilkan. Masukkan alias direktori dan pilih Buat. Jika error Entitas Sudah Ada dikembalikan, alias direktori tertentu telah dialokasikan. Pilih alias lain dan ulangi prosedur ini.

URL akses Anda ditampilkan dalam format `<alias>.awsapps.com`.

Mengaktifkan single sign-on

AWS Directory Service memberikan kemampuan untuk memungkinkan pengguna Anda mengakses WorkDocs dari komputer yang bergabung ke direktori tanpa harus memasukkan kredensialnya secara terpisah.

Sebelum mengaktifkan sing-on tunggal, Anda perlu mengambil langkah tambahan agar peramban web pengguna dapat mendukung sign-on tunggal. Pengguna mungkin perlu memodifikasi pengaturan peramban web mereka untuk mengaktifkan sign-on tunggal.

 Note

Sign-on tunggal hanya bekerja bila digunakan pada komputer yang digabungkan ke direktori Directory Service. Ini tidak dapat digunakan pada komputer yang tidak bergabung ke direktori.

Jika direktori Anda adalah direktori AD Connector dan akun layanan AD Connector tidak memiliki izin untuk menambahkan atau menghapus atribut nama utama layanannya, maka untuk Langkah 5 dan 6 di bawah ini, Anda memiliki dua pilihan:

1. Anda dapat melanjutkan dan akan diminta untuk nama pengguna dan kata sandi untuk pengguna direktori yang memiliki izin ini untuk menambah atau menghapus atribut nama utama layanan pada akun layanan AD Connector. Kredensial ini hanya digunakan untuk mengaktifkan sign-on tunggal dan tidak disimpan oleh layanan. Izin akun layanan AD Connector tidak berubah.
2. Anda dapat mendelegasikan izin untuk mengizinkan akun layanan AD Connector menambah atau menghapus atribut nama utama layanan itu sendiri, Anda dapat menjalankan PowerShell perintah di bawah ini dari komputer yang bergabung dengan domain menggunakan akun yang memiliki izin untuk mengubah izin pada akun layanan AD Connector. Perintah di bawah ini akan memberikan akun layanan AD Connector kemampuan untuk menambah dan menghapus atribut nama utama layanan hanya untuk dirinya sendiri.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
  $RootDse.SchemaNamingContext -Filter { LDAPDisplayName -eq 'servicePrincipalName' } -
  Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
  $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
  Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
  'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
  'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Untuk mengaktifkan atau menonaktifkan sistem masuk tunggal dengan WorkDocs

1. Di panel navigasi [konsol AWS Directory Service](#), pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.

4. Di bagian URL akses aplikasi, pilih Aktifkan untuk mengaktifkan sistem masuk tunggal WorkDocs

Jika Anda tidak melihat tombol Aktifkan, Anda mungkin harus terlebih dahulu membuat URL Akses sebelum opsi ini akan ditampilkan. Untuk informasi selengkapnya tentang cara membuat URL akses, lihat [Membuat URL akses untuk Microsoft AD yang AWS Dikelola](#).

5. Di kotak dialog Aktifkan Sign-On Tunggal untuk direktori ini,, pilih Aktifkan. Sign-on tunggal diaktifkan untuk direktori.
6. Jika nanti Anda ingin menonaktifkan sistem masuk tunggal dengan WorkDocs, pilih Nonaktifkan, dan kemudian di kotak dialog Nonaktifkan Single Sign-On untuk direktori ini, pilih Nonaktifkan lagi.

Topik

- [Sign-on tunggal untuk IE dan Chrome](#)
- [Sign-on tunggal untuk Firefox](#)

Sign-on tunggal untuk IE dan Chrome

Untuk mengizinkan peramban Microsoft Internet Explorer (IE) dan Google Chrome untuk mendukung sign-on tunggal, tugas berikut harus dilakukan pada komputer klien:

- Tambahkan URL akses Anda (mis., <https://<alias>.awsapps.com>) ke daftar situs yang disetujui untuk sistem masuk tunggal.
- Aktifkan skrip aktif (JavaScript).
- Izinkan masuk otomatis.
- Aktifkan autentikasi terintegrasi.

Anda atau pengguna Anda dapat melakukan tugas-tugas ini secara manual, atau Anda dapat mengubah pengaturan ini menggunakan pengaturan Kebijakan Grup.

Topik

- [Pembaruan manual untuk sign-on tunggal pada Windows](#)
- [Pembaruan manual untuk sign-on tunggal pada OS X](#)
- [Pengaturan kebijakan grup untuk sign-on tunggal](#)

Pembaruan manual untuk sign-on tunggal pada Windows

Untuk mengaktifkan sign-on tunggal secara manual pada komputer Windows, lakukan langkah-langkah berikut pada komputer klien. Beberapa pengaturan ini mungkin sudah diatur dengan benar.

Cara mengaktifkan sign-on tunggal untuk Internet Explorer dan Chrome secara manual di Windows

1. Untuk membuka kotak dialog Properti internet, pilih menu Start, ketik Internet Options di kotak pencarian, lalu pilih Opsi Internet.
2. Tambahkan URL akses Anda ke daftar situs yang disetujui untuk sign-on tunggal dengan melakukan langkah-langkah berikut:
 - a. Di kotak dialog Properti internet, pilih tab Keamanan.
 - b. Pilih Intranet lokal dan pilih Situs.
 - c. Di kotak dialog Intranet lokal, pilih Advanced.
 - d. Tambahkan URL akses Anda ke daftar situs web dan pilih tutup.
 - e. Di dialog box Intranet lokal, pilih OK.
3. Untuk mengaktifkan penulisan aktif, lakukan langkah-langkah berikut ini:
 - a. Di tab Keamanan dari kotak dialog Properti internet, pilih Tingkat kustom.
 - b. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, gulir ke bawah untuk Penulisan dan pilih Aktifkan di bawah Penulisan aktif.
 - c. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.
4. Untuk mengaktifkan masuk otomatis, lakukan langkah-langkah berikut ini:
 - a. Di tab Keamanan dari kotak dialog Properti internet, pilih Tingkat kustom.
 - b. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, gulir ke bawah untuk Autentikasi Pengguna dan pilih Masuk otomatis hanya di zona Intranet di bawah Masuk.
 - c. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.
 - d. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.
5. Untuk mengaktifkan autentikasi terintegrasi, lakukan langkah-langkah berikut ini:
 - a. Di kotak dialog Properti internet, pilih tab Advanced.
 - b. Gulir ke bawah ke Keamanan dan pilih Mengaktifkan Autentikasi Windows Terintegrasi.
 - c. Di kotak dialog Properti Internet, pilih OK.
6. Tutup dan buka kembali peramban Anda agar perubahan ini berlaku.

Pembaruan manual untuk sign-on tunggal pada OS X

Untuk mengaktifkan sign-on tunggal secara manual untuk Chrome pada OS X, lakukan langkah-langkah berikut pada komputer klien. Anda memerlukan hak administrator di komputer Anda untuk menyelesaikan langkah-langkah ini.

Cara mengaktifkan sign-on tunggal untuk Chrome di OS X secara manual

1. Tambahkan URL akses Anda ke [AuthServerAllowlist](#) kebijakan dengan menjalankan perintah berikut:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Buka Preferensi Sistem, buka panel Profil, dan hapus profil Chrome Kerberos Configuration.
3. Mulai ulang Chrome dan buka `chrome://policy` di Chrome untuk mengonfirmasi bahwa pengaturan baru sudah terpasang.

Pengaturan kebijakan grup untuk sign-on tunggal

Administrator domain dapat menerapkan pengaturan Kebijakan Grup untuk membuat perubahan sign-on tunggal pada komputer klien yang digabungkan ke domain.

Note

Jika Anda mengelola browser web Chrome di komputer di domain Anda dengan kebijakan Chrome, Anda harus menambahkan URL akses ke [AuthServerAllowlist](#) kebijakan. Untuk informasi selengkapnya tentang mengatur kebijakan Chrome, kunjungi [Pengaturan Kebijakan di Chrome](#).

Cara mengaktifkan sign-on tunggal untuk Internet Explorer dan Chrome menggunakan pengaturan Kebijakan Grup

1. Membuat objek Kebijakan Grup baru dengan melakukan langkah-langkah berikut:
 - a. Buka alat Pengelolaan Kebijakan Grup, arahkan ke domain Anda, lalu pilih Objek Kebijakan Grup.
 - b. Dari menu utama, pilih Tindakan dan pilih Baru.

- c. Di kotak dialog GPO baru, masukkan nama deskriptif untuk objek Kebijakan Grup, seperti IAM Identity Center Policy, dan biarkan Sumber Starter GPO diatur ke (tidak ada). Klik OK.
2. Tambahkan URL akses ke daftar situs yang disetujui untuk sign-on tunggal dengan melakukan langkah-langkah berikut:
 - a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.
 - b. Di pohon kebijakan, arahkan ke Konfigurasi Pengguna > Preferensi > Pengaturan Windows.
 - c. Di daftar Pengaturan Windows, buka menu konteks (klik kanan) untuk Registri dan pilih Item registri baru.
 - d. Di kotak dialog Properti Registri Baru, masukkan pengaturan berikut dan pilih OK:

Tindakan

Update

Sarang

HKEY_CURRENT_USER

Jalan

Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com*<alias>*

Nilai untuk *<alias>* berasal dari URL akses Anda. Jika URL akses Anda adalah `https://examplecorp.awsapps.com`, alias adalah `examplecorp`, dan kunci registri akan menjadi `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

Nama nilai

https

Jenis nilai

REG_DWORD

Data nilai

3. Untuk mengaktifkan penulisan aktif, lakukan langkah-langkah berikut ini:
 - a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.
 - b. Di pohon kebijakan, arahkan ke Konfigurasi komputer > Kebijakan > Templat Administrasi > Komponen Windows > Internet Explorer > Panel Kontrol Internet > Halaman Keamanan > Zona Intranet.
 - c. Di daftar Zona Intranet, buka menu konteks (klik kanan) untuk Izinkan penulisan aktif dan pilih Edit.
 - d. Di kotak dialog Izinkan penulisan aktif, masukkan pengaturan berikut dan pilih OK:
 - Pilih tombol radio Diaktifkan.
 - Di bawah Opsi atur Izinkan penulisan aktif ke Aktifkan.
4. Untuk mengaktifkan masuk otomatis, lakukan langkah-langkah berikut ini:
 - a. Pada alat Pengelolaan Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan SSO Anda, lalu pilih Edit.
 - b. Di pohon kebijakan, arahkan ke Konfigurasi komputer > Kebijakan > Templat Administrasi > Komponen Windows > Internet Explorer > Panel Kontrol Internet > Halaman Keamanan > Zona Intranet.
 - c. Di daftar Zona Intranet, buka menu konteks (klik kanan) untuk Opsi masuk dan pilih Edit.
 - d. Di kotak dialog Opsi masuk, masukkan pengaturan berikut dan pilih OK:
 - Pilih tombol radio Diaktifkan.
 - Di bawah Opsi atur Opsi masuk ke Masuk otomatis hanya di zona Intranet.
5. Untuk mengaktifkan autentikasi terintegrasi, lakukan langkah-langkah berikut ini:
 - a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.
 - b. Di pohon kebijakan, arahkan ke Konfigurasi Pengguna > Preferensi > Pengaturan Windows.
 - c. Di daftar Pengaturan Windows, buka menu konteks (klik kanan) untuk Registri dan pilih Item registri baru.
 - d. Di kotak dialog Properti Registri Baru, masukkan pengaturan berikut dan pilih OK:

Tindakan

Update

Sarang

HKEY_CURRENT_USER

Jalan

Software\Microsoft\Windows\CurrentVersion\Internet Settings

Nama nilai

EnableNegotiate

Jenis nilai

REG_DWORD

Data nilai

1

6. Tutup jendela Editor Pengelolaan Kebijakan Grup jika masih terbuka.
7. Tetapkan kebijakan baru ke domain Anda dengan mengikuti langkah-langkah berikut:
 - a. Di pohon Pengelolaan Kebijakan Grup, buka menu konteks (klik kanan) untuk domain Anda, lalu pilih Menautkan GPO yang Ada.
 - b. Dalam daftar Objek Kebijakan Grup, pilih kebijakan Pusat Identitas IAM Anda dan pilih OK.

Perubahan ini akan berlaku setelah pembaruan Kebijakan Grup berikutnya pada klien, atau waktu berikutnya pengguna masuk.

Sign-on tunggal untuk Firefox

Untuk mengizinkan browser Mozilla Firefox mendukung sistem masuk tunggal, tambahkan URL akses Anda (mis., <https://<alias>.awsapps.com>) ke daftar situs yang disetujui untuk sistem masuk tunggal. Ini bisa dilakukan secara manual, atau otomatis dengan skrip.

Topik

- [Pembaruan manual untuk sign-on tunggal](#)
- [Pembaruan otomatis untuk sign-on tunggal](#)

Pembaruan manual untuk sign-on tunggal

Untuk menambahkan URL akses Anda ke daftar situs yang disetujui di Firefox secara manual, lakukan langkah-langkah berikut pada komputer klien.

Untuk menambahkan URL akses Anda secara manual ke daftar situs yang disetujui di Firefox

1. Buka Firefox dan buka halaman `about:config`.
2. Buka preferensi `network.negotiate-auth.trusted-uris` dan tambahkan URL akses Anda ke daftar situs. Gunakan koma (,) untuk memisahkan beberapa entri.

Pembaruan otomatis untuk sign-on tunggal

Sebagai administrator domain, Anda dapat menggunakan skrip untuk menambahkan URL akses ke preferensi pengguna `network.negotiate-auth.trusted-uris` Firefox pada semua komputer di jaringan Anda. Untuk informasi lebih lanjut, kunjungi <https://support.mozilla.org/en-US/questions/939037>.

Cara untuk bergabung dengan instans Amazon EC2 ke Simple AD Anda

Anda dapat menggabungkan instans Amazon EC2 dengan mulus ke domain Direktori Aktif saat instans diluncurkan. Untuk informasi selengkapnya, lihat [Bergabung dengan instans Windows Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola](#). Anda juga dapat meluncurkan instans EC2 dan menggabungkannya ke domain Active Directory langsung dari Directory Service konsol dengan [AWS Systems Manager Automation](#).

Jika Anda perlu menggabungkan instans EC2 secara manual ke domain Active Directory, Anda harus meluncurkan instance di Region yang tepat dan grup keamanan atau subnet, lalu gabungkan instance ke domain.

Untuk dapat terhubung dari jarak jauh ke instans ini, Anda harus memiliki konektivitas IP ke instans dari jaringan di mana Anda menghubungkannya dari. Dalam kebanyakan kasus, ini mengharuskan gateway internet dilampirkan ke VPC Anda dan instans tersebut memiliki alamat IP publik.

Topik

- [Bergabung dengan instans Windows Amazon EC2 ke Simple AD Active Directory](#)
- [Bergabunglah dengan instans Amazon EC2 Linux ke Simple AD Active Directory](#)

- [Mendelegasikan hak istimewa bergabung direktori untuk Simple AD](#)
- [Membuat opsi DHCP yang ditetapkan untuk Simple AD](#)

Bergabung dengan instans Windows Amazon EC2 ke Simple AD Active Directory

Anda dapat meluncurkan dan bergabung dengan Windows instans Amazon EC2 ke Simple AD. Atau, Anda dapat secara manual menggabungkan Windows instans EC2 yang ada ke Simple AD

Seamlessly join an EC2 Windows

Agar domain bergabung dengan instans EC2 dengan mulus, Anda harus menyelesaikan yang berikut ini:

Prasyarat

- Memiliki Iklan Sederhana Untuk mempelajari lebih lanjut, lihat [Buat Simple AD Anda](#).
- Anda memerlukan izin IAM berikut untuk bergabung dengan instans EC2 dengan mulus: Windows
 - Profil Instans IAM dengan izin IAM berikut:
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - Domain pengguna yang bergabung dengan EC2 ke Simple AD dengan mulus memerlukan izin IAM berikut:
 - Directory Service Izin:
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Izin VPC Amazon:
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
 - Izin EC2:

- "ec2:DescribeInstances"
- "ec2:DescribeImages"
- "ec2:DescribeInstanceTypes"
- "ec2:RunInstances"
- "ec2:CreateTags"
- AWS Systems Manager Izin:
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"

Saat Simple AD dibuat, grup keamanan dibuat dengan aturan masuk dan keluar. Untuk mempelajari lebih lanjut tentang aturan dan port ini, lihat [Apa yang dibuat dengan Simple AD Anda](#). Agar domain bergabung dengan Windows instans EC2 dengan mulus, VPC tempat Anda meluncurkan instans harus mengizinkan port yang sama yang diizinkan dalam aturan masuk dan keluar grup keamanan Simple AD Anda.

- Bergantung pada keamanan jaringan dan pengaturan firewall Anda, Anda mungkin diminta untuk mengizinkan lalu lintas keluar tambahan. Lalu lintas ini akan untuk HTTPS (port 443) ke titik akhir berikut:

Titik akhir	Peran
ec2messages. <i>region</i> .amazonaws.com	Membuat dan menghapus saluran sesi dengan layanan Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .
ssm. <i>region</i> .amazonaws.com	Titik akhir untuk AWS Systems Manager Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .

Titik akhir	Peran
ssmmessages. <i>region</i> .amazonaws.com	Membuat dan menghapus saluran sesi dengan layanan Session Manager. Untuk informasi lebih lanjut, lihat AWS Systems Manager kuota dan titik akhir .
ds. <i>region</i> .amazonaws.com	Titik akhir untuk Directory Service. Untuk informasi selengkapnya, lihat Ketersediaan wilayah untuk Directory Service .

- Sebaiknya gunakan server DNS yang akan menyelesaikan nama domain Simple AD Anda. Untuk melakukannya, Anda dapat membuat set opsi DHCP. Untuk informasi selengkapnya, lihat [Membuat opsi DHCP yang ditetapkan untuk Simple AD](#).
 - Jika Anda memilih untuk tidak membuat set opsi DHCP, maka server DNS Anda akan statis dan dikonfigurasi oleh Simple AD Anda.
1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
 2. Di bilah navigasi, pilih yang AWS Region sama dengan direktori yang ada.
 3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
 4. Pada halaman Luncurkan instance, di bawah bagian Nama dan Tag, masukkan nama yang ingin Anda gunakan untuk instans Windows EC2 Anda.
 5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
 6. Di bagian Application and OS Image (Amazon Machine Image), pilih Windows di panel Mulai Cepat. Anda dapat mengubah Windows Amazon Machine Image (AMI) dari daftar dropdown Amazon Machine Image (AMI).
 7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
 8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada.
 - a. Untuk membuat key pair baru, pilih Create new key pair.

- b. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format.
- c. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk.
- d. Pilih create key pair.
- e. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

**Important**

Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat [Connect to the internet menggunakan gateway internet](#) di Panduan Pengguna Amazon VPC.

11. Di bawah Auto-assign IP publik, pilih Aktifkan.

Untuk informasi selengkapnya tentang pengalamatan IP publik dan pribadi, lihat pengalamatan [IP instans Amazon EC2](#) di Panduan Pengguna Amazon EC2.

12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

**Note**

Setelah memilih direktori Gabung Domain, Anda mungkin melihat:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:

- Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
- Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, Anda dapat memilih profil instans IAM yang ada atau membuat yang baru. Pilih profil instans IAM yang memiliki kebijakan AWS terkelola Amazon SSMManged InstanceCore dan Amazon yang SSMDirectory ServiceAccess dilampirkan padanya dari daftar dropdown profil instans IAM. Untuk membuat yang baru, pilih Buat tautan profil IAM baru, lalu lakukan hal berikut:

1. Pilih Buat peran.
2. Di bawah Pilih entitas tepercaya, pilih AWS layanan.
3. Di bawah Kasus penggunaan, pilih EC2.
4. Di bawah Tambahkan izin, dalam daftar kebijakan, pilih SSMDirectory ServiceAccess kebijakan Amazon SSMManged InstanceCore dan Amazon. Untuk memfilter daftar, **SSM** ketik kotak pencarian. Pilih Berikutnya.

 Note

Amazon SSMDirectory ServiceAccess menyediakan izin untuk menggabungkan instance ke Active Directory yang dikelola oleh Directory ServiceAmazon SSMManged InstanceCore memberikan izin minimum yang diperlukan untuk menggunakan AWS Systems Manager layanan ini. Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan

kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat [Buat profil instans IAM untuk Systems Manager](#) di Panduan Pengguna AWS Systems Manager .

5. Pada halaman Nama, tinjau, dan buat, masukkan nama Peran. Anda akan memerlukan nama peran ini untuk melampirkan ke instans EC2.
 6. (Opsional) Anda dapat memberikan deskripsi profil instans IAM di bidang Deskripsi.
 7. Pilih Buat peran.
 8. Kembali ke Luncurkan halaman instans dan pilih ikon penyegaran di sebelah profil instans IAM. Profil instans IAM baru Anda harus terlihat di daftar dropdown profil instans IAM. Pilih profil baru dan biarkan pengaturan lainnya dengan nilai defaultnya.
16. Pilih Luncurkan instans.

Manually join an EC2 Windows

Untuk menggabungkan instans Windows Amazon EC2 yang ada secara manual ke Simple AD Active Directory, instance harus diluncurkan menggunakan parameter seperti yang ditentukan dalam. [Bergabung dengan instans Windows Amazon EC2 ke Simple AD Active Directory](#)

Anda akan memerlukan alamat IP dari server DNS Simple AD. Informasi ini dapat ditemukan di bawah Layanan Direktori > Direktori > tautan ID Direktori untuk direktori Anda> Detail direktori dan bagian Jaringan & Keamanan.

The screenshot displays the AWS Directory Service console for a specific directory instance. The left sidebar shows the navigation menu with 'Directories' selected under 'Active Directory'. The main content area shows the directory details for 'd-1234567890'. The 'Directory details' section includes fields for Directory type (Microsoft AD), Edition (Standard), Operating system version (Windows Server 2019), Directory DNS name (corp.example.com), Directory NetBIOS name (corp), and Directory administration EC2 instance(s) (-). Below this, the 'Networking details' section shows the VPC, Availability zones (us-east-2a, us-east-2b), and Subnets. A red box highlights the DNS addresses 192.0.2.1 and 198.51.100.1.

Untuk menggabungkan instance Windows ke Simple AD Active Directory

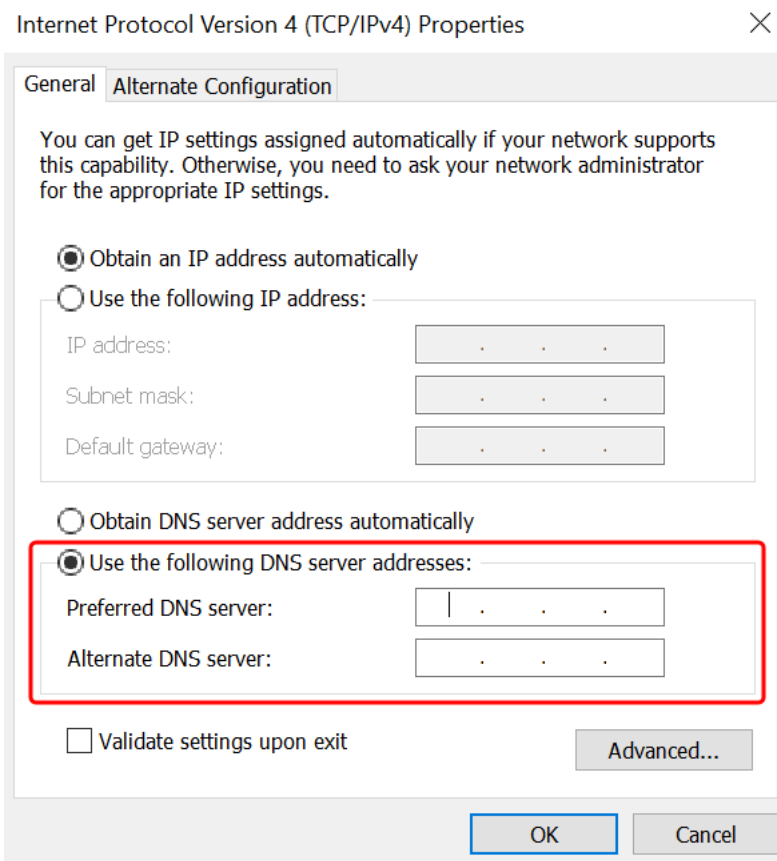
1. Connect ke instans menggunakan klien Remote Desktop Protocol.
2. Buka kotak dialog IPv4 TCP/properties pada instance.
 - a. Buka Koneksi Jaringan.

Tip

Anda dapat membuka Koneksi Jaringan langsung dengan menjalankan hal berikut dari prompt perintah pada instans.

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. Buka menu konteks (klik kanan) untuk koneksi jaringan yang aktif mana pun dan pilih Properti .
 - c. Dalam kotak dialog properti koneksi, buka (klik dua kali) Protokol Internet Versi 4.
3. Pilih Gunakan alamat server DNS berikut, ubah server DNS pilihan dan alamat server DNS alternatif ke alamat IP server DNS yang disediakan Iklan Sederhana Anda, dan pilih OK.



4. Buka kotak dialog Properti Sistem untuk instans, pilih tab Nama Komputer, dan pilih Ubah.

Tip

Anda dapat membuka kotak dialog Properti Sistem langsung dengan menjalankan hal berikut dari prompt perintah pada instans.

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. Di bidang Anggota, pilih Domain, masukkan nama yang sepenuhnya memenuhi syarat dari Simple AD Active Directory Anda, dan pilih OK.
6. Saat diminta nama dan kata sandi untuk administrator domain, masukkan nama pengguna dan kata sandi akun yang memiliki hak istimewa bergabung domain. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk Simple AD](#).

 Note

Anda dapat memasukkan nama domain yang sepenuhnya memenuhi syarat atau nama NetBIOS, diikuti dengan garis miring terbalik (\), dan kemudian nama pengguna. Nama pengguna akan menjadi Administrator. Misalnya, **corp.example.com\administrator** atau **corp\administrator**.

7. Setelah Anda menerima pesan yang menyambut Anda ke domain, mulai ulang instans agar perubahan berlaku.

Sekarang instans Anda telah bergabung ke domain Simple AD Active Directory, Anda dapat masuk ke instance itu dari jarak jauh dan menginstal utilitas untuk mengelola direktori, seperti menambahkan pengguna dan grup. Alat Administrasi Direktori Aktif dapat digunakan untuk membuat pengguna dan grup. Untuk informasi selengkapnya, lihat [Menginstal Alat Administrasi Direktori Aktif untuk Simple AD](#).

Bergabunglah dengan instans Amazon EC2 Linux ke Simple AD Active Directory

Anda dapat meluncurkan dan bergabung dengan instans Amazon EC2 Linux ke Simple AD Anda di. Konsol Manajemen AWS Anda juga dapat menggabungkan instans EC2 Linux secara manual ke Simple AD Anda.

Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Server Perusahaan 15 SP1

 Note

Distribusi sebelum Ubuntu 14 dan Red Hat Enterprise Linux 7 dan 8 tidak mendukung fitur join domain yang mulus.

Cara domain bergabung dengan instans Linux EC2:

- [Bergabunglah dengan instans Amazon EC2 Linux dengan mulus ke Simple AD Active Directory](#)
- [Menggabungkan instans Amazon EC2 Linux secara manual ke Simple AD Active Directory](#)

Bergabunglah dengan instans Amazon EC2 Linux dengan mulus ke Simple AD Active Directory

Prosedur ini menggabungkan instans Amazon EC2 Linux dengan mulus ke Simple AD Active Directory Anda.

Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Server Perusahaan 15 SP1

 Note

Distribusi sebelum Ubuntu 14 dan Red Hat Enterprise Linux 7 dan 8 tidak mendukung fitur join domain yang mulus.

Prasyarat

Sebelum Anda dapat mengatur gabungan domain tanpa batas ke instance Linux, Anda harus menyelesaikan prosedur di bagian ini.

Pilih akun layanan penggabungan domain mulus Anda

Anda dapat menggabungkan komputer Linux secara mulus ke domain Simple AD Anda. Untuk melakukannya, Anda harus membuat akun pengguna dengan membuat izin akun komputer untuk menggabungkan komputer ke domain. Meskipun anggota Admin Domain atau grup lain mungkin memiliki hak istimewa yang memadai untuk menggabungkan komputer ke domain, kami tidak menyarankan untuk menggunakan ini. Sebagai praktik terbaik, kami rekomendasikan Anda menggunakan akun layanan yang memiliki hak istimewa minimum yang diperlukan untuk menggabungkan komputer ke domain.

Untuk informasi tentang cara memproses dan mendelegasikan izin ke akun layanan Anda untuk pembuatan akun komputer, lihat [Mendelegasikan hak istimewa ke akun layanan Anda](#).

Membuat rahasia untuk menyimpan akun layanan domain

Anda dapat menggunakan AWS Secrets Manager untuk menyimpan akun layanan domain. Untuk informasi selengkapnya, lihat [Membuat AWS Secrets Manager rahasia](#).

Note

Ada biaya yang terkait dengan Secrets Manager. Untuk informasi selengkapnya lihat, [Harga](#) di Panduan AWS Secrets Manager Pengguna.

Untuk Membuat rahasia dan menyimpan informasi akun layanan domain

1. Masuk ke Konsol Manajemen AWS dan buka AWS Secrets Manager konsol di <https://console.aws.amazon.com/secretsmanager/>.
2. Pilih Simpan rahasia baru.
3. Pada halaman Simpan rahasia baru, lakukan hal berikut:
 - a. Di bawah Tipe rahasia, pilih Jenis rahasia lainnya.
 - b. Di bawah pasangan kunci/nilai, lakukan hal berikut:
 - i. Dalam kotak pertama, masukkan **awsSeamlessDomainUsername**. Pada baris yang sama, di kotak berikutnya, masukkan nama pengguna untuk akun layanan Anda. Misalnya, jika Anda menggunakan PowerShell perintah sebelumnya, nama akun layanan akan menjadi **awsSeamlessDomain**.

Note

Anda harus memasukkan **awsSeamlessDomainUsername** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

The screenshot shows the AWS Secrets Manager console interface for creating a new secret. The breadcrumb navigation is **AWS Secrets Manager > Secrets > Store a new secret**. The left sidebar shows the steps: **Step 1: Choose secret type**, **Step 2: Configure secret**, **Step 3 - optional: Configure rotation**, and **Step 4: Review**. The main content area is titled **Choose secret type**. Under **Secret type**, four options are available: **Credentials for Amazon RDS database**, **Credentials for Amazon DocumentDB database**, **Credentials for Amazon Redshift cluster**, and **Other type of secret** (which is selected and highlighted with a red box). Below this, the **Key/value pairs** section shows a table with two columns: **Key/value** and **Plaintext**. The first row has **awsSeamlessDomainUsername** in the **Key/value** column (highlighted with a red box) and an empty **Plaintext** column. There is an **+ Add row** button below the table. The **Encryption key** section shows a dropdown menu with **aws/secretsmanager** selected and a **Refresh** button. At the bottom right, there are **Cancel** and **Next** buttons.

- ii. Pilih Tambahkan baris.
- iii. Pada baris baru, di kotak pertama, masukkan **awsSeamlessDomainPassword**. Pada baris yang sama, di kotak berikutnya, masukkan kata sandi untuk akun layanan Anda.

 Note

Anda harus memasukkan **awsSeamlessDomainPassword** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

- iv. Di bawah kunci Enkripsi, tinggalkan nilai default `aws/secretsmanager`. AWS Secrets Manager selalu mengenkripsi rahasia ketika Anda memilih opsi ini. Anda juga dapat memilih kunci yang Anda buat.
 - v. Pilih Berikutnya.
4. Di bawah nama Rahasia, masukkan nama rahasia yang menyertakan ID direktori Anda menggunakan format berikut, ganti `d-xxxxxxxx` dengan ID direktori Anda:

```
aws/directory-services/d-xxxxxxxx/seamless-domain-join
```

Ini akan digunakan untuk mengambil rahasia dalam aplikasi.

 Note

Anda harus memasukkan **aws/directory-services/d-xxxxxxxx/seamless-domain-join** persis seperti itu tetapi ganti `d-xxxxxxxx` dengan ID direktori Anda. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

Services Search [Alt+S] Ohio

AWS Secrets Manager > Secrets > Store a new secret

Step 1
[Choose secret type](#)

Step 2
Configure secret

Step 3 - optional
[Configure rotation](#)

Step 4
[Review](#)

Configure secret

Secret name and description [Info](#)

Secret name
A descriptive name that helps you find your secret later.

aws/directory-services/d-xxxxxxx/seamless-domain-join

Secret name must contain only alphanumeric characters and the characters `/_+:@-`.

Description - optional

Access to MYSQL prod database for my AppBeta

Maximum 250 characters.

Tags - optional

No tags associated with the secret.

[Add](#)

Resource permissions - optional [Info](#)

Add or edit a resource policy to access secrets across AWS accounts.

[Edit permissions](#)

► Replicate secret - optional

Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

[Cancel](#) [Previous](#) [Next](#)

5. Biarkan yang lainnya diatur ke default, dan kemudian pilih Selanjutnya.
6. Di bawah Konfigurasi rotasi otomatis, pilih Nonaktifkan rotasi otomatis, lalu pilih Selanjutnya.

Anda dapat mengaktifkan rotasi untuk rahasia ini setelah Anda menyimpannya.

7. Tinjau pengaturan, dan kemudian pilih Simpan untuk menyimpan perubahan Anda. Konsol Secrets Manager mengembalikan Anda ke daftar rahasia di akun Anda dengan rahasia baru Anda masuk di dalam daftar.
8. Pilih nama rahasia Anda yang baru dibuat dari daftar, dan perhatikan nilai ARN rahasia. Anda akan membutuhkannya di bagian selanjutnya.

Aktifkan rotasi untuk rahasia akun layanan domain

Kami menyarankan Anda memutar rahasia secara teratur untuk meningkatkan postur keamanan Anda.

Untuk mengaktifkan rotasi untuk rahasia akun layanan domain

- Ikuti petunjuk di [Mengatur rotasi otomatis untuk AWS Secrets Manager rahasia](#) di Panduan AWS Secrets Manager Pengguna.

Untuk Langkah 5, gunakan template rotasi [kredensial Microsoft Active Directory](#) di AWS Secrets Manager Panduan Pengguna.

Untuk bantuan, lihat [Memecahkan masalah AWS Secrets Manager rotasi](#) di AWS Secrets Manager Panduan Pengguna.

Untuk membuat kebijakan dan peran IAM yang diperlukan

Gunakan langkah-langkah prasyarat berikut untuk membuat kebijakan khusus yang memungkinkan akses hanya-baca ke rahasia gabungan domain tanpa batas Secrets Manager Anda (yang Anda buat sebelumnya), dan untuk membuat peran IAM Linux baru. EC2 DomainJoin

Membuat kebijakan membaca IAM Secrets Manager

Anda menggunakan konsol IAM untuk membuat kebijakan yang memberikan akses hanya-baca ke rahasia Secrets Manager Anda.

Untuk membuat kebijakan membaca IAM Secrets Manager

- Masuk ke pengguna Konsol Manajemen AWS sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Kemudian buka konsol IAM di <https://console.aws.amazon.com/iam/>.
- Di panel navigasi, Manajemen Akses, pilih Kebijakan.
- Pilih Buat kebijakan.
- Pilih tab JSON dan salin teks dari dokumen kebijakan JSON berikut. Kemudian tempelkan ke dalam kotak teks JSON.

Note

Pastikan Anda mengganti Region and Resource ARN dengan Region dan ARN sebenarnya dari rahasia yang Anda buat sebelumnya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-east-1:xxxxxxxx:secret:aws/directory-
services/d-xxxxxxxx/seamless-domain-join"
      ]
    }
  ]
}
```

5. Setelah selesai, pilih Selanjutnya. Validator kebijakan melaporkan kesalahan sintaksis. Untuk informasi selengkapnya, lihat [Memvalidasi kebijakan IAM](#).
6. Pada halaman Tinjau kebijakan, masukkan nama kebijakan, seperti **SM-Secret-Linux-DJ-d-xxxxxxxx-Read**. Tinjau bagian Ringkasan untuk melihat izin yang diberikan oleh kebijakan Anda. Lalu pilih Buat kebijakan untuk menyimpan perubahan Anda. Kebijakan baru muncul di daftar kebijakan terkelola dan siap dilampirkan pada identitas.

Note

Kami rekomendasikan Anda membuat satu kebijakan per rahasia. Melakukan hal tersebut memastikan bahwa instans hanya memiliki akses ke rahasia yang sesuai dan meminimalkan dampak jika sebuah instans dikompromikan.

Buat EC2 DomainJoin peran Linux

Anda menggunakan konsol IAM untuk membuat peran yang akan Anda gunakan untuk penggabungan domain dengan instans EC2 Linux Anda.

Untuk membuat EC2 DomainJoin peran Linux

1. Masuk ke pengguna Konsol Manajemen AWS sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Kemudian buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi, di bawah Manajemen Akses, pilih Peran.
3. Di panel konten, pilih Buat peran.
4. Di bawah Pilih jenis entitas terpercaya, pilih AWS layanan.
5. Di bawah Kasus penggunaan, pilih EC2, lalu pilih Berikutnya.

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected. The 'Service or use case' dropdown is set to 'EC2'.

6. Untuk Kebijakan filter, lakukan hal berikut:

- a. Masukkan **AmazonSSMManagedInstanceCore**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.
- b. Masukkan **AmazonSSMDirectoryServiceAccess**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.
- c. Masukkan **SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read** (atau nama kebijakan yang Anda buat dalam prosedur sebelumnya). Lalu pilih kotak centang untuk item tersebut di dalam daftar.

- d. Setelah menambahkan tiga kebijakan yang tercantum di atas, pilih Buat peran.

 Note

Amazon SSMDirectory ServiceAccess menyediakan izin untuk menggabungkan instance ke Active Directory yang dikelola oleh Directory Service Amazon SSMMManaged InstanceCore memberikan izin minimum yang diperlukan untuk menggunakan AWS Systems Manager layanan ini. Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat [Buat profil instans IAM untuk Systems Manager](#) di Panduan Pengguna AWS Systems Manager .

7. Masukkan nama untuk peran baru Anda, seperti **LinuxEC2DomainJoin** atau nama lain yang Anda inginkan di bidang Nama peran.
8. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
9. (Opsional) Pilih Tambahkan tag baru di bawah Langkah 3: Tambahkan tag untuk menambahkan tag. Pasangan nilai kunci tag digunakan untuk mengatur, melacak, atau mengontrol akses untuk peran ini.
10. Pilih Buat peran.

Bergabunglah dengan instans Linux dengan mulus ke Simple AD Active Directory Anda

Untuk bergabung dengan instans Linux Anda dengan mulus

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Dari pemilih Region di bilah navigasi, pilih yang AWS Region sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Name and Tags, masukkan nama yang ingin Anda gunakan untuk instans Linux EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih AMI Linux yang ingin Anda luncurkan.

 Note

AMI yang digunakan harus memiliki AWS Systems Manager (Agen SSM) versi 2.3.1644.0 atau lebih tinggi. Untuk memeriksa versi SSM Agent yang diinstal di AMI Anda dengan meluncurkan sebuah instans dari AMI tersebut, lihat [Mendapatkan versi Agen SSM yang saat ini diinstal](#). Jika Anda perlu meningkatkan Agen SSM, lihat [Menginstal dan mengkonfigurasi SSM Agent pada instans EC2 untuk Linux](#).

SSM menggunakan `aws:domainJoin` plugin saat menggabungkan instance Linux ke domain Active Directory. Plugin mengubah nama host untuk instance Linux ke format EC2 AMAZ-`XXXXXXXX`. Untuk informasi selengkapnya `aws:domainJoin`, lihat [referensi plugin dokumen AWS Systems Manager perintah](#) di Panduan AWS Systems Manager Pengguna.

7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada. Untuk membuat key pair baru, pilih Create new key pair. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk. Pilih create key pair. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

 Important

Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat [Connect to the internet menggunakan gateway internet](#) di Panduan Pengguna Amazon VPC.

11. Di bawah Auto-assign IP publik, pilih Aktifkan.

Untuk informasi selengkapnya tentang pengalamatan IP publik dan pribadi, lihat pengalamatan [IP instans Amazon EC2](#) di Panduan Pengguna Amazon EC2.

12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

Note

Setelah memilih direktori Gabung Domain, Anda mungkin melihat:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:

- Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
- Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, pilih peran IAM yang sebelumnya Anda buat di bagian prasyarat Langkah 2: Buat peran Linux. EC2 DomainJoin
16. Pilih Luncurkan instans.

 Note

Jika Anda menjalankan penggabungan domain yang mulus dengan SUSE Linux, reboot diperlukan sebelum autentikasi akan bekerja. Untuk me-reboot SUSE dari terminal Linux, ketik `sudo reboot`.

Menggabungkan instans Amazon EC2 Linux secara manual ke Simple AD Active Directory

Selain instans Windows Amazon EC2, Anda juga dapat menggabungkan instans Amazon EC2 Linux tertentu ke Simple AD Active Directory. Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Server Perusahaan 15 SP1

 Note

Distribusi dan versi Linux lainnya mungkin bekerja namun belum diuji.

Prasyarat

Sebelum Anda dapat menggabungkan instans Amazon Linux, CentOS, Red Hat, atau Ubuntu ke direktori Anda, instans harus terlebih dahulu diluncurkan sebagaimana ditentukan dalam [Bergabunglah dengan instans Amazon EC2 Linux dengan mulus ke Simple AD Active Directory](#).

 Important

Beberapa prosedur berikut, jika tidak dilakukan dengan benar, dapat membuat instans anda tidak terjangkau atau tidak dapat digunakan. Oleh karena itu, kami sangat menyarankan

Anda membuat backup atau mengambil snapshot dari instans Anda sebelum melakukan prosedur ini.

Untuk bergabung dengan instance Linux ke direktori Anda

Ikuti langkah-langkah untuk instans Linux tertentu Anda menggunakan salah satu tab berikut:

Amazon Linux

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat](#) dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Amazon Linux - 64bit Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Amazon Linux yang diperlukan pada instans Linux Anda.

Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli  
krb5-workstation
```

 Note

Untuk bantuan dalam menentukan versi Amazon Linux yang Anda gunakan, lihat [Mengidentifikasi image Amazon Linux](#) dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...  
* Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.
 - a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan PasswordAuthentication ke yes.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:


```
sudo service sshd restart
```

7. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH mana pun dan tambahkan grup admin domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan hal berikut ini ke bagian bawah file sudoers dan simpan.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "<space>" untuk membuat karakter spasi Linux.)

CentOS

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasi instance Linux untuk menggunakan alamat IP server DNS dari server DNS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat](#) dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans CentOS 7 Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket CentOS 7 yang diperlukan pada instans Linux Anda.

Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...  
* Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

- a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan PasswordAuthentication ke `yes`.

```
PasswordAuthentication yes
```

- c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

7. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH mana pun dan tambahkan grup admin domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan hal berikut ini ke bagian bawah file sudoers dan simpan.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "<space>" untuk membuat karakter spasi Linux.)

Red hat

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasi instance Linux untuk menggunakan alamat IP server DNS dari server DNS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat](#) dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Red Hat - 64bit adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Red Hat yang diperlukan pada instans Linux Anda.

Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -v -U join_account example.com --install=/  
join_account
```

join_account

AMAccountName s untuk akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...  
* Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

b. Atur pengaturan PasswordAuthentication ke yes.

```
PasswordAuthentication yes
```

c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

7. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH mana pun dan tambahkan grup admin domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

- a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

- b. Tambahkan hal berikut ini ke bagian bawah file sudoers dan simpan.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "<space>" untuk membuat karakter spasi Linux.)

Ubuntu

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasi instance Linux untuk menggunakan alamat IP server DNS dari server DNS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat [Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat](#) dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Ubuntu - 64bit Anda adalah yang terbaru.

```
sudo apt-get update  
sudo apt-get -y upgrade
```

4. Instal paket Ubuntu yang diperlukan pada instans Linux Anda.

Note

Beberapa paket ini mungkin sudah diinstal.

Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Nonaktifkan resolusi Reverse DNS dan atur ranah default ke FQDN domain Anda. Instans Ubuntu harus dapat dipecahkan terbalik di DNS sebelum ranah akan bekerja. Jika tidak, Anda harus menonaktifkan DNS terbalik di `/etc/krb5.conf` sebagai berikut:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

AMAccountNama s untuk akun di *example.com* domain yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa bergabung direktori untuk AWS Microsoft AD yang Dikelola](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
* Successfully enrolled machine in realm
```

7. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.
 - a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vi /etc/ssh/sshd_config
```

- b. Atur pengaturan PasswordAuthentication ke yes.

```
PasswordAuthentication yes
```

c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

8. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH mana pun dan tambahkan grup admin domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

a. Buka file sudoers dengan perintah berikut:

```
sudo visudo
```

b. Tambahkan hal berikut ini ke bagian bawah file sudoers dan simpan.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan "<space>" untuk membuat karakter spasi Linux.)

 Note

Saat menggunakan Simple AD, jika Anda membuat akun pengguna pada instans Linux dengan opsi "Paksa pengguna untuk mengubah kata sandi saat login pertama," pengguna tersebut tidak akan dapat mengubah kata sandi mereka menggunakan kpasswd. Untuk mengubah kata sandi pertama kalinya, administrator domain harus memperbarui sandi pengguna menggunakan Alat Pengelolaan Direktori Aktif.

Mengelola akun dari instans Linux

Untuk mengelola akun di Simple AD dari instans Linux, Anda harus memperbarui file konfigurasi tertentu pada instans Linux Anda sebagai berikut:

1. Setel `krb5_use_kdcinfo` ke `False` di `file/.conf. etc/sss/sss` Contoh:

```
[domain/example.com]
krb5_use_kdcinfo = False
```

2. Agar konfigurasi mulai berlaku Anda perlu memulai ulang layanan `sss`:

```
$ sudo systemctl restart sss.service
```

Atau, Anda dapat menggunakan .

```
$ sudo service sss start
```

3. Jika Anda akan mengelola pengguna dari instans CentOS Linux, Anda juga harus mengedit file `/etc/smb.conf` untuk memasukkan:

```
[global]
workgroup = EXAMPLE.COM
realm = EXAMPLE.COM
netbios name = EXAMPLE
security = ads
```

Membatasi akses login akun

Karena semua akun ditetapkan dalam Direktori Aktif, secara default, semua pengguna dalam direktori tersebut dapat masuk ke instans. Anda dapat mengizinkan hanya pengguna tertentu untuk masuk ke instans dengan `ad_access_filter` di `sss.conf`. Contoh:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Menunjukkan bahwa pengguna hanya boleh diizinkan akses ke instans jika mereka adalah anggota dari grup tertentu.

cn

Nama umum grup yang harus memiliki akses. Dalam contoh ini, nama grup adalah *admins*.

ou

Ini adalah unit organisasi tempat grup di atas berada. Dalam contoh ini, OU adalah *Testou*.

dc

Ini adalah komponen domain dari domain Anda. Dalam contoh ini, *example*.

dc

Ini adalah komponen domain tambahan. Dalam contoh ini, *com*.

Anda harus menambahkan `ad_access_filter` secara manual ke `/etc/sssdc/sssdc.conf`.

Buka file `/etc/sssdc/sssdc.conf` di editor teks.

```
sudo vi /etc/sssdc/sssdc.conf
```

Setelah melakukan hal ini, `sssdc.conf` Anda mungkin terlihat seperti ini:

```
[sssdc]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Agar konfigurasi mulai berlaku, Anda perlu memulai ulang layanan `sssdc`:

```
sudo systemctl restart sssdc.service
```

Atau, Anda dapat menggunakan .

```
sudo service sssd restart
```

Pemetaan ID

Pemetaan ID dapat dilakukan dengan dua metode untuk mempertahankan pengalaman terpadu antara UNIX/Linux User Identifier (UID) dan Group Identifier (GID) dan identitas Windows dan Active Directory Security Identifier (SID). Metode-metode ini adalah:

1. Tersentralisasi
2. Didistribusikan

Note

Pemetaan identitas pengguna terpusat di Active Directory memerlukan Antarmuka Sistem Operasi Portabel atau POSIX.

Pemetaan identitas pengguna terpusat

Active Directory atau layanan Lightweight Directory Access Protocol (LDAP) lainnya menyediakan UID dan GID kepada pengguna Linux. Di Active Directory, pengidentifikasi ini disimpan dalam atribut pengguna jika ekstensi POSIX dikonfigurasi:

- UID - Nama pengguna Linux (String)
- Nomor UID - Nomor ID Pengguna Linux (Integer)
- Nomor GID - Nomor ID Grup Linux (Integer)

Untuk mengkonfigurasi instance Linux untuk menggunakan UID dan GID dari Active Directory, atur `ldap_id_mapping = False` dalam file `sssd.conf`. Sebelum menyetel nilai ini, verifikasi bahwa Anda telah menambahkan UID, nomor UID, dan nomor GID ke pengguna dan grup di Active Directory.

Pemetaan identitas pengguna terdistribusi

Jika Active Directory tidak memiliki ekstensi POSIX atau jika Anda memilih untuk tidak mengelola pemetaan identitas secara terpusat, Linux dapat menghitung nilai UID dan GID. Linux menggunakan Security Identifier (SID) unik pengguna untuk menjaga konsistensi.

Untuk mengonfigurasi pemetaan ID pengguna terdistribusi, atur `ldap_id_mapping = True` dalam file `sssd.conf`.

Masalah umum

Jika Anda mengatur `ldap_id_mapping = False`, terkadang memulai layanan SSSD akan gagal. Alasan kegagalan ini adalah karena perubahan UIDs tidak didukung. Kami menyarankan Anda menghapus cache SSSD setiap kali Anda mengubah dari pemetaan ID ke atribut POSIX atau dari atribut POSIX ke pemetaan ID. Untuk detail lebih lanjut tentang pemetaan ID dan parameter `ldap_id_mapping`, lihat halaman manual `sssd-ldap` (8) di baris perintah Linux.

Connect ke instance Linux

Ketika pengguna terhubung ke instance menggunakan klien SSH, mereka diminta untuk nama pengguna mereka. Pengguna dapat memasukkan nama pengguna dalam `EXAMPLE\username` format `username@example.com` atau. Respons akan muncul mirip dengan yang berikut ini, tergantung pada distribusi Linux yang Anda gunakan:

Amazon Linux, Red Hat Enterprise Linux, dan CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

```
As "root" (sudo or sudo -i) use the:
```

- zypper command for package management
- yast command for configuration management

```
Management and Config: https://www.suse.com/suse-in-the-cloud-basics
```

```
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Sat Apr 18 22:03:35 UTC 2020

System load:  0.01               Processes:            102
Usage of /:   18.6% of 7.69GB    Users logged in:     2
Memory usage: 16%               IP address for eth0: 10.24.34.1
Swap usage:   0%
```

Mendelegasikan hak istimewa bergabung direktori untuk Simple AD

Untuk bergabung dengan komputer ke direktori Anda, Anda memerlukan akun yang memiliki hak istimewa untuk menggabungkan komputer ke direktori.

Dengan Simple AD, anggota grup Admin domain memiliki hak istimewa yang memadai untuk menggabungkan komputer ke direktori.

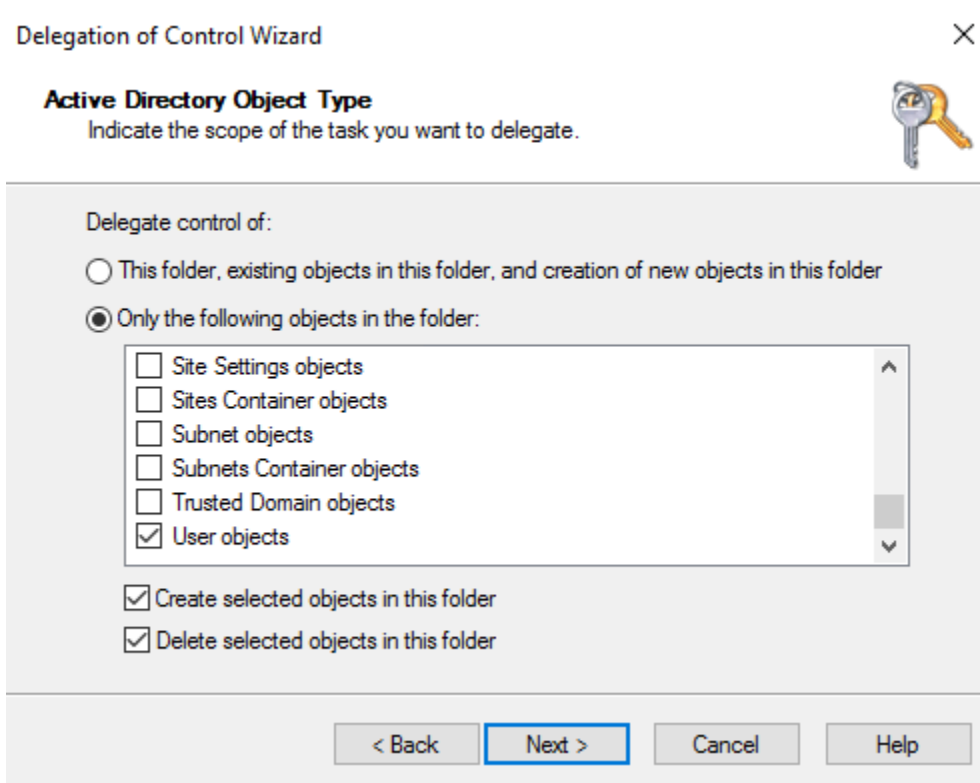
Namun, sebagai praktik terbaik, Anda harus menggunakan akun yang hanya memiliki hak istimewa minimum yang diperlukan. Prosedur berikut menunjukkan cara membuat grup baru yang disebut **Joiners** dan mendelegasikan hak istimewa untuk grup ini yang diperlukan untuk menggabungkan komputer ke direktori.

Anda harus melakukan prosedur ini pada komputer yang telah tergabung ke direktori Anda dan memiliki MMC snap-in Pengguna dan Komputer Direktori Aktif terinstal. Anda juga harus masuk sebagai administrator domain.

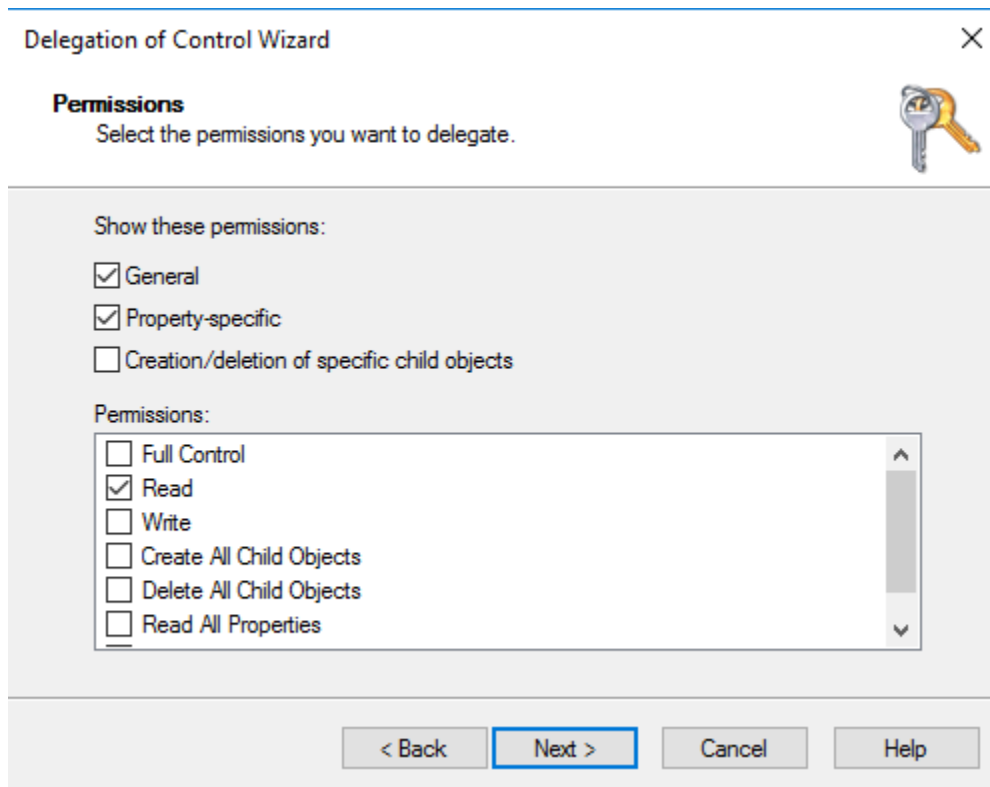
Untuk mendelegasikan hak istimewa penggabungan direktori untuk Simple AD

1. Buka Pengguna dan Komputer Direktori Aktif dan pilih root domain Anda di pohon navigasi.
2. Di pohon navigasi sebelah kiri, buka menu konteks (klik kanan) untuk Pengguna, pilih Baru, lalu pilih Grup.
3. Di kotak Objek Baru - Grup, ketik hal berikut dan pilih OK.

- Untuk Nama grup, ketik **Joiners**.
 - Untuk Cakupan grup, pilih Global.
 - Untuk Jenis grup, pilih Keamanan.
4. Pada pohon navigasi, pilih root domain Anda. Dari menu Tindakan, pilih Kendali Delegasi.
 5. Pada halaman Delegasi Control Wizard, pilih Selanjutnya, lalu pilih Tambahkan.
 6. Di kotak Pilih Pengguna, Komputer, atau Grup, ketik Joiners dan pilih OK. Jika ditemukan lebih dari satu objek, pilih grup Joiners yang dibuat di atas. Pilih Berikutnya.
 7. Pada halaman Tugas untuk Didelegasikan, pilih Buat tugas kustom untuk didelegasikan, lalu pilih Selanjutnya.
 8. Pilih Hanya objek berikut dalam folder, lalu pilih Objek komputer.
 9. Pilih Buat objek yang dipilih dalam folder ini dan Hapus objek yang dipilih dalam folder ini. Lalu pilih Selanjutnya.



10. Pilih Baca dan Tulis, lalu pilih Selanjutnya.



11. Verifikasi informasi pada halaman Menyelesaikan Delegasi Control Wizard, dan klik Selesai.
12. Buat pengguna dengan kata sandi yang kuat dan tambahkan pengguna tersebut ke grup Joiners. Pengguna kemudian akan memiliki hak istimewa yang cukup untuk terhubung Directory Service ke direktori.

Membuat opsi DHCP yang ditetapkan untuk Simple AD

AWS merekomendasikan agar Anda membuat set opsi DHCP untuk Directory Service direktori Anda dan menetapkan opsi DHCP yang disetel ke VPC tempat direktori Anda berada. Ini memungkinkan setiap instans di VPC tersebut mengarah ke domain tertentu, dan server DNS untuk menyelesaikan nama domain mereka.

Untuk informasi selengkapnya tentang set opsi DHCP, lihat [Set opsi DHCP](#) di Panduan Pengguna Amazon VPC.

Untuk membuat set opsi DHCP untuk direktori Anda

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Di panel navigasi, pilih Set Opsi DHCP, lalu pilih Buat set opsi DHCP.
3. Pada halaman Buat set opsi DHCP, masukkan nilai berikut untuk direktori Anda:

Nama

Tanda opsional untuk set opsi.

Nama domain

Nama yang memenuhi syarat untuk direktori, seperti `corp.example.com`.

Server nama domain

Alamat IP server DNS direktori AWS-provided Anda.

 Note

Anda dapat menemukan alamat ini dengan membuka panel navigasi [Konsol AWS Directory Service](#), memilih direktori dan kemudian memilih ID direktori yang benar.

Server NTP

Biarkan bidang ini kosong.

Server nama NetBIOS

Biarkan bidang ini kosong.

Jenis simpul NetBIOS

Biarkan bidang ini kosong.

4. Pilih Buat set opsi DHCP. Set opsi DHCP baru muncul dalam daftar opsi DHCP Anda.
5. Catat ID set baru opsi DHCP (dopt-**xxxxxxxx**). Anda menggunakannya untuk mengasosiasikan set opsi yang baru dengan VPC Anda.

Untuk mengubah set opsi DHCP yang terkait dengan VPC

Setelah Anda membuat set opsi DHCP, Anda tidak dapat mengubahnya. Jika Anda ingin VPC Anda untuk menggunakan set opsi DHCP yang berbeda, Anda harus membuat satu set baru dan mengasosiasikannya dengan VPC Anda. Anda juga dapat mengatur VPC Anda untuk tidak menggunakan opsi DHCP sama sekali.

1. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>

2. Di panel navigasi, pilih Your VPCs.
3. Pilih VPC, lalu pilih Tindakan, Edit pengaturan VPC.
4. Untuk Set opsi DHCP, pilih satu set opsi atau pilih Tidak ada set opsi DHCP, lalu pilih Simpan.

Untuk mengubah set opsi DHCP yang terkait dengan VPC menggunakan baris perintah lihat berikut ini:

- AWS CLI: [associate-dhcp-options](#)
- AWS Tools for Windows PowerShell: [Register-EC2DhcpOption](#)

Manajemen pengguna dan grup di Simple AD

Pengguna merepresentasikan orang individu atau entitas yang memiliki akses ke direktori Anda. Grup sangat berguna untuk memberikan atau menolak hak akses ke grup pengguna, daripada harus menerapkan hak akses tersebut ke setiap pengguna. Jika pengguna berpindah ke organisasi yang berbeda, Anda memindahkan pengguna tersebut ke grup yang berbeda dan mereka secara otomatis menerima hak istimewa yang diperlukan untuk organisasi baru.

Untuk membuat pengguna dan grup dalam Directory Service direktori, Anda harus menggunakan instans apa pun (baik dari lokal maupun EC2) yang telah bergabung ke Directory Service direktori Anda, dan masuk sebagai pengguna yang memiliki hak istimewa untuk membuat pengguna dan grup. Anda juga perlu menginstal Active Directory Tools pada EC2 instans Anda sehingga Anda dapat menambahkan pengguna dan grup Anda dengan snap-in Active Directory Users and Computers. Untuk informasi selengkapnya tentang cara mengatur EC2 instance dan menginstal alat yang diperlukan, lihat [Cara untuk bergabung dengan instans Amazon EC2 ke Simple AD Anda](#).

Note

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Ini adalah pengaturan default untuk akun pengguna baru, tetapi tidak boleh diubah. Untuk informasi selengkapnya tentang pengaturan ini, buka [Preauthentication](#) di Microsoft. TechNet

Topik berikut termasuk petunjuk tentang cara membuat dan mengelola pengguna dan grup.

Topik

- [Menginstal Alat Administrasi Direktori Aktif untuk Simple AD](#)
- [Membuat pengguna AD Sederhana](#)
- [Menghapus pengguna Simple AD](#)
- [Menyetel ulang kata sandi pengguna Simple AD](#)
- [Membuat grup AD Sederhana](#)
- [Menambahkan pengguna Simple AD ke grup](#)

Menginstal Alat Administrasi Direktori Aktif untuk Simple AD

Untuk mengelola Active Directory dari instans Amazon EC2 Windows Server, Anda perlu menginstal Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools pada instans. Gunakan prosedur berikut untuk menginstal alat ini pada instance Windows Server EC2.

Prasyarat

Sebelum Anda dapat memulai prosedur ini, selesaikan yang berikut ini:

1. Buat Direktori Aktif AD Sederhana. Untuk informasi selengkapnya, lihat [Buat Simple AD Anda](#).
2. Luncurkan dan gabungkan instans Windows Server EC2 ke Simple AD Active Directory Anda. Instans EC2 memerlukan kebijakan berikut untuk membuat pengguna dan grup: **AmazonSSMManagedInstanceCore** dan **AmazonSSMDirectoryServiceAccess**. Untuk informasi selengkapnya, lihat [Bergabung dengan instans Windows Amazon EC2 ke Simple AD Active Directory](#).
3. Anda akan memerlukan kredensi untuk Administrator domain Direktori Aktif Anda. Kredensi ini dibuat ketika Simple AD dibuat. Jika Anda mengikuti prosedur di [Buat Simple AD Anda](#), nama pengguna Administrator Anda menyertakan nama NetBIOS Anda, **corp\administrator**

Untuk menginstal alat administrasi Direktori Aktif pada instans EC2 Windows Server

1. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
2. Di konsol Amazon EC2, pilih Instans, pilih instance Windows Server, lalu pilih Connect.
3. Di halaman Connect to instance, pilih klien RDP.
4. Di tab klien RDP, pilih Unduh File Desktop Jarak Jauh, lalu pilih Dapatkan Kata Sandi untuk mengambil kata sandi Anda.

5. Dalam kata sandi Dapatkan Windows, pilih Unggah file kunci pribadi. Pilih file kunci pribadi.pem yang terkait dengan instance Windows Server. Setelah mengunggah file kunci pribadi, pilih Dekripsi kata sandi.
6. Di kotak dialog Keamanan Windows, salin kredensi administrator lokal Anda untuk komputer Windows Server untuk masuk. Nama pengguna dapat dalam format berikut: **NetBIOS-Name\administrator** atau **DNS-Name\administrator**. Misalnya, **corp\administrator** akan menjadi nama pengguna jika Anda mengikuti prosedur di [Buat Simple AD Anda](#).
7. Setelah masuk ke instance Windows Server, buka Server Manager dari menu Start dengan memilih Server Manager.
8. Di Dasbor Manajer Server, pilih Tambahkan peran dan fitur.
9. Di Tambahkan peran dan fitur Wizard pilih Jenis Instalasi, pilih Instalasi berbasis peran atau berbasis fitur, dan pilih Selanjutnya.
10. Di bawah Pilihan Server, pastikan server lokal dipilih, dan pilih Fitur di panel navigasi sebelah kiri.
11. Di pohon Fitur, pilih dan buka Alat Administrasi Server Jarak Jauh, Alat Administrasi Peran, dan Alat AD DS dan AD LDS. Dengan AD DS dan AD LDS Tools dipilih, modul Active Directory untuk PowerShell, AD DS Tools, dan AD LDS Snap-in dan Command-Line Tools dipilih. Gulir ke bawah dan pilih DNS Server Tools, lalu pilih Berikutnya.

Add Roles and Features Wizard



Select features

DESTINATION SERVER

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more features to install on the selected server.

Features

- ☐ Remote Differential Compression
- ☒ Remote Server Administration Tools
 - ☐ Feature Administration Tools
 - ☒ Role Administration Tools
 - ☒ AD DS and AD LDS Tools
 - ☒ Active Directory module for Windows PowerShell
 - ☒ AD DS Tools
 - ☒ AD LDS Snap-Ins and Command-Line Tools
 - ☐ Hyper-V Management Tools
 - ☐ Remote Desktop Services Tools
 - ☐ Windows Server Update Services Tools
 - ☐ Active Directory Certificate Services Tools
 - ☐ Active Directory Rights Management Services
 - ☐ DHCP Server Tools
 - ☒ DNS Server Tools
 - ☐ Fax Server Tools
 - ☐ File Services Tools
 - ☐ Network Controller Management Tools
 - ☐ Network Policy and Access Services Tools

Description

Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.

< Previous

Next >

Install

Cancel

12. Tinjau informasi dan pilih Instal. Ketika instalasi fitur selesai, Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools tersedia dari menu Start di folder Administrative Tools.

Membuat pengguna AD Sederhana

Gunakan prosedur berikut untuk membuat pengguna dengan EC2 instans Amazon yang digabungkan ke direktori Simple AD Anda. Sebelum Anda dapat membuat pengguna, Anda harus menyelesaikan prosedur di [Instalasi Alat Administrasi Direktori Aktif](#).

Note

Saat menggunakan Simple AD, jika Anda membuat akun pengguna pada instans Linux dengan opsi “Paksa pengguna untuk mengubah kata sandi saat login pertama,” pengguna tersebut tidak akan dapat mengubah kata sandi mereka menggunakan kpasswd. Untuk

mengubah kata sandi pertama kalinya, administrator domain harus memperbarui sandi pengguna menggunakan Alat Pengelolaan Direktori Aktif.

Untuk membuat pengguna

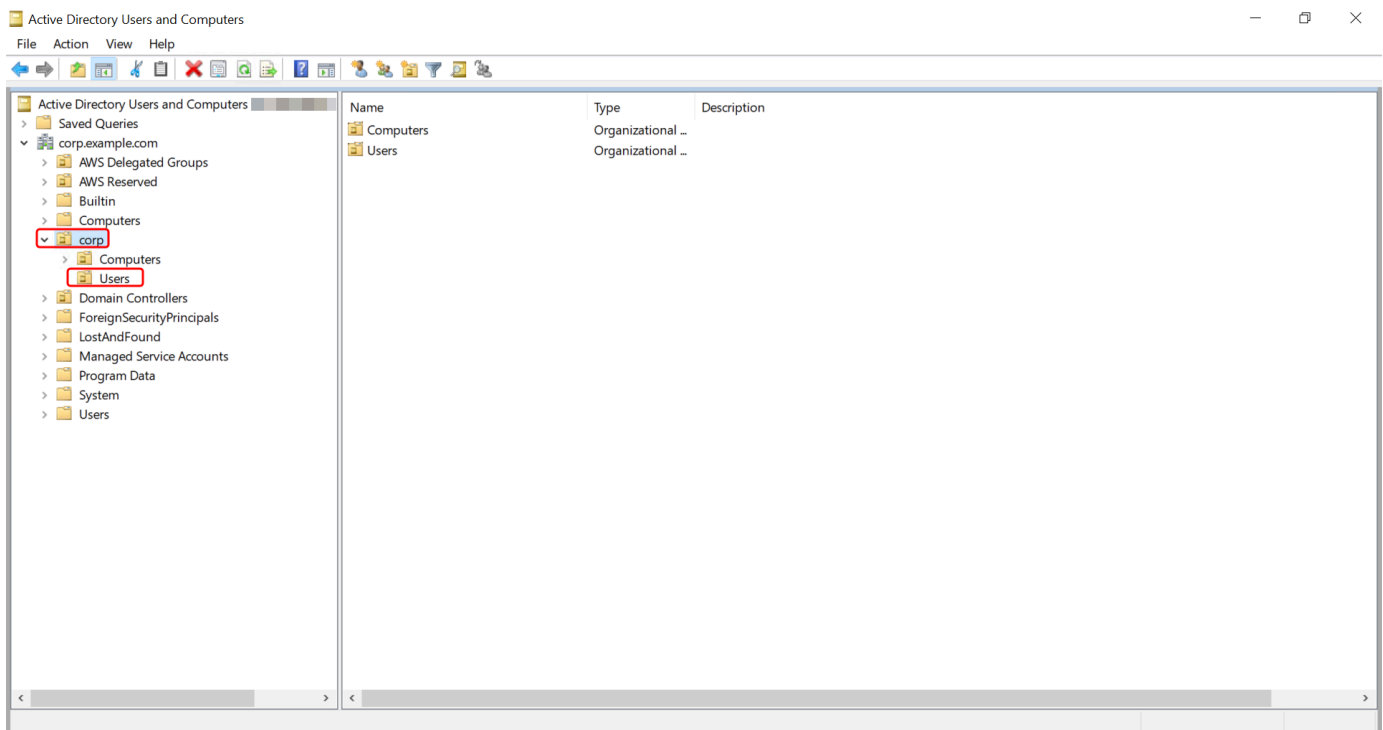
1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif dari menu Start Windows. Ada pintasan ke alat ini yang ditemukan di folder Alat Administratif Windows.

Tip

Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.

```
%SystemRoot%\system32\dsa.msc
```

3. Di pohon direktori, pilih OU di bawah nama NetBIOS direktori Anda OU di mana Anda ingin menyimpan pengguna Anda (misalnya, **corp\Users**). Untuk informasi lebih lanjut tentang struktur OU yang digunakan oleh direktori di AWS, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).



4. Pada menu Tindakan, pilih Baru, lalu pilih Pengguna untuk membuka wizard pengguna baru.
5. Pada halaman pertama wizard, masukkan nilai untuk bidang berikut, lalu pilih Berikutnya.
 - Nama depan
 - Nama belakang
 - Nama logon pengguna
6. Pada halaman kedua wizard, masukkan kata sandi sementara di Kata Sandi dan Konfirmasi Kata Sandi. Pastikan pilihan Pengguna harus mengubah kata sandi pada proses masuk berikutnya dipilih. Tidak satu pun dari pilihan lain harus dipilih. Pilih Berikutnya.
7. Pada halaman ketiga wizard, verifikasi bahwa informasi pengguna baru sudah benar dan pilih Selesai. Pengguna baru akan muncul di folder Pengguna.

Menghapus pengguna Simple AD

Gunakan prosedur berikut untuk menghapus pengguna dengan instans Amazon EC2 Windows yang digabungkan ke direktori Simple AD Anda.

Untuk menghapus kluster

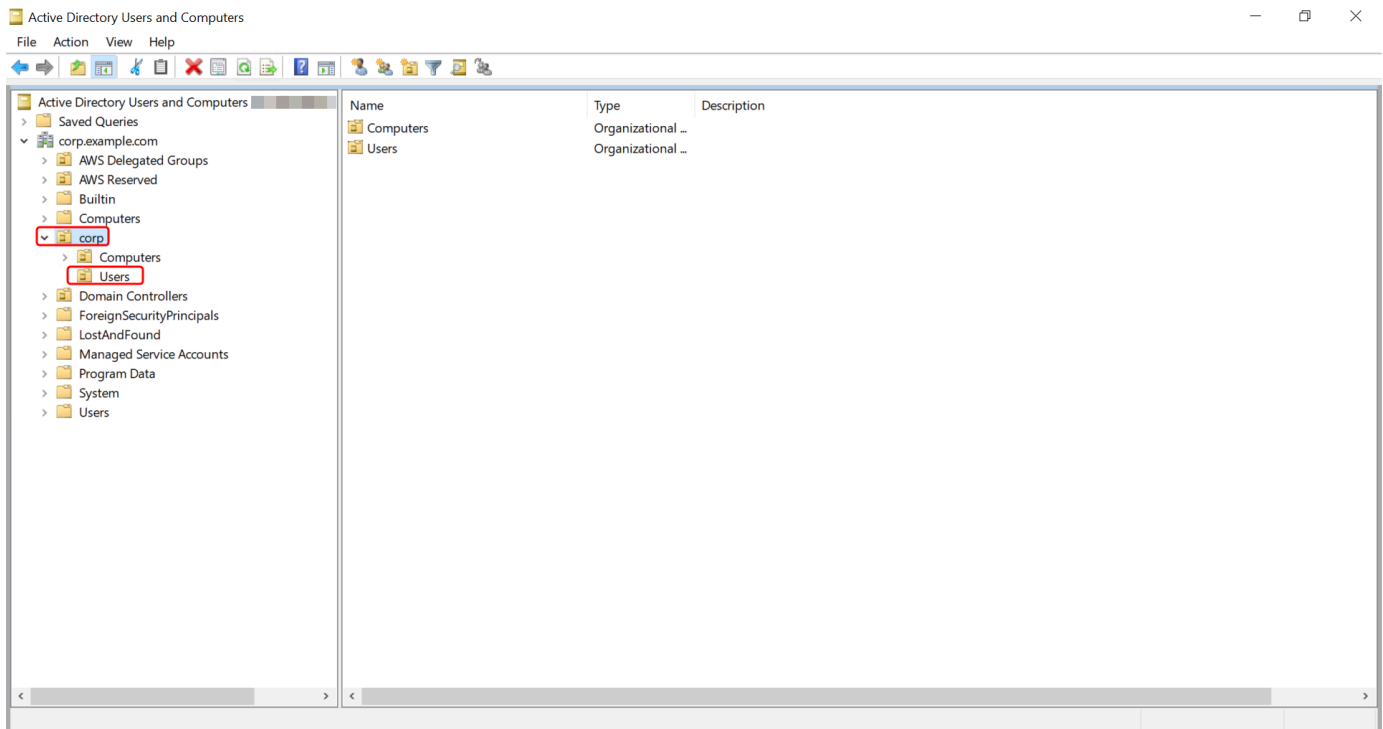
1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif dari menu Start Windows. Ada pintasan ke alat ini yang ditemukan di folder Alat Administratif Windows.

Tip

Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.

```
%SystemRoot%\system32\dsa.msc
```

3. Di pohon direktori, pilih OU yang berisi pengguna yang ingin Anda hapus (misalnya, **corp \Users**).



4. Pilih pengguna yang ingin Anda hapus. Pada menu Tindakan, pilih Hapus.
5. Kotak dialog akan muncul meminta Anda untuk mengonfirmasi bahwa Anda ingin menghapus pengguna. Pilih Ya untuk menghapus pengguna. Ini menghapus pengguna yang dipilih secara permanen.

Menyetel ulang kata sandi pengguna Simple AD

Pengguna harus mematuhi kebijakan kata sandi sebagaimana didefinisikan dalam Direktori Aktif. Terkadang ini bisa mendapatkan yang terbaik dari pengguna, termasuk administrator Direktori Aktif, dan mereka lupa kata sandi mereka. Ketika ini terjadi, Anda dapat dengan cepat mengatur ulang kata sandi pengguna menggunakan Directory Service jika pengguna berada di Simple AD.

Anda harus masuk sebagai pengguna dengan izin yang diperlukan untuk mengatur ulang kata sandi. Untuk informasi selengkapnya tentang izin, lihat [Ikhtisar mengelola izin akses ke sumber daya Anda Directory Service](#).

Anda dapat mengatur ulang kata sandi untuk setiap pengguna di Direktori Aktif Anda dengan pengecualian berikut:

- Anda dapat mengatur ulang kata sandi untuk setiap pengguna dalam Unit Organisasi (OU) yang didasarkan dari nama NetBIOS yang Anda gunakan saat Anda membuat Direktori Aktif Anda.

Misalnya, jika Anda mengikuti prosedur di [Buat Simple AD Anda](#), nama NetBIOS Anda akan menjadi CORP dan kata sandi pengguna yang dapat Anda atur ulang akan menjadi anggota OU. Corp/Users

- Anda tidak dapat mengatur ulang kata sandi pengguna mana pun di luar OU yang didasarkan pada nama NetBIOS yang Anda gunakan saat membuat Direktori Aktif Anda. Untuk informasi selengkapnya tentang struktur OU untuk Simple AD, lihat [Apa yang dibuat dengan Simple AD Anda](#).
- Anda tidak dapat mengatur ulang kata sandi untuk pengguna mana pun yang merupakan anggota dari dua domain. Anda juga tidak dapat mengatur ulang kata sandi pengguna mana pun yang merupakan anggota dari grup Admin Domain atau Admin Perusahaan kecuali untuk pengguna Administrator.
- Anda tidak dapat mengatur ulang kata sandi untuk pengguna mana pun yang merupakan anggota dari grup Admin Domain atau Admin Perusahaan kecuali untuk pengguna administrator.

Anda dapat menggunakan salah satu metode berikut untuk mengatur ulang kata sandi pengguna:

- Konsol Manajemen AWS
- AWS CLI

Konsol Manajemen AWS

1. Di panel navigasi [Directory Service konsol](#), di bawah Direktori Aktif, pilih Direktori, lalu pilih Direktori Aktif dalam daftar tempat Anda ingin mengatur ulang kata sandi pengguna.
2. Pada halaman Detail direktori, pilih Tindakan, lalu pilih Setel ulang kata sandi pengguna.
3. Dalam dialog Reset kata sandi pengguna, di Nama pengguna ketikkan nama pengguna pengguna yang kata sandinya perlu diubah.
4. Ketik kata sandi di Kata sandi baru dan Konfirmasi kata sandi, lalu pilih Atur ulang sandi.

AWS CLI

1. Untuk menginstal AWS CLI, lihat [Menginstal atau memperbarui versi terbaru dari file AWS CLI](#).
2. Buka AWS CLI.
3. Ketik perintah berikut dan ganti ID Direktori, nama pengguna **jane.doe**, dan kata sandi **P@ssw0rd** dengan ID Direktori Direktori Aktif dan kredensial yang diinginkan. Lihat [reset-user-password](#) di Referensi AWS CLI Perintah untuk informasi lebih lanjut.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

Membuat grup AD Sederhana

Gunakan prosedur berikut untuk membuat grup keamanan dengan EC2 instans Amazon yang digabungkan ke direktori Simple AD Anda. Sebelum Anda dapat membuat grup keamanan, Anda harus menyelesaikan prosedur di [Menginstal Alat Administrasi Direktori Aktif](#).

Untuk membuat grup

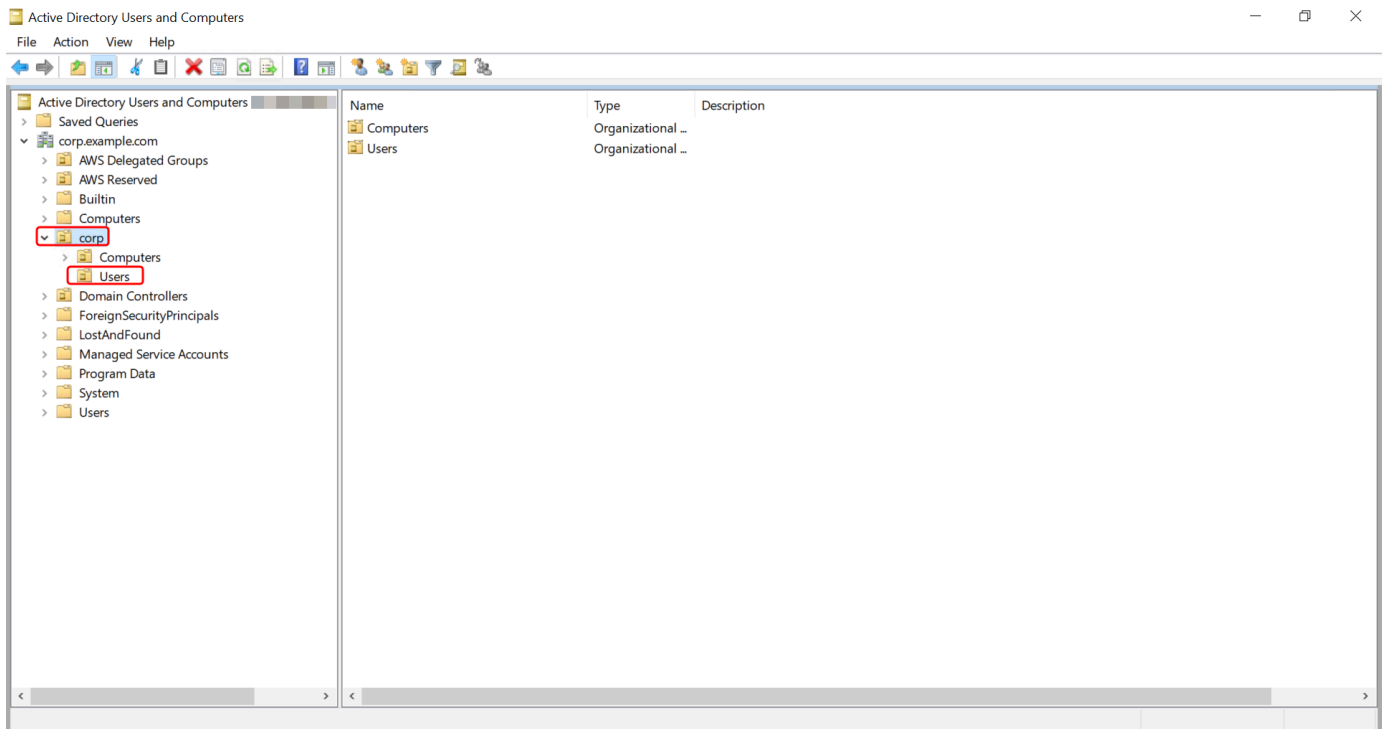
1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif. Ada jalan pintas untuk alat ini di folder Alat Administratif.

Tip

Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.

```
%SystemRoot%\system32\dsa.msc
```

3. Pada pohon direktori, pilih OU di bawah direktori OU nama NetBIOS Anda di mana Anda ingin menyimpan grup Anda (misalnya, Corp\Users). Untuk informasi lebih lanjut tentang struktur OU yang digunakan oleh direktori di AWS, lihat [Apa yang dibuat dengan Microsoft AD yang AWS Dikelola](#).



4. Pada menu Tindakan, klik Baru, dan kemudian klik Grup untuk membuka wizard grup baru.
5. Ketik nama untuk grup di Nama grup, pilih Lingkup grup yang memenuhi kebutuhan Anda, dan pilih Keamanan untuk jenis Grup. Untuk informasi selengkapnya tentang lingkup grup Active Directory dan grup keamanan, lihat [Grup keamanan Active Directory](#) di dokumentasi Microsoft Windows Server.
6. Klik OK. Grup keamanan baru akan muncul di folder Pengguna.

Menambahkan pengguna Simple AD ke grup

Gunakan prosedur berikut untuk menambahkan pengguna ke grup keamanan dengan EC2 instance yang digabungkan ke direktori Simple AD Anda.

Untuk menambahkan pengguna ke grup

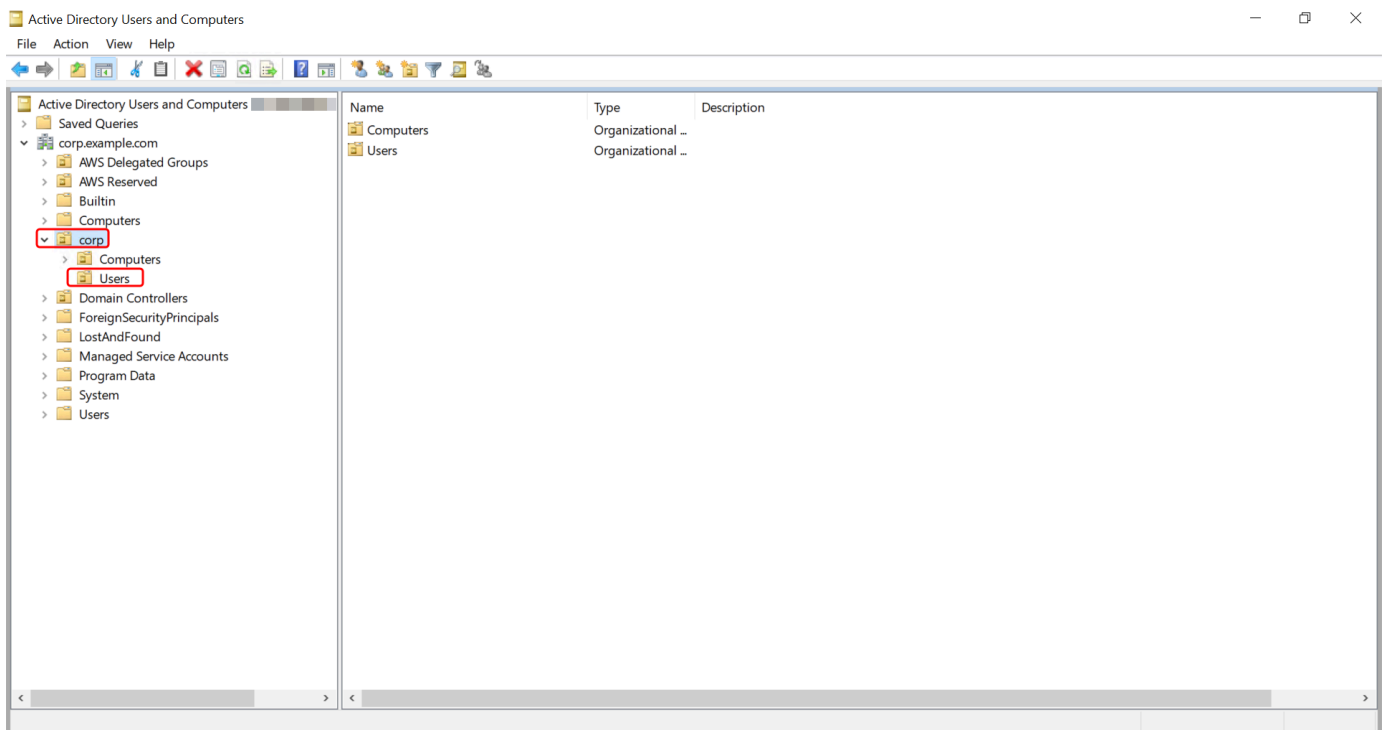
1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif. Ada jalan pintas untuk alat ini di folder Alat Administratif.

Tip

Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.

```
%SystemRoot%\system32\dsa.msc
```

3. Pada pohon direktori, pilih OU di bawah direktori Anda NetBIOS nama OU di mana Anda disimpan grup Anda, dan pilih grup yang Anda ingin tambahkan pengguna sebagai anggota.



4. Pada menu Tindakan, klik Properti untuk membuka kotak dialog properti untuk grup.
5. Pilih tab Anggota dan klik Tambahkan.
6. Untuk Masukkan nama objek yang akan dipilih, ketik nama pengguna yang ingin Anda tambahkan dan klik OK. Nama akan ditampilkan dalam daftar Anggota. Klik OK lagi untuk memperbarui keanggotaan grup.
7. Verifikasikan bahwa pengguna tersebut sekarang adalah anggota grup dengan memilih pengguna di folder Pengguna dan klik Properti di menu Tindakan untuk membuka kotak dialog properti. Pilih tab Anggota dari. Anda harus melihat nama grup dalam daftar grup yang dimiliki pengguna.

Kuota Simple AD

Umumnya, Anda tidak harus menambahkan lebih dari 500 pengguna ke direktori Simple AD Small dan tidak lebih dari 5.000 pengguna ke direktori AD sederhana Large. Untuk opsi penskalaan yang lebih fleksibel dan fitur Active Directory tambahan, pertimbangkan untuk menggunakan AWS Directory Service untuk Microsoft Active Directory (Edisi Standar atau Edisi Perusahaan) sebagai gantinya.

Berikut ini adalah kuota default untuk Simple AD. Kecuali dinyatakan lain, masing-masing kuota adalah per Region.

Kuota Simple AD

Sumber daya	Kuota default
Direktori Simple AD	10
Snapshot manual *	5 per Simple AD

* Kuota snapshot manual tidak dapat diubah.

Note

Anda tidak dapat melampirkan alamat IP publik ke AWS elastic network interface (ENI) Anda.

Pemecahan masalah Simple AD

Berikut ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temui saat membuat atau menggunakan Simple AD Active Directory.

Topik

- [Pemulihan kata sandi](#)
- [Saya menerima kesalahan 'KDC tidak dapat memenuhi opsi yang diminta' saat menambahkan pengguna ke Simple AD](#)
- [Saya tidak dapat memperbarui nama DNS atau alamat IP instans bergabung ke domain saya \(pembaruan dinamis DNS\).](#)

- [Saya tidak bisa masuk ke SQL Server menggunakan akun SQL Server](#)
- [Simple AD saya macet dalam status 'Diminta'](#)
- [Saya menerima kesalahan 'AZ terkendali' saat membuat Simple AD](#)
- [Beberapa pengguna saya tidak dapat mengautentikasi dengan Simple AD saya](#)
- [Sumber daya tambahan](#)
- [Memecahkan masalah Pesan status direktori Simple AD](#)

Pemulihan kata sandi

Jika pengguna lupa kata sandi atau mengalami masalah saat masuk ke direktori Simple AD Anda, Anda dapat mengatur ulang kata sandi mereka menggunakan Konsol Manajemen AWS, PowerShell atau AWS CLI

Untuk informasi selengkapnya, lihat [Menyetel ulang kata sandi pengguna Simple AD](#).

Saya menerima kesalahan 'KDC tidak dapat memenuhi opsi yang diminta' saat menambahkan pengguna ke Simple AD

Ini dapat terjadi ketika klien CLI Samba tidak mengirim perintah dengan benar ke semua net pengontrol domain. Jika Anda melihat pesan galat ini saat menggunakan `net ads` perintah untuk menambahkan pengguna ke direktori Simple AD Anda, gunakan `-S` argumen dan tentukan alamat IP salah satu pengontrol domain Anda. Jika Anda masih melihat kesalahan, coba pengendali domain lainnya. Anda juga dapat menggunakan Alat Administrasi Direktori Aktif untuk menambahkan pengguna ke direktori Anda. Untuk informasi selengkapnya, lihat [Menginstal Alat Administrasi Direktori Aktif untuk Simple AD](#).

Saya tidak dapat memperbarui nama DNS atau alamat IP instans bergabung ke domain saya (pembaruan dinamis DNS).

Pembaruan dinamis DNS tidak didukung di domain Simple AD. Sebagai gantinya Anda dapat membuat perubahan secara langsung dengan menghubungkan ke direktori Anda menggunakan Pengelola DNS pada instans yang digabungkan ke domain Anda.

Saya tidak bisa masuk ke SQL Server menggunakan akun SQL Server

Anda mungkin menerima kesalahan jika mencoba menggunakan SQL Server Management Studio (SSMS) dengan akun SQL Server untuk masuk ke SQL Server yang berjalan pada instans

Amazon EC2 2012 Windows R2. Masalah terjadi ketika SSMS berjalan sebagai pengguna domain dan dapat mengakibatkan kesalahan `Login failed for user`, bahkan ketika kredensi yang valid disediakan. Ini adalah masalah yang diketahui dan AWS secara aktif bekerja untuk menyelesaikannya.

Untuk mengatasi masalah ini, Anda dapat masuk ke SQL Server dengan Windows Authentication, bukan SQL Authentication. Atau luncurkan SSMS sebagai pengguna lokal, bukan pengguna domain Simple AD.

Simple AD saya macet dalam status 'Diminta'

Jika Anda memiliki Simple AD yang telah berada dalam `Requested` status selama lebih dari lima menit, coba hapus direktori dan buat ulang. Jika masalah ini berlanjut, kontak [Pusat AWS Dukungan](#).

Saya menerima kesalahan 'AZ terkendali' saat membuat Simple AD

Beberapa AWS akun yang dibuat sebelum 2012 mungkin memiliki akses ke Availability Zones di AS Timur (Virginia N.), AS Barat (California N.), atau Wilayah Asia Pasifik (Tokyo) yang tidak mendukung Directory Service direktori. Jika Anda menerima kesalahan seperti ini saat membuat direktori, pilih subnet di Availability Zone yang berbeda dan coba untuk membuat direktori lagi.

Beberapa pengguna saya tidak dapat mengautentikasi dengan Simple AD saya

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Ini adalah pengaturan default untuk akun pengguna baru, dan seharusnya tidak diubah. Untuk informasi selengkapnya tentang pengaturan ini, buka [Preauthentication](#) on Simple AD. TechNet

Sumber daya tambahan

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengannya. AWS

- [AWS Pusat Pengetahuan](#) —Temukan FAQs dan tautkan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- [AWS Support Center](#) —Dapatkan dukungan teknis.
- [AWS Pusat Support Premium](#) —Dapatkan dukungan teknis premium.

Topik

- [Memecahkan masalah Pesan status direktori Simple AD](#)

Memecahkan masalah Pesan status direktori Simple AD

Ketika Simple AD terganggu atau tidak dapat dioperasikan, pesan status direktori berisi informasi tambahan. Pesan status ditampilkan di Directory Service konsol, atau ditampilkan di [DirectoryDescription.StageReason](#) anggota oleh [DescribeDirectories](#) API. Untuk informasi selengkapnya tentang status direktori, lihat [Memahami status direktori Microsoft AD yang AWS Dikelola](#).

Berikut ini adalah pesan status untuk direktori Simple AD:

Topik

- [Antarmuka jaringan elastis layanan direktori tidak terpasang](#)
- [Masalah terdeteksi oleh instans](#)
- [Pengguna Directory Service cadangan kritis hilang dari direktori](#)
- [Pengguna Directory Service cadangan kritis harus menjadi bagian dari grup Admin Domain](#)
- [Pengguna Directory Service cadangan kritis dinonaktifkan](#)
- [Pengendali domain utama tidak memiliki semua peran FSMO](#)
- [Kegagalan replikasi pengendali domain](#)

Antarmuka jaringan elastis layanan direktori tidak terpasang

Deskripsi

Critical elastic network interface (ENI) yang dibuat atas nama Anda selama pembuatan direktori untuk membangun konektivitas jaringan dengan VPC Anda tidak dilampirkan ke instance direktori. AWS aplikasi yang didukung oleh direktori ini tidak akan berfungsi. Direktori Anda tidak dapat terhubung ke jaringan on-premise Anda.

Pemecahan masalah

Jika ENI terlepas tapi masih ada, hubungi Dukungan. Jika ENI dihapus, tidak ada cara untuk menyelesaikan masalah tersebut dan direktori Anda secara permanen tidak dapat digunakan. Anda harus menghapus direktori tersebut dan membuat direktori baru.

Masalah terdeteksi oleh instans

Deskripsi

Kesalahan internal terdeteksi oleh instans. Hal ini biasanya menandakan bahwa layanan pemantauan mencoba untuk memulihkan secara aktif instans yang terganggu.

Pemecahan masalah

Dalam kebanyakan kasus, ini adalah masalah sementara, dan direktori akhirnya kembali ke keadaan Aktif. Jika masalah berlanjut, hubungi Dukungan untuk bantuan lebih lanjut.

Pengguna Directory Service cadangan kritis hilang dari direktori

Deskripsi

Saat Simple AD dibuat, Directory Service buat akun layanan di direktori dengan nama `AWSAdminD-xxxxxxxxxx`. Kesalahan ini diterima saat akun layanan ini tidak dapat ditemukan. Tanpa akun ini, Directory Service tidak dapat melakukan fungsi administratif pada direktori, rendering direktori tidak dapat digunakan.

Pemecahan masalah

Untuk memperbaiki masalah ini, pulihkan direktori ke snapshot sebelumnya yang dibuat sebelum akun layanan dihapus. Snapshot otomatis diambil dari direktori Simple AD Anda satu kali sehari. Jika sudah lebih dari lima hari setelah akun ini dihapus, Anda mungkin tidak dapat memulihkan direktori ke keadaan di mana akun ini berada. Jika Anda tidak dapat memulihkan direktori dari snapshot di mana akun ini berada, direktori Anda mungkin menjadi tidak dapat digunakan secara permanen. Jika ini adalah kasusnya, Anda harus menghapus direktori Anda dan membuat direktori baru.

Pengguna Directory Service cadangan kritis harus menjadi bagian dari grup Admin Domain

Deskripsi

Saat Simple AD dibuat, Directory Service buat akun layanan di direktori dengan nama `AWSAdminD-xxxxxxxxxx`. Kesalahan ini diterima saat akun layanan ini bukan anggota dari grup Domain Admins. Keanggotaan dalam grup ini diperlukan untuk memberikan Directory

Service hak istimewa yang dibutuhkan untuk melakukan operasi pemeliharaan dan pemulihan, seperti mentransfer peran FSMO, domain bergabung dengan pengontrol direktori baru, dan memulihkan dari snapshot.

Pemecahan masalah

Menggunakan alat Pengguna dan Komputer Direktori Aktif untuk menambahkan akun layanan ke grup Domain Admins.

Pengguna Directory Service cadangan kritis dinonaktifkan

Deskripsi

Saat Simple AD dibuat, Directory Service buat akun layanan di direktori dengan nama `AWSAdminD-xxxxxxxxxx`. Kesalahan ini diterima saat akun layanan ini dinonaktifkan. Akun ini harus diaktifkan sehingga Directory Service dapat melakukan operasi pemeliharaan dan pemulihan pada direktori.

Pemecahan masalah

Menggunakan alat Pengguna dan Komputer Direktori Aktif untuk mengaktifkan kembali akun layanan.

Pengendali domain utama tidak memiliki semua peran FSMO

Deskripsi

Semua peran FSMO tidak dimiliki oleh pengendali direktori Simple AD. Directory Service tidak dapat menjamin perilaku tertentu dan fungsi jika peran FSMO tidak milik pengendali direktori Simple AD yang benar.

Pemecahan masalah

Menggunakan alat Direktori Aktif untuk memindahkan peran FSMO kembali ke pengendali direktori kerja asli. Untuk informasi lebih lanjut tentang memindahkan peran FSMO, buka <https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer--or-seize-fsmo-roles>. in-ad-ds
Jika ini tidak memperbaiki masalah, silakan hubungi Dukungan untuk bantuan lebih lanjut.

Kegagalan replikasi pengendali domain

Deskripsi

Pengendali direktori Simple AD gagal untuk mereplikasi dengan satu sama lain. Hal ini dapat disebabkan oleh satu atau beberapa masalah berikut:

- Grup keamanan untuk pengendali direktori tidak memiliki port-port yang benar terbuka.
- Jaringan ACLs terlalu ketat.
- Tabel rute VPC tidak merutekan lalu lintas jaringan antara pengendali direktori dengan benar.
- Instans lain telah dipromosikan ke pengendali domain di direktori.

Pemecahan masalah

Untuk informasi selengkapnya tentang persyaratan jaringan VPC Anda, lihat salah satu [AWS Dikelola Microsoft AD](#) [Prasyarat untuk membuat iklan Microsoft yang Dikelola AWS](#), [AD Connector](#) [Prasyarat AD Connector](#), atau Simple AD [Prasyarat Simple AD](#). Jika ada pengendali domain yang tidak dikenal di direktori Anda, Anda harus menurunkannya. Jika pengaturan jaringan VPC Anda benar, tetapi kesalahan tetap ada, silakan hubungi Dukungan untuk mendapatkan bantuan lebih lanjut.

Keamanan di AWS Directory Service

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](#) menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di 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 berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku AWS Directory Service, lihat [AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan](#).
- **Keamanan di cloud** — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Directory Service. Topik berikut menunjukkan cara mengonfigurasi Directory Service untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan Directory Service sumber daya Anda.

Topik keamanan

Topik keamanan berikut dapat ditemukan di bagian ini:

- [Identitas dan manajemen akses untuk Directory Service](#)
- [Penebangan dan pemantauan di AWS Directory Service](#)
- [Validasi kepatuhan untuk AWS Directory Service](#)
- [Ketahanan di AWS Directory Service](#)
- [Keamanan infrastruktur di AWS Directory Service](#)

Topik keamanan tambahan

Topik keamanan tambahan berikut dapat ditemukan dalam panduan ini:

Akun, perwalian, dan akses AWS sumber daya

- [AWS Akun Administrator Microsoft AD yang dikelola dan izin grup](#)
- [Akun Layanan yang Dikelola Grup](#)
- [Membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan AD yang dikelola sendiri](#)
- [Delegasi terbatas Kerberos](#)
- [Memberikan pengguna dan grup Microsoft AD AWS Terkelola akses ke AWS sumber daya dengan peran IAM](#)
- [Otorisasi untuk AWS aplikasi dan layanan menggunakan Directory Service](#)

Amankan direktori Anda

- [Amankan Microsoft AD yang AWS Dikelola](#)
- [Mengamankan direktori AD Connector Anda](#)

Pencatatan dan pemantauan

- [Pantau iklan Microsoft yang AWS Dikelola](#)
- [Memantau direktori AD Connector Anda](#)

Ketahanan

- [Penambalan dan pemeliharaan untuk Microsoft AD yang AWS Dikelola](#)

Identitas dan manajemen akses untuk Directory Service

Akses ke Directory Service memerlukan kredensial yang AWS dapat digunakan untuk mengautentikasi permintaan Anda. Kredensial tersebut harus memiliki izin untuk mengakses AWS sumber daya, seperti direktori. Directory Service Bagian berikut memberikan rincian tentang bagaimana Anda dapat menggunakan [AWS Identity and Access Management \(IAM\)](#) dan Directory Service untuk membantu mengamankan sumber daya Anda dengan mengontrol siapa yang dapat mengaksesnya:

- [Autentikasi](#)
- [Kontrol akses](#)

Autentikasi

Pelajari cara mengakses AWS menggunakan [identitas IAM](#).

Kontrol akses

Anda dapat memiliki kredensi yang valid untuk mengautentikasi permintaan Anda, tetapi kecuali Anda memiliki izin, Anda tidak dapat membuat atau mengakses sumber daya. Directory Service Misalnya, Anda harus memiliki izin untuk membuat Directory Service direktori atau membuat snapshot direktori.

Bagian berikut menjelaskan cara mengelola izin untuk Directory Service. Anda sebaiknya membaca gambaran umum terlebih dahulu.

- [Ikhtisar mengelola izin akses ke sumber daya Anda Directory Service](#)
- [Menggunakan kebijakan berbasis identitas \(kebijakan IAM\) untuk Directory Service](#)
- [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#)

Ikhtisar mengelola izin akses ke sumber daya Anda Directory Service

Setiap AWS sumber daya dimiliki oleh AWS akun. Akibatnya, izin untuk membuat atau mengakses sumber daya diatur oleh kebijakan izin. Namun, administrator akun, yang merupakan pengguna dengan izin administrator, dapat melampirkan izin ke sumber daya. Ini juga memiliki kemampuan untuk melampirkan kebijakan izin ke identitas IAM, seperti pengguna, grup, dan peran, dan beberapa layanan, seperti AWS Lambda juga mendukung melampirkan kebijakan izin ke sumber daya.

Note

Untuk informasi tentang peran administrator akun, lihat [Praktik terbaik IAM](#) di Panduan Pengguna IAM.

Topik

- [Directory Service sumber daya dan operasi](#)
- [Memahami kepemilikan sumber daya](#)
- [Mengelola akses ke sumber daya](#)
- [Menentukan elemen kebijakan: Tindakan, efek, sumber daya, dan principal](#)
- [Menentukan kondisi dalam kebijakan](#)

Directory Service sumber daya dan operasi

Di Directory Service, sumber daya utama adalah direktori. Karena Directory Service mendukung sumber daya snapshot direktori, Anda dapat membuat snapshot hanya dalam konteks direktori yang ada. Snapshot ini disebut sebagai subresource.

Sumber daya ini memiliki Nama Sumber Daya Amazon (ARNs) unik yang terkait dengannya seperti yang ditunjukkan pada tabel berikut.

Jenis Sumber Daya	Format ARN
Direktori	arn:aws:ds: <i>region</i> : <i>account-id</i> :directory/ <i>external-directory-id</i>
Snapshot	arn:aws:ds: <i>region</i> : <i>account-id</i> :snapshot/ <i>external-snapshot-id</i>

Directory Service mencakup dua ruang nama layanan berdasarkan jenis operasi yang Anda lakukan.

- Namespace ds layanan menyediakan serangkaian operasi untuk bekerja dengan sumber daya yang sesuai. Untuk daftar operasi yang tersedia, lihat [Tindakan Directory Service](#).
- Namespace ds-data layanan menyediakan satu set operasi ke objek Active Directory. Untuk mengetahui daftar operasi yang tersedia, lihat [Referensi API Directory Service Data](#).

Memahami kepemilikan sumber daya

Pemilik sumber daya adalah AWS akun yang membuat sumber daya. Artinya, pemilik sumber daya adalah AWS akun entitas utama (akun root, pengguna IAM, atau peran IAM) yang mengautentikasi permintaan yang membuat sumber daya. Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredensi akun root AWS akun Anda untuk membuat Directory Service sumber daya, seperti direktori, AWS akun Anda adalah pemilik sumber daya tersebut.
- Jika Anda membuat pengguna IAM di AWS akun Anda dan memberikan izin untuk membuat Directory Service sumber daya kepada pengguna tersebut, pengguna juga dapat membuat Directory Service sumber daya. Namun, AWS akun Anda, tempat pengguna berada, memiliki sumber daya.
- Jika Anda membuat peran IAM di AWS akun Anda dengan izin untuk membuat Directory Service sumber daya, siapa pun yang dapat mengambil peran tersebut dapat membuat Directory Service sumber daya. AWS Akun Anda, tempat peran itu berada, memiliki Directory Service sumber daya.

Mengelola akses ke sumber daya

Kebijakan izin menjelaskan siapa yang memiliki akses ke suatu objek. Bagian berikut menjelaskan opsi yang tersedia untuk membuat kebijakan izin.

Note

Bagian ini membahas penggunaan IAM dalam konteks. Directory Service Bagian ini tidak memberikan informasi yang mendetail tentang layanan IAM. Untuk dokumentasi lengkap IAM, lihat [Apa yang Dimaksud dengan IAM?](#) dalam Panduan Pengguna IAM. Untuk informasi tentang sintaksis dan penjelasan kebijakan IAM, lihat [Referensi Kebijakan IAM JSON](#) dalam Panduan Pengguna IAM.

Kebijakan yang melekat pada identitas IAM disebut sebagai kebijakan berbasis identitas (kebijakan IAM) dan kebijakan yang melekat pada sumber daya disebut sebagai kebijakan berbasis sumber daya. Directory Service hanya mendukung kebijakan berbasis identitas (kebijakan IAM).

Topik

- [Kebijakan berbasis identitas \(kebijakan IAM\)](#)
- [Kebijakan berbasis sumber daya](#)

Kebijakan berbasis identitas (kebijakan IAM)

Anda dapat melampirkan kebijakan ke identitas IAM Anda. Misalnya, Anda dapat melakukan hal berikut:

- Lampirkan kebijakan izin ke pengguna atau grup di akun Anda — Administrator akun dapat menggunakan kebijakan izin yang dikaitkan dengan pengguna tertentu untuk memberikan izin bagi pengguna tersebut untuk membuat Directory Service sumber daya, seperti direktori baru.
- Melampirkan kebijakan izin pada peran (memberikan izin lintas akun) – Anda dapat melampirkan kebijakan izin berbasis identitas ke peran IAM untuk memberikan izin lintas akun.

Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mendelegasikan izin, lihat [Manajemen Akses](#) dalam Panduan Pengguna IAM.

Kebijakan izin berikut memberikan izin kepada pengguna untuk menjalankan semua tindakan yang dimulai dengan `Describe`. Tindakan ini menampilkan informasi tentang Directory Service sumber daya, seperti direktori atau snapshot. Perhatikan bahwa karakter wildcard (*) dalam `Resource` elemen menunjukkan bahwa tindakan diizinkan untuk semua Directory Service sumber daya yang dimiliki oleh akun.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "*"
    }
  ]
}
```

Untuk informasi selengkapnya tentang menggunakan kebijakan berbasis identitas dengan Directory Service, lihat [Menggunakan kebijakan berbasis identitas \(kebijakan IAM\) untuk Directory Service](#)

Untuk informasi lebih lanjut tentang pengguna, kelompok, peran, dan izin, lihat [Identitas \(Pengguna, Grup, dan Peran\)](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Layanan lain, seperti Amazon S3, juga mendukung kebijakan izin berbasis sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket S3 untuk mengelola izin akses ke bucket tersebut. Directory Service tidak mendukung kebijakan berbasis sumber daya.

Menentukan elemen kebijakan: Tindakan, efek, sumber daya, dan principal

Untuk setiap Directory Service sumber daya, layanan mendefinisikan satu set operasi API. Untuk informasi selengkapnya, lihat [Directory Service sumber daya dan operasi](#). Untuk daftar operasi API yang tersedia, lihat [Tindakan Directory Service](#).

Untuk memberikan izin untuk operasi API ini, Directory Service tentukan serangkaian tindakan yang dapat Anda tentukan dalam kebijakan. Perhatikan bahwa melakukan operasi API bisa memerlukan izin untuk lebih dari satu tindakan.

Berikut ini adalah elemen-elemen kebijakan dasar:

- **Sumber Daya** - Dalam kebijakan, Anda menggunakan Amazon Resource Name (ARN) untuk mengidentifikasi sumber daya yang menerapkan kebijakan tersebut. Untuk Directory Service sumber daya, Anda selalu menggunakan karakter wildcard (*) dalam kebijakan IAM. Untuk informasi selengkapnya, lihat [Directory Service sumber daya dan operasi](#).
- **Tindakan** – Anda menggunakan kata kunci tindakan untuk mengidentifikasi operasi sumber daya yang ingin Anda izinkan atau tolak. Misalnya, izin `ds:DescribeDirectories` memungkinkan pengguna untuk melakukan Directory Service `DescribeDirectories` operasi.
- **Pengaruh** – Anda menentukan pengaruh saat pengguna meminta tindakan tertentu. Hal ini bisa berupa mengizinkan atau menolak. Jika Anda tidak secara eksplisit memberikan akses untuk (mengizinkan) sumber daya, akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat mengaksesnya, meskipun kebijakan yang berbeda memberikan akses.
- **Principal** – Dalam kebijakan berbasis identitas (Kebijakan IAM), pengguna yang kebijakannya terlampir adalah principal yang implisit. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang ingin Anda terima izin (hanya berlaku untuk kebijakan berbasis sumber daya). Directory Service tidak mendukung kebijakan berbasis sumber daya.

Untuk mempelajari sintaksis dan penjelasan kebijakan IAM selengkapnya, lihat [Referensi Kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Untuk tabel yang menunjukkan semua tindakan Directory Service API dan sumber daya yang diterapkan, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#).

Menentukan kondisi dalam kebijakan

Ketika Anda memberikan izin, Anda dapat menggunakan bahasa kebijakan akses untuk menentukan syarat kapan kebijakan akan berlaku. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu. Untuk informasi selengkapnya tentang menentukan kondisi dalam bahasa kebijakan, lihat [Kondisi](#) dalam Panduan Pengguna IAM.

Untuk menyatakan kondisi, Anda menggunakan kunci kondisi standar. Tidak ada kunci syarat khusus untuk Directory Service. Namun, ada tombol AWS kondisi yang dapat Anda gunakan sesuai kebutuhan. Untuk daftar lengkap AWS kunci, lihat [Kunci kondisi global yang tersedia](#) di Panduan Pengguna IAM.

AWS kebijakan terkelola untuk AWS Directory Service

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

Bagian berikut menjelaskan kebijakan AWS terkelola yang khusus untuk Directory Service. Anda dapat melampirkan kebijakan ini ke pengguna di akun Anda.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSDirectoryServiceFullAccess

Anda dapat melampirkan kebijakan AWSDirectoryServiceFullAccess ke identitas IAM Anda. Untuk melihat izin lengkap untuk kebijakan ini, lihat [AWSDirectoryServiceFullAccess](#) di Referensi Kebijakan AWS Terkelola.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua Directory Service tindakan. Prinsipal dengan izin ini dapat membuat, mengkonfigurasi, dan mengelola direktori, termasuk Simple AD, AD Connector, dan Managed Microsoft AD. Mereka juga dapat mengelola berbagi direktori, hubungan kepercayaan, dan konfigurasi pemantauan. Kebijakan ini mencakup izin untuk mengelola infrastruktur jaringan dasar yang diperlukan untuk layanan direktori.

Detail izin

Kebijakan ini mencakup izin berikut:

- `ds` – Mengizinkan bagian utama untuk mendapatkan akses penuh ke semua tindakan Directory Service .
- `ec2`— Memungkinkan prinsipal untuk mengelola antarmuka jaringan, grup keamanan, dan menjelaskan sumber daya VPC yang diperlukan untuk operasi direktori.
- `sns`— Memungkinkan kepala sekolah untuk membuat dan mengelola topik SNS untuk pemantauan direktori, khususnya topik dengan nama yang dimulai dengan `"`. `DirectoryMonitoring`
- `iam`— Memungkinkan kepala sekolah untuk daftar peran IAM untuk operasi layanan direktori.
- `organizations`— Memungkinkan prinsipal untuk mengelola integrasi AWS Organisasi dan akses enable/disable layanan untuk layanan direktori.

AWS kebijakan terkelola: `AWSDirectoryServiceReadOnlyAccess`

Anda dapat melampirkan kebijakan `AWSDirectoryServiceReadOnlyAccess` ke identitas IAM Anda. Untuk melihat izin lengkap untuk kebijakan ini, lihat [AWSDirectoryServiceReadOnlyAccess](#) di Referensi Kebijakan AWS Terkelola.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna untuk melihat informasi. Directory Service Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun ke direktori atau konfigurasinya. Misalnya, prinsipal dengan izin ini dapat melihat detail direktori, hubungan kepercayaan, dan konfigurasi pemantauan, tetapi tidak dapat membuat direktori baru atau memodifikasi yang sudah ada. Mereka juga dapat melihat sumber daya jaringan EC2 terkait dan topik SNS yang terkait dengan direktori.

Detail izin

Kebijakan ini mencakup izin berikut:

- **ds**— Memungkinkan pengguna untuk melakukan tindakan read-only yang mengembalikan informasi direktori. Ini termasuk operasi API yang dimulai dengan `Check`, `Describe`, `Get`, `List`, atau `Verify`.
- **ec2**— Memungkinkan pengguna untuk menggambarkan antarmuka jaringan, subnet, dan VPCs terkait dengan layanan direktori.
- **sns**— Memungkinkan pengguna untuk daftar dan mendapatkan informasi tentang topik SNS dan langganan yang digunakan untuk pemantauan direktori.
- **organizations**— Memungkinkan pengguna untuk mendeskripsikan AWS Organizations akun dan konfigurasi akses layanan yang terkait dengan layanan direktori.

AWS kebijakan terkelola: `AWSDirectoryServiceDataFullAccess`

Anda dapat melampirkan kebijakan `AWSDirectoryServiceDataFullAccess` ke identitas IAM Anda. Untuk melihat izin lengkap untuk kebijakan ini, lihat [AWSDirectoryServiceDataFullAccess](#) di Referensi Kebijakan AWS Terkelola.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke operasi Directory Service Data. Prinsipal dengan izin ini dapat membuat, memperbarui, dan menghapus pengguna dan grup Active Directory dalam direktori terkelola. Mereka dapat mengelola keanggotaan grup, mengaktifkan atau menonaktifkan pengguna, dan melakukan operasi manajemen pengguna dan grup yang komprehensif. Kebijakan ini dirancang untuk administrator yang perlu mengelola objek Active Directory secara terprogram.

Detail izin

Kebijakan ini mencakup izin berikut:

- **ds**— Memungkinkan prinsipal untuk mengakses data direktori melalui Directory Service Data API.
- **ds-data**— Memungkinkan prinsipal akses penuh ke semua operasi Directory Service Data, termasuk membuat, memperbarui, dan menghapus pengguna dan grup, mengelola keanggotaan grup, dan mencari objek direktori.

AWS kebijakan terkelola: `AWSDirectoryServiceDataReadOnlyAccess`

Anda dapat melampirkan kebijakan `AWSDirectoryServiceDataReadOnlyAccess` ke identitas IAM Anda. Untuk melihat izin lengkap untuk kebijakan ini, lihat [AWSDirectoryServiceDataReadOnlyAccess](#) di Referensi Kebijakan AWS Terkelola.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna untuk melihat dan mencari objek Direktori Aktif dalam direktori terkelola. Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun kepada pengguna, grup, atau keanggotaan grup. Misalnya, prinsipal dengan izin ini dapat mencari pengguna dan grup, melihat detail pengguna dan grup, dan daftar keanggotaan grup, tetapi tidak dapat membuat, memodifikasi, atau menghapus objek direktori apa pun.

Detail izin

Kebijakan ini mencakup izin berikut:

- `ds`— Memungkinkan prinsipal untuk mengakses data direktori melalui Directory Service Data API.
- `ds-data`— Memungkinkan pengguna untuk melakukan tindakan read-only yang mengembalikan informasi objek direktori. Ini termasuk operasi API yang dimulai dengan `Describe`, `List`, atau `Search`.

AWSDirectoryServiceServiceRolePolicy

Anda tidak dapat melampirkan `AWSDirectoryServiceServiceRolePolicy` kebijakan ke identitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan AWS Directory Service melakukan tindakan atas nama Anda. Untuk melihat izin kebijakan ini, lihat [AWSDirectoryServiceServiceRolePolicy](#) di Referensi Kebijakan AWS Terkelola.

Kebijakan ini memberikan izin yang memungkinkan Directory Service untuk memantau dan menilai pengontrol domain yang dikelola sendiri di lingkungan Active Directory hybrid. Layanan ini menggunakan izin ini untuk menjalankan penilaian kesehatan otomatis, menjalankan PowerShell skrip untuk pengujian kompatibilitas, dan mengumpulkan informasi konfigurasi jaringan untuk memastikan konektivitas hibrida yang tepat dan kemampuan pemulihan otomatis.

Detail izin

Kebijakan ini mencakup izin berikut:

- `ssm`— Memungkinkan layanan mengirim PowerShell perintah ke pengontrol domain lokal dan mengambil hasil eksekusi perintah untuk tujuan pemantauan dan penilaian.
- `ec2`— Memungkinkan layanan untuk menggambarkan sumber daya jaringan seperti VPCs, subnet, grup keamanan, dan antarmuka jaringan untuk memvalidasi konfigurasi konektivitas hybrid.

IAM dan Directory Service pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan IAM dan kebijakan AWS terkelola sejak layanan mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman IAM dan Riwayat Directory Service Dokumen.

Ubah	Deskripsi	Date
AWSDirectoryServiceServiceRolePolicy – Kebijakan baru	Directory Service menambahkan kebijakan baru AWS untuk memungkinkan memantau pengontrol domain yang dikelola sendiri oleh pelanggan.	Juli 30, 2025
AWS kebijakan terkelola: AWSDirectoryServiceDataReadOnlyAccess – Kebijakan baru	Directory Service menambahkan kebijakan baru untuk memungkinkan pengguna atau grup mengakses melihat dan menelusuri pengguna, anggota, dan grup AD.	September 17, 2024
AWS kebijakan terkelola: AWSDirectoryServiceDataFullAccess – Kebijakan baru	Directory Service menambahkan kebijakan baru untuk mengizinkan pengguna atau grup mengakses pengelolaan objek bawaan dengan Directory Service Data untuk membuat, mengelola, dan melihat pengguna, anggota, dan grup AD.	September 17, 2024
Directory Service mulai melacak perubahan	Directory Service mulai melacak perubahan untuk kebijakan AWS terkelolanya.	September 17, 2024

Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk Directory Service

Topik ini memberikan contoh kebijakan berbasis identitas di mana administrator akun dapat melampirkan kebijakan izin ke identitas IAM (pengguna, grup, dan peran). Contoh-contoh ini menunjukkan kebijakan IAM di Directory Service. Anda harus memodifikasi dan membuat kebijakan Anda sendiri sesuai dengan kebutuhan dan lingkungan Anda.

Important

Kami menyarankan Anda terlebih dahulu meninjau topik pengantar yang menjelaskan konsep dasar dan opsi yang tersedia bagi Anda untuk mengelola akses ke Directory Service sumber daya Anda. Untuk informasi selengkapnya, lihat [Ikhtisar mengelola izin akses ke sumber daya Anda Directory Service](#).

Bagian dalam topik ini membahas hal berikut:

- [Izin yang diperlukan untuk menggunakan konsol Directory Service](#)
- [AWS kebijakan terkelola \(standar\) untuk Directory Service](#)
- [Contoh kebijakan yang dikelola pelanggan](#)
- [Menggunakan tanda dengan kebijakan IAM](#)

Berikut adalah contoh kebijakan izin.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDsEc2IamGetRole",
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
```

```

        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "iam:GetRole"
    ],
    "Resource": "*"
},
{
    "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
},
{
    "Sid": "AllowPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::111122223333:role/Your-Role-Name",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "cloudwatch.amazonaws.com"
        }
    }
}
]
}

```

Tiga pernyataan dalam kebijakan memberikan izin sebagai berikut:

- Pernyataan pertama memberikan izin untuk membuat Directory Service direktori. Karena Directory Service tidak mendukung izin di tingkat sumber daya, kebijakan menetapkan karakter wildcard (*) sebagai nilainya. Resource

- Pernyataan kedua memberikan izin untuk mengakses tindakan IAM, sehingga Directory Service dapat membaca dan membuat peran IAM atas nama Anda. Karakter wildcard (*) di akhir nilai Resource berarti bahwa pernyataan itu memungkinkan izin untuk tindakan IAM di setiap IAM role. Untuk membatasi izin ini ke peran tertentu, ganti karakter wildcard (*) di ARN sumber daya dengan nama peran tertentu. Untuk informasi selengkapnya, lihat [Tindakan IAM](#).
- Pernyataan ketiga memberikan izin ke kumpulan sumber daya tertentu di Amazon EC2 yang diperlukan untuk Directory Service memungkinkan membuat, mengonfigurasi, dan menghancurkan direktorinya. Ganti peran ARN dengan peran Anda. Untuk informasi selengkapnya, lihat [Tindakan Amazon EC2](#).

Anda tidak melihat Principal elemen dalam kebijakan, karena dalam kebijakan berbasis identitas Anda tidak menentukan kepala sekolah yang mendapatkan izin. Saat Anda melampirkan kebijakan ke pengguna, pengguna adalah prinsipal implisit. Saat Anda menyematkan kebijakan izin pada peran IAM, pengguna utama yang diidentifikasi dalam kebijakan kepercayaan peran tersebut akan mendapatkan izin.

Untuk tabel yang menunjukkan semua tindakan Directory Service API dan sumber daya yang diterapkan, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#).

Izin yang diperlukan untuk menggunakan konsol Directory Service

Agar pengguna dapat bekerja dengan Directory Service konsol, pengguna tersebut harus memiliki izin yang tercantum dalam kebijakan sebelumnya atau izin yang diberikan oleh peran Directory Service Full Access Role atau Directory Service Read Only, yang dijelaskan dalam [AWS kebijakan terkelola \(standar\) untuk Directory Service](#)

Jika Anda membuat kebijakan IAM yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya bagi pengguna dengan kebijakan IAM tersebut.

AWS kebijakan terkelola (standar) untuk Directory Service

AWS menangani banyak kasus penggunaan umum dengan menyediakan kebijakan IAM yang telah ditentukan, atau dikelola, yang dibuat dan dikelola oleh AWS Kebijakan terkelola memberikan izin yang diperlukan untuk kasus penggunaan umum, yang membantu Anda memutuskan izin apa yang Anda perlukan. Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola untuk AWS Directory Service](#).

Contoh kebijakan yang dikelola pelanggan

Di bagian ini, Anda dapat menemukan contoh kebijakan pengguna yang memberikan izin untuk berbagai Directory Service tindakan.

Note

Semua contoh menggunakan Wilayah Barat AS (Oregon) (us-west-2) dan berisi akun fiktif. IDs

Contoh

- [Contoh 1: Izinkan pengguna melakukan tindakan Deskripsikan apa pun pada Directory Service sumber daya apa pun](#)
- [Contoh 2: Mengizinkan pengguna untuk membuat direktori](#)

Contoh 1: Izinkan pengguna melakukan tindakan Deskripsikan apa pun pada Directory Service sumber daya apa pun

Kebijakan izin berikut memberikan izin kepada pengguna untuk menjalankan semua tindakan yang dimulai Describe dalam iklan AWS Microsoft Terkelola dengan ID d-1234567890 direktori di. Akun AWS 111122223333 Tindakan ini menampilkan informasi tentang Directory Service sumber daya, seperti direktori atau snapshot. Pastikan untuk mengubah nomor akun AWS Region dan ke wilayah yang ingin Anda gunakan dan nomor akun Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "arn:aws:ds:us-west-2:111122223333:directory/d-1234567890"
    }
  ]
}
```

Contoh 2: Mengizinkan pengguna untuk membuat direktori

Kebijakan izin berikut memberikan izin untuk memungkinkan pengguna untuk membuat direktori dan semua sumber daya terkait lainnya, seperti snapshot dan trust. Untuk melakukannya, izin untuk layanan Amazon EC2 tertentu juga diperlukan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory",
        "ds:DescribeDirectories"
      ],
      "Resource": "arn:aws:ds:*:111122223333:"
    }
  ]
}
```

Menggunakan tanda dengan kebijakan IAM

Anda dapat menerapkan izin tingkat sumber daya berbasis tag dalam kebijakan IAM yang Anda gunakan untuk sebagian besar tindakan API. Directory Service Hal ini memberi Anda kontrol yang lebih baik atas sumber daya yang dapat dibuat, dimodifikasi, atau digunakan oleh pengguna. Anda menggunakan elemen `Condition` (juga disebut blok `Condition`) dengan kunci konteks syarat berikut dan nilai-nilai dalam kebijakan IAM untuk mengontrol akses pengguna (izin) berdasarkan tanda sumber daya:

- Gunakan `aws:ResourceTag/tag-key: tag-value` untuk mengizinkan atau menolak tindakan pengguna pada sumber daya dengan tanda tertentu.
- Gunakan `aws:ResourceTag/tag-key: tag-value` untuk mengharuskan penggunaan (atau tidak mengharuskan penggunaan) tanda tertentu saat membuat permintaan API untuk membuat atau memodifikasi sumber daya yang mengizinkan tanda.
- Gunakan `aws:TagKeys: [tag-key, ...]` untuk mengharuskan penggunaan (atau tidak mengharuskan penggunaan) serangkaian kunci tanda tertentu saat membuat permintaan API untuk membuat atau memodifikasi sumber daya yang mengizinkan tanda.

Note

Kunci dan nilai konteks syarat dalam kebijakan IAM hanya berlaku untuk tindakan Directory Service tersebut di mana pengidentifikasi untuk sumber daya yang dapat ditandai adalah parameter yang diperlukan.

[Mengontrol akses menggunakan tanda](#) di Panduan Pengguna IAM memiliki informasi tambahan tentang cara menggunakan tanda. Bagian [Referensi kebijakan JSON IAM](#) dari panduan tersebut menyajikan sintaks terperinci, deskripsi, dan contoh elemen, variabel, dan logika evaluasi kebijakan JSON di IAM.

Kebijakan tag berikut memungkinkan pembuatan Directory Service direktori selama tag berikut digunakan:

- Lingkungan: Produksi
- Pemilik: Infrastructure Team
- Pusat biaya: 1234

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Environment": "Production",
          "aws:RequestTag/Owner": "Infrastructure-Team",
          "aws:RequestTag/CostCenter": "12345"
        }
      }
    }
  ]
}
```

Kebijakan tag berikut memungkinkan memperbarui dan menghapus Directory Service direktori selama tag berikut digunakan:

- Proyek: Atlas
- Departemen: Teknik
- Lingkungan: Pementasan

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:DeleteDirectory",
        "ds:UpdateDirectory"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/Project": "Atlas",
            "aws:ResourceTag/Department": "Engineering",
            "aws:ResourceTag/Environment": "Staging"
        }
    }
}
]
}

```

Kebijakan tag berikut menolak penandaan sumber daya Directory Service di mana sumber daya memiliki salah satu tag berikut:

- Produksi
- Keamanan
- Rahasia

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ds:AddTagsToResource"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": ["Production", "Security", "Confidential"]
        }
      }
    }
  ]
}

```

Untuk informasi selengkapnya ARNs, lihat [Amazon Resource Names \(ARNs\) dan Ruang Nama AWS Layanan](#).

Daftar operasi Directory Service API berikut mendukung izin tingkat sumber daya berbasis tag:

- [AcceptSharedDirectory](#)
- [AddIpRoutes](#)
- [AddTagsToResource](#)
- [CancelSchemaExtension](#)
- [CreateAlias](#)
- [CreateComputer](#)
- [CreateConditionalForwarder](#)
- [CreateSnapshot](#)
- [CreateLogSubscription](#)
- [CreateTrust](#)
- [DeleteConditionalForwarder](#)
- [DeleteDirectory](#)
- [DeleteLogSubscription](#)
- [DeleteSnapshot](#)
- [DeleteTrust](#)
- [DeregisterEventTopic](#)
- [DescribeConditionalForwarders](#)
- [DescribeDomainControllers](#)
- [DescribeEventTopics](#)
- [DescribeSharedDirectories](#)
- [DescribeSnapshots](#)
- [DescribeTrusts](#)
- [DisableRadius](#)
- [DisableSso](#)
- [EnableRadius](#)
- [EnableSso](#)
- [GetSnapshotLimits](#)

- [ListIpRoutes](#)
- [ListSchemaExtensions](#)
- [ListTagsForResource](#)
- [RegisterEventTopic](#)
- [RejectSharedDirectory](#)
- [RemovelpRoutes](#)
- [RemoveTagsFromResource](#)
- [ResetUserPassword](#)
- [RestoreFromSnapshot](#)
- [ShareDirectory](#)
- [StartSchemaExtension](#)
- [UnshareDirectory](#)
- [UpdateConditionalForwarder](#)
- [UpdateNumberOfDomainControllers](#)
- [UpdateRadius](#)
- [UpdateTrust](#)
- [VerifyTrust](#)

Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi

Saat menyiapkan [Kontrol akses](#) dan menulis kebijakan izin yang dapat dilampirkan ke identitas IAM (kebijakan berbasis identitas), Anda dapat menggunakan tabel sebagai referensi. [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#) Setiap entri API dalam mencakup hal-hal berikut:

- Nama setiap operasi API
- Setiap tindakan atau tindakan terkait operasi API di mana Anda dapat memberikan izin untuk melakukan tindakan
- Sumber AWS daya di mana Anda dapat memberikan izin

Anda menentukan tindakan dalam bidang `Action` kebijakan, dan nilai sumber daya di dalam bidang `Resource` kebijakan. Untuk menentukan tindakan, gunakan awalan `ds:`

diikuti dengan nama operasi API (misalnya, `ds:CreateDirectory`). Beberapa AWS aplikasi mungkin memerlukan penggunaan operasi Directory Service API nonpublik seperti `ds:AuthorizeApplication`, `ds:CheckAlias`, `ds:CreateIdentityPoolDirectory`, `ds:GetAuthorizedApplicationDetails`, `ds:UpdateAuthorizedApplication`, dan `ds:UnauthorizeApplication` dalam kebijakan mereka.

Beberapa hanya Directory Service APIs bisa dipanggil melalui Konsol Manajemen AWS. Mereka tidak publik APIs, dalam arti mereka tidak dapat disebut secara terprogram, dan mereka tidak disediakan oleh SDK apa pun. Mereka menerima kredensi pengguna. Operasi API ini meliputi `ds:DisableRoleAccess`, `ds:EnableRoleAccess`, dan `ds:UpdateDirectory`.

Anda dapat menggunakan kunci kondisi AWS global dalam kebijakan Directory Service Data Directory Service dan Directory Service untuk menyatakan kondisi. Untuk daftar lengkap AWS kunci, lihat [Kunci Kondisi Global yang Tersedia](#) di Panduan Pengguna IAM.

Directory Service API dan izin yang diperlukan untuk tindakan

AWS Directory Service Data API dan izin yang diperlukan untuk tindakan

 Note

Untuk menentukan tindakan, gunakan `ds-data:` awalan yang diikuti dengan nama operasi API (misalnya, `ds-data:AddGroupMember`).

Operasi API Directory Service Data	Izin yang Diperlukan (Tindakan API)	Sumber daya
AddGroupMember	<code>ds-data:AddGroupMember</code>	*
CreateGroup	<code>ds-data:CreateGroup</code>	*
CreateUser	<code>ds-data:CreateUser</code>	*
DeleteGroup	<code>ds-data>DeleteGroup</code>	*
DeleteUser	<code>ds-data>DeleteUser</code>	*
DescribeGroup	<code>ds-data:DescribeGroup</code>	*

Operasi API Directory Service Data	Izin yang Diperlukan (Tindakan API)	Sumber daya
DescribeUser	ds-data:DescribeUser	*
DisableUser	ds-data:DisableUser	*
ListGroup	ds-data:ListGroup	*
ListGroupMembers	ds-data:ListGroupMembers	*
ListGroupForMember	ds-data:ListGroupForMember	*
ListUsers	ds-data:ListUsers	*
RemoveGroupMember	ds-data:RemoveGroupMember	*
SearchGroups	ds-data:DescribeGroup ds-data:SearchGroups	*
SearchUsers	ds-data:DescribeUser ds-data:SearchUsers	*
UpdateGroup	ds-data:UpdateGroup	*
UpdateUser	ds-data:UpdateUser	*

Topik Terkait

- [Kontrol akses](#)

Kunci kondisi Directory Service Data

Gunakan kunci kondisi [Directory Service Data](#) untuk menambahkan pernyataan spesifik ke pengguna dan akses tingkat grup. Ini memungkinkan pengguna untuk memutuskan prinsip mana yang dapat melakukan tindakan pada sumber daya apa dan dalam kondisi apa.

Elemen Kondisi, atau blok Kondisi, memungkinkan Anda menentukan kondisi di mana pernyataan berlaku. Elemen Syarat bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, seperti sama dengan (=) atau kurang dari (<), untuk mencocokkan kondisi dalam kebijakan dengan nilai dalam permintaan.

Jika Anda menentukan beberapa elemen Kondisi dalam pernyataan, atau beberapa kunci dalam satu elemen Kondisi, AWS evaluasi mereka dengan menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi dengan menggunakan operasi OR logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan. Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika diberi tag dengan nama pengguna mereka. Untuk selengkapnya, lihat [Kondisi dengan beberapa kunci atau nilai](#) dalam Panduan Pengguna IAM.

Untuk daftar tindakan yang mendukung kunci kondisi ini, lihat [Tindakan yang ditentukan oleh AWS Directory Service Data](#) dalam Referensi Otorisasi Layanan.

 Note

Untuk informasi tentang izin tingkat sumber daya berbasis tag, lihat. [Menggunakan tanda dengan kebijakan IAM](#)

ds-data: Nama SAMAccount

Bekerja dengan [operator String](#).

Gunakan kunci ini untuk secara eksplisit mengizinkan atau menolak peran IAM agar tidak melakukan tindakan pada pengguna dan grup tertentu.

 Important

Saat menggunakan SAMAccountName atau MemberName, kami sarankan untuk menentukan ds-data:Identifier sebagai SAMAccountName. Hal ini mencegah pengenalan future yang didukung AWS Directory Service Data, seperti SID, dari melanggar izin yang ada.

Kebijakan berikut menyangkal prinsipal IAM untuk mendeskripsikan pengguna joe atau mendeskripsikan grup. joegroup

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyDescribe",
      "Effect": "Deny",
      "Action": "ds-data:Describe*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "joe",
            "joegroup"
          ],
          "ds-data:identifier": [
            "SAMAccountName"
          ]
        }
      }
    }
  ]
}
```

 Note

Kunci kondisi ini tidak peka huruf besar/kecil. Anda harus menggunakan [StringEqualsIgnoreCase](#) atau [StringNotEqualsIgnoreCase](#) mengkondisikan operator untuk membandingkan nilai string terlepas dari kasus huruf.

DS-data: Pengidentifikasi

Bekerja dengan [operator String](#).

Gunakan kunci ini untuk menentukan pengenalan mana yang akan digunakan dalam izin kebijakan IAM. Saat ini, hanya SAMAccountName didukung.

Kebijakan berikut memungkinkan prinsipal IAM untuk memperbarui pengguna joe.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateJoe",
      "Effect": "Allow",
      "Action": "ds-data:UpdateUser",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "joe"
          ],
          "ds-data:identifier": [
            "SAMAccountName"
          ]
        }
      }
    }
  ]
}
```

ds-data: MemberName

Bekerja dengan [operator String](#).

Gunakan kunci ini untuk menentukan anggota yang dapat melakukan operasi pada mereka.

Important

Saat menggunakan MemberName atau SAMAccountName, kami sarankan untuk menentukan ds-data:Identifier sebagai SAMAccountName. Hal ini mencegah pengenalan future yang didukung Directory Service Data, seperti SID, dari melanggar izin yang ada.

Kebijakan berikut memungkinkan kepala IAM untuk tampil AddGroupMember pada anggota joe dalam kelompok mana pun.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddJoe",
      "Effect": "Allow",
      "Action": "ds-data:AddGroupMember",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": "joe"
        }
      }
    }
  ]
}
```

 Note

Kunci kondisi ini tidak peka huruf besar/kecil. Anda harus menggunakan [StringEqualsIgnoreCase](#) atau [StringNotEqualsIgnoreCase](#) mengkondisikan operator untuk membandingkan nilai string, terlepas dari kasus huruf.

ds-data: MemberRealm

Bekerja dengan [operator String](#).

Gunakan kunci ini untuk memeriksa apakah ds-data:MemberRealm nilai dalam kebijakan cocok dengan ranah anggota dalam permintaan.

 Note

Kunci kondisi ini tidak peka huruf besar/kecil. Anda harus menggunakan [StringEqualsIgnoreCase](#) atau [StringNotEqualsIgnoreCase](#) mengkondisikan operator untuk membandingkan nilai string, terlepas dari kasus huruf.

Kebijakan berikut memungkinkan kepala IAM `AddGroupMember` untuk memanggil anggota bob di `ranahONE.TRU1.AMAZON.COM`.

Note

Contoh berikut hanya menggunakan kunci `ds-data:MemberName` konteks.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "addbob",
      "Effect": "Allow",
      "Action": "ds-data:AddGroupMember",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": "bob",
          "ds-data:MemberRealm": "one.tru1.amazon.com"
        }
      }
    }
  ]
}
```

DS-Data: Realm

Bekerja dengan [operator String](#).

Gunakan kunci ini untuk memeriksa apakah `ds-data:Realm` nilai dalam kebijakan cocok dengan ranah yang dapat digunakan oleh prinsipal IAM untuk membuat permintaan ke Directory Service Data APIs.

 Note

Kunci kondisi ini tidak peka huruf besar/kecil. Anda harus menggunakan [StringEqualsIgnoreCase](#) atau [StringNotEqualsIgnoreCase](#) mengkondisikan operator untuk membandingkan nilai string terlepas dari kasus huruf.

Kebijakan berikut menyangkal kepala IAM dari menyerukan ListUsers ranah.
one.tru1.amazon.com

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyTrustedList",
      "Effect": "Deny",
      "Action": "ds-data:ListUsers",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:Realm": [
            "one.tru1.amazon.com"
          ]
        }
      }
    }
  ]
}
```

Otorisasi untuk AWS aplikasi dan layanan menggunakan Directory Service

Topik ini menjelaskan otorisasi untuk AWS aplikasi dan layanan menggunakan AWS Directory Service dan AWS Directory Service Data

Mengotorisasi AWS aplikasi pada Active Directory

Directory Service memberikan izin khusus untuk aplikasi yang dipilih untuk diintegrasikan secara mulus dengan Direktori Aktif Anda saat Anda mengotorisasi aplikasi. AWS AWS aplikasi hanya diberikan akses yang diperlukan untuk kasus penggunaan spesifiknya. Berikut ini adalah seperangkat izin internal yang diberikan kepada aplikasi dan administrator aplikasi setelah otorisasi:

Note

`ds:AuthorizationApplication` izin diperlukan untuk mengotorisasi AWS aplikasi baru untuk Direktori Aktif. Izin untuk tindakan ini hanya boleh diberikan kepada Administrator yang mengonfigurasi integrasi dengan Directory Service.

- Baca akses ke data pengguna, grup, unit organisasi, komputer, atau otoritas sertifikasi Active Directory di semua Unit Organisasi (OU) direktori AD Microsoft AWS Terkelola, Simple AD, AD Connector, serta domain tepercaya untuk AWS Microsoft AD Terkelola jika diizinkan oleh hubungan kepercayaan.
- Tulis akses ke pengguna, grup, keanggotaan grup, komputer, atau data otoritas sertifikasi di unit organisasi Microsoft AD yang AWS Dikelola. Tulis akses ke semua OU Simple AD.
- Otentikasi dan manajemen sesi pengguna Active Directory untuk semua jenis direktori.

Aplikasi Microsoft AD AWS Terkelola tertentu seperti Amazon RDS dan Amazon FSx terintegrasi melalui koneksi jaringan langsung ke Active Directory Anda. Dalam hal ini, interaksi direktori menggunakan protokol Active Directory asli seperti LDAP dan Kerberos. Izin AWS aplikasi ini dikendalikan oleh akun pengguna direktori yang dibuat di Unit Organisasi AWS Cadangan (OU) selama otorisasi aplikasi, yang mencakup manajemen DNS dan akses penuh ke OU khusus yang dibuat untuk aplikasi. Untuk menggunakan akun ini, aplikasi memerlukan izin untuk `ds:GetAuthorizedApplicationDetails` bertindak melalui kredensial pemanggil atau peran IAM.

Untuk informasi selengkapnya tentang izin Directory Service API, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#).

Untuk informasi selengkapnya tentang mengaktifkan AWS aplikasi dan layanan untuk Microsoft AD yang AWS Dikelola, lihat [Akses ke AWS aplikasi dan layanan dari Microsoft AD yang AWS Dikelola](#). Untuk informasi selengkapnya tentang mengaktifkan AWS aplikasi dan layanan untuk Simple AD, lihat [Akses ke AWS aplikasi dan layanan dari Simple AD](#). Untuk informasi tentang mengaktifkan

AWS aplikasi dan layanan untuk AD Connector, lihat [Akses ke AWS aplikasi dan layanan dari AD Connector](#).

Membatalkan otorisasi AWS aplikasi pada Active Directory

`ds:UnauthorizedApplication` izin diperlukan untuk menghapus izin bagi AWS aplikasi untuk mengakses Direktori Aktif. Ikuti prosedur yang disediakan aplikasi untuk menonaktifkannya.

AWS otorisasi aplikasi dengan Directory Service Data

Untuk direktori Microsoft AD AWS Terkelola, API Directory Service Data (`ds-data`) menyediakan akses terprogram ke tugas manajemen pengguna dan grup. Model otorisasi AWS aplikasi terpisah dari kontrol akses Directory Service Data, yang berarti bahwa kebijakan akses untuk tindakan Directory Service Data tidak mempengaruhi otorisasi untuk AWS aplikasi. Menolak akses ke direktori dalam `ds-data` tidak akan mengganggu integrasi AWS Aplikasi atau kasus penggunaan aplikasi. AWS

Saat menulis kebijakan akses untuk direktori Microsoft AD AWS Terkelola yang mengotorisasi AWS aplikasi, ketahuilah bahwa fungsionalitas pengguna dan grup mungkin tersedia dengan memanggil AWS Application resmi atau Directory Service Data API. Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, Amazon Quick, dan Amazon Chime semuanya menyediakan tindakan manajemen pengguna dan grup di dalamnya. APIs Kontrol akses ke fungsionalitas AWS aplikasi ini dengan kebijakan IAM.

Contoh

Cuplikan berikut menunjukkan cara yang salah dan benar untuk menolak `DeleteUser` fungsionalitas saat AWS aplikasi, seperti dan WorkDocs Amazon WorkMail, diotorisasi di direktori.

Salah

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "ds-data:DeleteUser"
    ]
  }]
}
```

```

    ],
    "Resource": "*"
  }
]
}

```

Benar

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "ds-data:DeleteUser",
      "workmail:DeleteUser",
      "workdocs:DeleteUser"
    ],
    "Resource": "*"
  }
]
}

```

Menggunakan peran terkait layanan untuk Directory Service

AWS Directory Service menggunakan AWS Identity and Access Management peran [terkait layanan](#) (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. Directory Service Peran terkait layanan telah ditentukan sebelumnya oleh Directory Service dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Directory Service lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Directory Service mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Directory Service dapat mengambil perannya. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, yang tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini mencegah Anda kehilangan akses ke Directory Service sumber daya karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [Layanan AWS yang bekerja dengan IAM](#).

Topik

- [Izin peran terkait layanan untuk Directory Service](#)
- [Membuat peran terkait layanan untuk Directory Service](#)
- [Mengedit peran terkait layanan untuk Directory Service](#)
- [Menghapus peran terkait layanan untuk Directory Service](#)
- [Wilayah yang Didukung untuk Directory Service peran terkait layanan](#)

Izin peran terkait layanan untuk Directory Service

Directory Service menggunakan peran terkait layanan bernama `AWSServiceRoleForDirectoryService`— Memungkinkan AWS untuk memantau pengontrol domain yang dikelola sendiri oleh pelanggan.

Peran tertaut layanan `AWSServiceRoleForDirectoryService` memercayai layanan berikut untuk mengambil peran tersebut:

- `ds.amazonaws.com`

Kebijakan izin peran bernama `AWSDirectoryServiceServiceRolePolicy` memungkinkan Directory Service untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan. Untuk izin kebijakan lengkap, lihat [AWSDirectoryServiceServiceRolePolicy](#) di Referensi Kebijakan AWS Terkelola.

- `ec2`— Memungkinkan layanan untuk menggambarkan sumber daya jaringan seperti VPCs, subnet, grup keamanan, dan antarmuka jaringan untuk memvalidasi konfigurasi konektivitas hybrid:
 - `ec2:DescribeAvailabilityZones`
 - `ec2:DescribeDhcpOptions`
 - `ec2:DescribeNetworkInterfaces`
 - `ec2:DescribeRouteTables`

- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ssm`— Memungkinkan layanan mengirim dan memantau PowerShell guilabel ke pengontrol domain lokal untuk tujuan pemantauan dan penilaian:
 - `ssm:Sendguilabel`
 - `ssm:Listguilabels`
 - `ssm:GetguilabelInvocation`
 - `ssm:DescribeInstanceInformation`
 - `ssm:GetConnectionStatus`

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 Directory Service

Anda tidak perlu membuat peran terkait layanan secara manual. Jika Anda mengizinkan AWS untuk memantau pengontrol domain yang dikelola sendiri pelanggan di Konsol Manajemen AWS, API AWS CLI, atau AWS API, Directory Service buat peran terkait layanan untuk Anda. Untuk informasi selengkapnya tentang perubahan ini, lihat [Pembaruan kebijakan](#).

Important

Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Juga, jika Anda menggunakan Directory Service layanan sebelum 1 Januari 2017, ketika mulai mendukung peran terkait layanan, maka Directory Service buat `AWSServiceRoleForDirectoryService` peran di akun Anda. Untuk mempelajari lebih lanjut, lihat [Peran baru muncul di saya Akun AWS](#).

Mengedit peran terkait layanan untuk Directory Service

Directory Service tidak memungkinkan Anda untuk mengedit peran `AWSServiceRoleForDirectoryService` 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 Directory Service

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 Directory Service layanan menggunakan peran pada saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus Directory Service sumber daya yang digunakan oleh AWSServiceRoleForDirectoryService

- Untuk menghapus direktori Anda, lihat [Menghapus iklan Microsoft yang AWS Dikelola](#).

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForDirectoryService terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk Directory Service peran terkait layanan

Directory Service tidak mendukung penggunaan peran terkait layanan di setiap Wilayah tempat layanan tersedia. Namun, Directory Service gunakan AWSServiceRoleForDirectoryService peran hanya di Wilayah AWS mana Anda dapat ikut serta ke direktori hybrid.

Dukungan wilayah keikutsertaan direktori hibrid

Nama wilayah	Identitas wilayah	dukungan opt-in
US East (Northern Virginia)	us-east-1	Ya

Nama wilayah	Identitas wilayah	dukungan opt-in
US East (Ohio)	us-east-2	Ya
US West (N. California)	us-west-1	Ya
US West (Oregon)	us-west-2	Ya
Eropa (Stockholm)	eu-north-1	Ya
Timur Tengah (Bahrain)	me-south-1	Ya
Asia Pacific (Mumbai)	ap-south-1	Ya
Europe (Paris)	eu-west-3	Ya
Asia Pasifik (Jakarta)	ap-southeast-3	Ya
Africa (Cape Town)	af-south-1	Ya
Eropa (Irlandia)	eu-west-1	Ya
Timur Tengah (UAE)	me-central-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
South America (São Paulo)	sa-east-1	Ya
Asia Pasifik (Hong Kong)	ap-east-1	Ya
Asia Pasifik (Hyderabad)	ap-south-2	Ya
Asia Pacific (Seoul)	ap-northeast-2	Ya
Asia Pacific (Osaka)	ap-northeast-3	Ya
Eropa (London)	eu-west-2	Ya
Asia Pacific (Melbourne)	ap-southeast-4	Ya
Europe (Milan)	eu-south-1	Ya

Nama wilayah	Identitas wilayah	dukungan opt-in
Asia Pacific (Tokyo)	ap-northeast-1	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya
Canada (Central)	ca-sentral-1	Ya
Eropa (Spanyol)	eu-south-2	Ya
Europe (Zurich)	eu-central-2	Ya

Penebangan dan pemantauan di AWS Directory Service

Sebagai praktik terbaik, pantau organisasi Anda untuk memastikan bahwa perubahan dicatat. Ini membantu Anda memastikan bahwa setiap perubahan tak terduga dapat diselidiki dan perubahan yang tidak diinginkan dapat dibatalkan. AWS Directory Service saat ini mendukung dua AWS layanan berikut, sehingga Anda dapat memantau organisasi Anda dan aktivitas yang terjadi di dalamnya.

- Amazon CloudWatch - Anda dapat menggunakan CloudWatch Acara dengan jenis direktori Microsoft AD yang AWS Dikelola. Untuk informasi selengkapnya, lihat [Mengaktifkan penerusan CloudWatch log Amazon Logs untuk Microsoft AD yang Dikelola AWS](#). Selain itu, Anda dapat menggunakan CloudWatch Metrik untuk memantau kinerja pengontrol domain. Untuk informasi selengkapnya, lihat [Menentukan kapan harus menambahkan pengontrol domain dengan metrik CloudWatch](#).
- AWS CloudTrail
 - Anda dapat menggunakan CloudTrail dengan semua jenis Directory Service direktori. Untuk informasi selengkapnya, lihat [Pencatatan panggilan AWS Directory Service API menggunakan AWS CloudTrail](#).
 - Anda dapat menggunakan Microsoft AD CloudTrail yang AWS Dikelola di Directory Service Data API. Untuk informasi selengkapnya, lihat [Pencatatan panggilan API AWS Directory Service Data menggunakan AWS CloudTrail](#).

Pencatatan panggilan AWS Directory Service API menggunakan AWS CloudTrail

Microsoft AD API AWS Terkelola terintegrasi dengan AWS CloudTrail, layanan yang menangkap panggilan API yang dilakukan oleh atau atas nama Microsoft AD AWS Terkelola di Anda Akun AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail menangkap panggilan API dari konsol Microsoft AD AWS Terkelola dan dari panggilan kode ke Microsoft AD AWS APIs Terkelola. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan apa yang dibuat untuk Microsoft AD yang AWS dikelola, alamat IP sumber dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan sebagainya. Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

AWS Informasi Microsoft AD yang Dikelola di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Microsoft AD yang AWS Dikelola, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat Acara dengan Riwayat CloudTrail Acara](#).

Untuk catatan peristiwa yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Microsoft AD yang AWS Dikelola, 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 AWS Wilayah. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi 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](#)

Saat CloudTrail logging diaktifkan di Anda Akun AWS, semua panggilan API yang dilakukan ke tindakan Microsoft AD AWS Terkelola dilacak dalam file log. AWS Catatan Microsoft AD yang dikelola ditulis bersama dengan catatan AWS layanan lain dalam file log. CloudTrail menentukan kapan harus

membuat dan menulis ke file baru berdasarkan periode waktu dan ukuran file. Semua panggilan yang dilakukan ke panggilan Directory Service API atau CLI dicatat oleh CloudTrail

Setiap entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas pengguna di log membantu Anda menentukan apakah permintaan dibuat dengan kredensial pengguna root atau IAM, dengan kredensial keamanan sementara untuk peran atau pengguna federasi, atau oleh layanan lain. AWS Untuk informasi selengkapnya, lihat bidang UserIdentity di Referensi [CloudTrail Acara](#).

Anda dapat menyimpan file log dalam bucket selama yang diinginkan, tetapi Anda juga dapat menentukan aturan siklus hidup Amazon S3 untuk mengarsipkan atau menghapus file log secara otomatis. Secara default, file log Anda dienkripsi dengan menggunakan enkripsi di sisi server (SSE) Amazon S3.

Anda dapat memilih untuk CloudTrail mempublikasikan notifikasi Amazon SNS saat file log baru dikirimkan jika Anda ingin mengambil tindakan cepat saat pengiriman file log. Untuk informasi lebih lanjut, lihat [Mengonfigurasi pemberitahuan Amazon SNS](#).

Anda juga dapat menggabungkan file log Microsoft AD AWS Terkelola dari beberapa AWS Wilayah dan Akun AWS ke dalam satu bucket Amazon S3. Untuk informasi selengkapnya, lihat [Menggabungkan File CloudTrail Log ke Satu Bucket Amazon S3](#).

Memahami Entri File Log Microsoft AD yang AWS Dikelola

CloudTrail file log dapat berisi satu atau lebih entri log, di mana setiap entri terdiri dari beberapa peristiwa berformat JSON. Entri log mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, parameter apa pun, tanggal dan waktu tindakan, dan lain-lain. Entri log tidak dijamin berada dalam urutan tertentu; yaitu, mereka bukan jejak tumpukan terurut dari panggilan API publik.

Informasi sensitif, seperti kata sandi, token autentikasi, komentar file, dan konten file disunting dalam entri log.

Contoh berikut menunjukkan contoh entri CloudTrail log untuk Microsoft AD yang AWS Dikelola:

```
{
  "Records" : [
    {
      "eventVersion" : "1.02",
      "userIdentity" :
      {
```

```

    "type" : "IAMUser",
    "principalId" : "<user_id>",
    "arn" : "<user_arn>",
    "accountId" : "<account_id>",
    "accessKeyId" : "<access_key_id>",
    "userName" : "<username>"
  },
  "eventTime" : "<event_time>",
  "eventSource" : "ds.amazonaws.com",
  "eventName" : "CreateDirectory",
  "awsRegion" : "<region>",
  "sourceIPAddress" : "<IP_address>",
  "userAgent" : "<user_agent>",
  "requestParameters" :
  {
    "name" : "<name>",
    "shortName" : "<short_name>",
    "vpcSettings" :
    {
      "vpcId" : "<vpc_id>",
      "subnetIds" : [
        "<subnet_id_1>",
        "<subnet_id_2>"
      ]
    },
    "type" : "<size>",
    "setAsDefault" : <option>,
    "password" : "****OMITTED****"
  },
  "responseElements" :
  {
    "requestId" : "<request_id>",
    "directoryId" : "<directory_id>"
  },
  "requestID" : "<request_id>",
  "eventID" : "<event_id>",
  "eventType" : "AwsApiCall",
  "recipientAccountId" : "<account_id>"
}
]
}

```

Pencatatan panggilan API AWS Directory Service Data menggunakan AWS CloudTrail

AWS Directory Service Data terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Directory Service Data. CloudTrail menangkap semua panggilan API untuk Directory Service Data sebagai peristiwa. Panggilan yang diambil meliputi panggilan dari konsol Directory Service Data dan panggilan kode ke operasi Directory Service Data API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Directory Service Data. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Directory Service Data, 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 Directory Service Data di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas acara yang didukung (peristiwa manajemen) terjadi di Directory Service Data, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh 90 hari terakhir acara manajemen di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan Riwayat CloudTrail acara](#). Tidak ada biaya untuk melihat riwayat Acara.

Untuk catatan peristiwa yang sedang berlangsung di Anda Akun AWS, termasuk peristiwa untuk Directory Service Data, 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 AWS partisi 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 Directory Service Data dicatat oleh CloudTrail dan didokumentasikan dalam [Referensi API Directory Service Data](#). Misalnya, panggilan `keAddGroupMember`, `DescribeUser` dan `SearchGroups` 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 kredensial 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 berkas log Directory Service Data

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. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [CreateUser](#) tindakan.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",
    "accessKeyId": "021345abcdef6789",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",
        "accountId": "111222333444",
```

```
    "userName": "AdAdmin"
  },
  "attributes": {
    "creationDate": "2023-05-30T18:22:38Z",
    "mfaAuthenticated": "false"
  }
},
"eventTime": "2023-05-30T19:17:03Z",
"eventSource": "ds.amazonaws.com",
"eventName": "CreateUser",
"awsRegion": "ap-northeast-2",
"sourceIPAddress": ": 10.24.34.0",
"userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.create-user",
"requestParameters": {
  "directoryId": "d-1234567890",
  "sAMAccountName": "johnsmith",
  "clientToken": "example_token"
  "emailAddress": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "surname": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "otherAttributes": {
    "physicalDeliveryOfficeName": {
      "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "telephoneNumber": {
      "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "streetAddress": {
      "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "displayName": {
      "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "homePhone": {
      "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "postalCode": {
      "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "description": {
      "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
    }
  }
}
```

```

    },
    "clientToken": "createUserToken4"
  },
  "responseElements": {
    "directoryId": "d-1234567890",
    "sID": "S-1-5-21-1234567890-123456789-123456789-1234",
    "sAMAccountName": "johnsmith"
  },
  "additionalEventData": {
    "SID": "S-1-5-21-1234567890-123456789-123456789-1234"
  },
  "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
  "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111222333444",
      "type": "AWS::DirectoryService::MicrosoftAD",
      "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111222333444",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
  }
},

```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [ListUser](#) tindakan.

Tindakan yang tidak membuat atau memodifikasi objek mengembalikan respons nol.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",
    "accessKeyId": "021345abcdef6789",

```

```
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",
        "accountId": "111222333444",
        "userName": "AdAdmin"
      },
      "attributes": {
        "creationDate": "2023-05-30T18:22:38Z",
        "mfaAuthenticated": "false"
      }
    },
    "eventTime": "2023-05-30T18:22:52Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "ListUsers",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.list-users",
    "requestParameters": {
      "directoryId": "d-1234567890",
      "maxResults": 1
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1244",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111222333444",
        "type": "AWS::DirectoryService::MicrosoftAD",
        "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
```

```
}  
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [ListGroup](#) tindakan.

 Note

NextTokenElemen disunting dari semua entri log.

```
{  
  "eventVersion": "1.08",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "1234567890abcdef0:admin-role",  
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",  
    "accountId": "111222333444",  
    "accessKeyId": "021345abcdef6789",  
    "sessionContext": {  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "1234567890abcdef0",  
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",  
        "accountId": "111222333444",  
        "userName": "AdAdmin"  
      },  
      "attributes": {  
        "creationDate": "2023-05-30T18:22:38Z",  
        "mfaAuthenticated": "false"  
      }  
    }  
  },  
  "eventTime": "2023-05-30T18:29:15Z",  
  "eventSource": "ds.amazonaws.com",  
  "eventName": "ListGroup",  
  "awsRegion": "ap-northeast-2",  
  "sourceIPAddress": "10.24.34.0",  
  "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off  
command/ds-data.list-groups",  
  "requestParameters": {  
    "directoryId": "d-1234567890",  
    "nextToken": "REDACTED",  
  }  
}
```



```

    "maxResults": 1
  },
  "responseElements": null,
  "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
  "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111222333444",
      "type": "AWS::DirectoryService::MicrosoftAD",
      "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111222333444",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
  }
}

```

Entri log untuk kesalahan pengecualian

Contoh berikut menunjukkan entri CloudTrail log untuk kesalahan Akses Ditolak. Untuk bantuan terkait kesalahan ini, lihat [Memecahkan masalah akses ditolak pesan kesalahan](#) di Panduan Pengguna IAM.

Note

Log Access Denied tidak menampilkan parameter permintaan.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",

```

```
"accessKeyId": "021345abcdef6789",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "1234567890abcdef0",
    "arn": "arn:aws:iam::111222333444:role/AdAdmin",
    "accountId": "111222333444",
    "userName": "AdAdmin"
  },
  "attributes": {
    "creationDate": "2023-05-31T23:25:49Z",
    "mfaAuthenticated": "false"
  }
},
"eventTime": "2023-05-31T23:38:18Z",
"eventSource": "ds.amazonaws.com",
"eventName": "CreateUser",
"awsRegion": "ap-northeast-2",
"sourceIPAddress": "10.24.34.0",
"userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.create-user",
"errorCode": "AccessDenied",
"errorMessage": "User: arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-
role is not authorized to perform: ds-data:CreateUser on resource: arn:aws:ds:ap-
northeast-2:111222333444:directory/d-1234567890 because no identity-based policy allows
the ds-data:CreateUser action",
"requestParameters": null,
"responseElements": null,
"requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
"eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
"readOnly": false,
"resources": [
  {
    "accountId": "111222333444",
    "type": "AWS::DirectoryService::MicrosoftAD",
    "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111222333444",
"eventCategory": "Management",
"tlsDetails": {
```

```

    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
  }
}

```

Contoh berikut menunjukkan entri CloudTrail log untuk kesalahan Sumber Daya Tidak Ditemukan.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",
    "accessKeyId": "021345abcdef6789",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",
        "accountId": "111222333444",
        "userName": "AdAdmin"
      },
      "attributes": {
        "creationDate": "2023-05-30T20:41:50Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-05-30T21:10:16Z",
  "eventSource": "ds.amazonaws.com",
  "eventName": "DescribeUser",
  "awsRegion": "ap-northeast-2",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.describe-user",
  "errorCode": "ResourceNotFoundException",
  "errorMessage": "User not found in directory d-1234567890.",
  "requestParameters": {
    "directoryId": "d-1234567890",
    "sAMAccountName": "nonExistingUser",
    "otherAttributes": [

```

```
        "co",
        "givenName",
        "sn",
        "telephoneNumber"
    ]
},
"responseElements": null,
"requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
"eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
"readOnly": true,
"resources": [
    {
        "accountId": "111222333444",
        "type": "AWS::DirectoryService::MicrosoftAD",
        "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111222333444"
"eventCategory": "Management",
"tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
}
}
```

Validasi kepatuhan untuk AWS Directory Service

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](#).

Ketahanan di AWS Directory Service

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat [infrastruktur AWS global](#).

Selain infrastruktur AWS global, Directory Service menawarkan kemampuan untuk mengambil snapshot manual data kapan saja untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda. Untuk informasi selengkapnya, lihat [Memulihkan iklan Microsoft AWS Terkelola Anda dengan snapshot](#).

Keamanan infrastruktur di AWS Directory Service

Sebagai layanan terkelola, AWS Directory Service 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 Directory Service 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.

Pencegahan "confused deputy" lintas layanan

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk

melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan principal layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi [aws:SourceAccount](#) global [aws:SourceArn](#) dan global dalam kebijakan sumber daya untuk membatasi izin yang Directory Service untuk Microsoft Active Directory memberikan layanan lain ke sumber daya. Jika nilai `aws:SourceArn` tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global tersebut untuk membatasi izin. Jika Anda menggunakan kunci konteks kondisi global dan nilai `aws:SourceArn` berisi ID akun, nilai `aws:SourceAccount` dan akun dalam nilai `aws:SourceArn` harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama. Gunakan `aws:SourceArn` jika Anda ingin hanya satu sumber daya yang akan dikaitkan dengan akses lintas layanan. Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.

Untuk contoh berikut, nilai `aws:SourceArn` harus berupa grup CloudWatch log.

Cara paling efektif untuk melindungi dari masalah "confused deputy" adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:servicename:*:123456789012:*`.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan `aws:SourceArn` dan kunci konteks kondisi `aws:SourceAccount` global di Microsoft AD yang AWS Dikelola untuk mencegah masalah deputy yang membingungkan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    }
  }
}
```

```

    },
    "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/
directoryservice/Log_Group_Name:"
    ],
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/Directory_Name"
        },
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        }
    }
}

```

Untuk contoh berikut, nilai `aws:SourceArn` harus menjadi topik SNS di akun Anda. Misalnya, Anda dapat menggunakan sesuatu seperti `arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f` di mana “ap-southeast-1” adalah wilayah Anda, “123456789012” adalah id pelanggan Anda dan “_d-966739499f” adalah nama topik Amazon SNS yang Anda buat. `DirectoryMonitoring`

Cara paling efektif untuk melindungi dari masalah “confused deputy” adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:servicename:*:123456789012:*`.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan `aws:SourceArn` dan kunci konteks kondisi `aws:SourceAccount` global di Microsoft AD yang AWS Dikelola untuk mencegah masalah deputy yang membingungkan.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Principal": {
    "Service": "ds.amazonaws.com"
  },
  "Action": [
    "SNS:GetTopicAttributes",
    "SNS:SetTopicAttributes",
    "SNS:AddPermission",
    "SNS:RemovePermission",
    "SNS:DeleteTopic",
    "SNS:Subscribe",
    "SNS:ListSubscriptionsByTopic",
    "SNS:Publish"
  ],
  "Resource": [
    "arn:aws:sns:us-east-1:111122223333:SNS_TOPIC_NAME"
  ],
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:ds:us-east-1:111122223333:directory/EXTERNAL_DIRECTORY_ID"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
}

```

Contoh berikut menunjukkan kebijakan kepercayaan IAM untuk peran yang telah didelegasikan akses konsol. Nilai `aws:SourceArn` harus berupa sumber daya direktori di akun Anda. Untuk informasi selengkapnya, lihat [Jenis sumber daya yang ditentukan oleh Directory Service](#). Misalnya, Anda dapat menggunakan `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890` di `123456789012` mana ID pelanggan Anda dan `d-1234567890` ID direktori Anda.

JSON

```

{
  "Version": "2012-10-17",

```



```
"Statement": {
  "Effect": "Allow",
  "Principal": {
    "Service": "ds.amazonaws.com"
  },
  "Action": [
    "sts:AssumeRole"
  ],
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/YOUR_DIRECTORY_ID"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
}
```

Directory Service API dan antarmuka titik akhir Amazon VPC menggunakan AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan Directory Service dan Directory Service Data. APIs Ini memungkinkan Anda untuk mengakses Directory Service dan Directory Service Data APIs seperti yang ada di VPC Anda dan tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. Direct Connect Instans di Amazon VPC Anda tidak memerlukan alamat IP publik untuk Directory Service mengakses dan Directory Service Data. APIs

Untuk membuat koneksi pribadi, Anda membuat antarmuka titik akhir VPC Amazon yang mendukung. AWS PrivateLink Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola oleh permintaan, yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan untuk dan Directory AWS Directory Service Service Data. AWS

Untuk informasi selengkapnya, lihat [Aksees Layanan AWS melalui AWS PrivateLink](#) di AWS PrivateLink Panduan.

Pertimbangan untuk Directory Service dan Directory Service Data

Dengan Directory Service dan Directory Service Data, Anda dapat memanggil tindakan API melalui titik akhir antarmuka. Untuk informasi tentang prasyarat yang perlu Anda pertimbangkan sebelum membuat titik akhir antarmuka, lihat [Mengakses menggunakan Layanan AWS antarmuka titik akhir Amazon VPC](#) di Panduan.AWS PrivateLink

Directory Service dan Ketersediaan Data Directory Service

Directory Service dan Directory Service Data mendukung titik akhir antarmuka di semua Wilayah AWS tempat yang tersedia. Untuk informasi tentang dukungan Wilayah AWS tersebut Directory Service dan Directory Service Data, lihat [Ketersediaan wilayah untuk Directory Service](#).

Buat antarmuka titik akhir Amazon VPC untuk dan Directory Directory Service Service Data

Anda dapat membuat titik akhir antarmuka untuk Directory Service dan Directory Service Data APIs menggunakan konsol Amazon VPC atau AWS Command Line Interface ().AWS CLI

Contoh: Directory Service

Buat titik akhir antarmuka untuk Directory Service APIs menggunakan nama layanan berikut:

```
com.amazonaws.region.ds
```

Contoh: Directory Service Data

Buat endpoint antarmuka untuk Directory Service Data APIs menggunakan nama layanan berikut:

```
com.amazonaws.region.ds-data
```

Untuk informasi selengkapnya tentang membuat titik akhir antarmuka, lihat [Mengakses Layanan AWS menggunakan antarmuka titik akhir Amazon VPC](#) di Panduan.AWS PrivateLink

Buat kebijakan titik akhir VPC Amazon untuk antarmuka Anda Titik akhir Amazon VPC

Kebijakan endpoint adalah kebijakan sumber daya IAM yang Anda lampirkan ke titik akhir antarmuka.

 Note

Jika Anda tidak melampirkan kebijakan titik akhir ke titik akhir antarmuka Anda, AWS PrivateLink lampirkan kebijakan titik akhir default ke titik akhir antarmuka Anda atas nama Anda. Untuk informasi lebih lanjut, lihat [AWS PrivateLink konsep](#).

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal (Akun AWS, pengguna IAM, dan peran IAM) yang dapat melakukan tindakan
- Tindakan-tindakan yang dapat dilakukan
- Sumber daya di mana tindakan dapat dilakukan

Untuk informasi selengkapnya, lihat [Mengontrol akses ke layanan menggunakan kebijakan titik akhir](#) di Panduan AWS PrivateLink .

Anda dapat mengontrol akses APIs dari VPC Amazon Anda dengan melampirkan kebijakan endpoint kustom ke titik akhir antarmuka Anda.

Contoh: Kebijakan titik akhir Amazon VPC untuk tindakan API Directory Service

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka Anda, kebijakan ini akan memberikan akses ke Directory Service tindakan yang tercantum untuk semua prinsip di semua sumber daya.

Ganti *action-1* *action-2*, dan *action-3* dengan izin yang diperlukan untuk Directory Service APIs yang ingin Anda sertakan dalam kebijakan Anda. Untuk daftar lengkap, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#).

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "ds:action-1",
        "ds:action-2",
        "ds:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}  
]  
}
```

Contoh: Kebijakan endpoint Amazon VPC untuk tindakan Directory Service Data API

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka Anda, kebijakan ini akan memberikan akses ke tindakan Directory Service Data yang terdaftar untuk semua prinsipal di semua sumber daya.

Ganti *action-1*, *action-2*, dan *action-3* dengan izin yang diperlukan untuk Directory Service Data APIs yang ingin Anda sertakan dalam kebijakan Anda. Untuk daftar lengkap, lihat [Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi](#).

```
{  
  "Statement": [  
    {  
      "Principal": "*",  
      "Effect": "Allow",  
      "Action": [  
        "ds-data:action-1",  
        "ds-data:action-2",  
        "ds-data:action-3"  
      ],  
      "Resource": "*"   
    }  
  ]  
}
```

Perjanjian tingkat layanan untuk Directory Service

Directory Service adalah layanan yang sangat tersedia, dan dibangun di atas infrastruktur AWS yang dikelola. Ini didukung oleh perjanjian tingkat layanan (SLA) yang menentukan kebijakan ketersediaan layanan kami.

- SLA berlaku untuk AWS Managed Microsoft AD, AD Connector, dan Simple AD.
- SLA membahas kredit layanan, pengecualian SLA, dan mendefinisikan istilah seperti “Direktori Tercakup”, “Persentase Uptime Bulanan”, dan “Permintaan”.
- Untuk informasi selengkapnya, lihat [Perjanjian tingkat layanan untuk Directory Service](#).

Ketersediaan wilayah untuk Directory Service

Tabel berikut menyediakan daftar yang menjelaskan titik akhir khusus Region yang didukung oleh jenis direktori.

Nama Region	Wilayah	Titik Akhir	Protoko	AWS Microso AD yang Dikelola (Edisi Standar dan Perusahaan)	AWS Microso AD yang Dikelola (Edisi Hybrid)	AD Connec	Simple AD
US East (Northern Virginia)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Ya
AS Timur (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Tidak
AS Barat (California Utara)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Tidak
AS Barat (Oregon)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Ya

Nama Region	Wilayah	Titik Akhir	Protoko	AWS Microso AD yang Dikelola (Edisi Standar dan Perusa n)	AWS Microso AD yang Dikelola (Edisi Hybrid)	AD Connec	Simple AD
Africa (Cape Town)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Asia Pasifik (Hong Kong)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Asia Pasifik (Taipei)	ap-timur-2	ds.ap-east-2.amazonaws.com	HTTPS	 Y	 T	 Y	 Tidak
Asia Pasifik (Hyderabad)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Asia Pasifik (Jakarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Asia Pasifik (Malaysia)	ap-southeast-5	ds.ap-southeast-5.amazonaws.com	HTTPS	 Y	 T	 Y	 Tidak

Nama Region	Wilayah	Titik Akhir	Protoko	AWS Microso AD yang Dikelola (Edisi Standar dan Perusa n)	AWS Microso AD yang Dikelola (Edisi Hybrid)	AD Connec	Simple AD
Asia Pacific (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Asia Pasifik (Thailand)	ap-tenggara 7	ds.ap-southeast-7.amazonaws.com	HTTPS	 Y	 T	 Y	 Tidak
Asia Pasifik (Seland Baru)	ap-tenggara 6	ds.ap-southeast-6.amazonaws.com	HTTPS	 Y	 T	 Y	 Tidak
Asia Pasifik (Mumbai)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Asia Pacific (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Asia Pasifik (Seoul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak

Nama Region	Wilayah	Titik Akhir	Protoko	AWS Microso AD yang Dikelola (Edisi Standar dan Perusahaan)	AWS Microso AD yang Dikelola (Edisi Hybrid)	AD Connec	Simple AD
Asia Pasifik (Singapura)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Ya
Asia Pasifik (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Ya
Asia Pasifik (Tokyo)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Ya
Kanada (Pusat)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Tidak
Kanada Barat (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 Ya	 Tidak	 Ya	 Tidak
Tiongkok (Beijing)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 Ya	 Tidak	 Ya	 Tidak

Nama Region	Wilayah	Titik Akhir	Protoko	AWS Microso AD yang Dikelola (Edisi Standar dan Perusahaan)	AWS Microso AD yang Dikelola (Edisi Hybrid)	AD Connec	Simple AD
Tiongkok (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	 Ya	 Tidak	 Ya	 Tidak
Europa (Frankfurt)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Tidak
Europa (Irlandia)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Ya
Europa (London)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Tidak
Europa (Milan)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Tidak
Europa (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Tidak
Europa (Spanyol)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	 Ya	 Ya	 Ya	 Tidak

Nama Region	Wilayah	Titik Akhir	Protoko	AWS Microso AD yang Dikelola (Edisi Standar dan Perusahaan)	AWS Microso AD yang Dikelola (Edisi Hybrid)	AD Connec	Simple AD
Europa (Stockholm)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Europe (Zurich)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Israel (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	 Y	 T	 Y	 Tidak
Meksiko (Tengah)	mx-central-1	ds.mx-central-1.amazonaws.com	HTTPS	 Y	 T	 Y	 Tidak
Timur Tengah (Bahrain)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
Timur Tengah (UAE)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak

Nama Region	Wilayah	Titik Akhir	Protoko	AWS Microso AD yang Dikelola (Edisi Standar dan Perusa n)	AWS Microso AD yang Dikelola (Edisi Hybrid)	AD Connec	Simple AD
Amerika Selatan (Sao Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	 Y	 Y	 Y	 Tidak
AWS GovCloud (AS-Barat)	us-gov-west-1	ds.us-gov-west-1.amazonaws.com	HTTPS	 Y	 T	 Y	 Tidak
AWS GovCloud (AS-Timur)	us-gov-east-1	ds.us-gov-east-1.amazonaws.com	HTTPS	 Y	 T	 Y	 Tidak

Untuk informasi tentang penggunaan Directory Service di Wilayah AWS GovCloud (AS-Barat) dan Wilayah AWS GovCloud (AS-Timur), lihat [Titik akhir Layanan di Panduan Pengguna AWS GovCloud \(US\)](#)

Untuk informasi tentang penggunaan Directory Service di Wilayah Beijing dan Ningxia, lihat [Titik Akhir dan ARNs untuk Amazon Web Services di Tiongkok di Memulai di AWS Tiongkok](#).

Untuk informasi tentang endpoint FIPS yang didukung Directory Service Data, lihat [titik akhir dan kuota Directory Service Data di Panduan Referensi](#). Referensi Umum AWS

Didukung Wilayah AWS untuk Directory Service Data

Tabel berikut menyediakan daftar titik akhir khusus Wilayah yang didukung Directory Service Data menurut jenis direktori.

Nama wilayah	Wilayah	Titik Akhir	Protokol	AWS Microsoft AD yang dikelola	AD Connect	Simple AD
US East (Ohio)	us-east-2	ds-data.us-east-2.amazonaws.com	HTTPS	 Y	 T	 Tidak
US East (Northern Virginia)	us-east-1	ds-data.us-east-1.amazonaws.com	HTTPS	 Y	 T	 Tidak
AS Barat (California Utara)	us-west-1	ds-data.us-west-1.amazonaws.com	HTTPS	 Y	 T	 Tidak
AS Barat (Oregon)	us-west-2	ds-data.us-west-2.amazonaws.com	HTTPS	 Y	 T	 Tidak
Asia Pasifik (Hong Kong)	ap-east-1	ds-data.ap-east-1.amazonaws.com	HTTPS	 Y	 T	 Tidak
Asia Pasifik (Mumbai)	ap-south-1	ds-data.ap-south-1.amazonaws.com	HTTPS	 Y	 T	 Tidak

Nama wilayah	Wilayah	Titik Akhir	Protokol	AWS Microsoft AD yang dikelola	AD Connect	Simple AD
Asia Pacific (Osaka)	ap-northeast-3	ds-data.ap-northeast-3.amazonaws.com	HTTPS	 Y	 T	 Tidak
Asia Pasifik (Seoul)	ap-northeast-2	ds-data.ap-northeast-2.amazonaws.com	HTTPS	 Y	 T	 Tidak
Asia Pasifik (Singapura)	ap-southeast-1	ds-data.ap-southeast-1.amazonaws.com	HTTPS	 Y	 T	 Tidak
Asia Pasifik (Sydney)	ap-southeast-2	ds-data.ap-southeast-2.amazonaws.com	HTTPS	 Y	 T	 Tidak
Asia Pasifik (Tokyo)	ap-northeast-1	ds-data.ap-northeast-1.amazonaws.com	HTTPS	 Y	 T	 Tidak
Kanada (Pusat)	ca-central-1	ds-data.ca-central-1.amazonaws.com	HTTPS	 Y	 T	 Tidak
Europa (Frankfurt)	eu-central-1	ds-data.eu-central-1.amazonaws.com	HTTPS	 Y	 T	 Tidak
Europa (Irlandia)	eu-west-1	ds-data.eu-west-1.amazonaws.com	HTTPS	 Y	 T	 Tidak

Nama wilayah	Wilayah	Titik Akhir	Protokol	AWS Microsoft AD yang dikelola	AD Connect	Simple AD
Eropa (London)	eu-west-2	ds-data.eu-west-2.amazonaws.com	HTTPS	 Y	 T	 Tidak
Eropa (Paris)	eu-west-3	ds-data.eu-west-3.amazonaws.com	HTTPS	 Y	 T	 Tidak
Eropa (Stockholm)	eu-north-1	ds-data.eu-north-1.amazonaws.com	HTTPS	 Y	 T	 Tidak
Amerika Selatan (Sao Paulo)	sa-east-1	ds-data.sa-east-1.amazonaws.com	HTTPS	 Y	 T	 Tidak

Untuk informasi tentang endpoint FIPS yang didukung Directory Service Data, lihat [titik akhir dan kuota Directory Service Data di Panduan Referensi](#). Referensi Umum AWS

Kompatibilitas browser untuk AWS Directory Service

AWS aplikasi dan layanan seperti WorkSpaces, Amazon, Amazon WorkMail Connect, Amazon Chime WorkDocs, dan AWS IAM Identity Center semuanya memerlukan kredensial masuk yang valid dari browser yang kompatibel sebelum Anda dapat mengaksesnya. Tabel berikut menjelaskan hanya peramban dan versi peramban yang kompatibel untuk masuk.

Peramban	Versi	Kompatibilitas
Microsoft Edge	Versi 3 Terbaru	Kompatibel
Mozilla Firefox	Versi 3 Terbaru	Kompatibel
Google Chrome	Versi 3 Terbaru	Kompatibel
Apple Safari	Versi 3 Terbaru	Kompatibel

Sekarang setelah Anda memverifikasi bahwa Anda menggunakan versi browser yang didukung, kami sarankan Anda juga meninjau bagian di bawah ini untuk memverifikasi browser Anda telah dikonfigurasi untuk menggunakan pengaturan Transport Layer Security (TLS) yang diperlukan oleh AWS.

Apa itu TLS?

TLS adalah peramban web protokol dan aplikasi lain yang digunakan untuk bertukar data secara aman melewati jaringan. TLS memastikan bahwa hubungan ke titik akhir jauh adalah titik akhir yang dimaksudkan melalui enkripsi dan verifikasi identitas titik akhir. Versi TLS, hingga saat ini, adalah TLS 1.0, 1.1, 1.2 dan 1.3.

Versi TLS mana yang didukung oleh IAM Identity Center

AWS aplikasi dan layanan mendukung TLS 1.1, 1.2 dan 1.3 untuk login aman. Mulai 30 Oktober 2019, TLS 1.0 tidak lagi didukung, jadi penting agar semua peramban dikonfigurasi untuk mendukung TLS 1.1 atau yang di atasnya. Ini berarti, Anda tidak akan dapat masuk ke aplikasi dan layanan AWS jika Anda mengaksesnya saat TLS 1.0 diaktifkan. Untuk bantuan dalam membuat perubahan ini, kontak admin Anda.

Bagaimana cara mengaktifkan versi TLS yang didukung di peramban saya

Hal ini tergantung pada peramban Anda. Biasanya Anda dapat menemukan pengaturan ini di bawah area pengaturan lanjutan di pengaturan peramban Anda. Misalnya, di Internet Explorer Anda akan menemukan berbagai opsi TLS di bawah Internet Properties, tab Advanced, dan kemudian di bawah bagian Keamanan. Periksa situs web Bantuan produsen browser Anda untuk petunjuk spesifik.

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir dari AWS Directory Service Panduan Administrator.

Perubahan	Deskripsi	Tanggal
Dukungan tipe jaringan dual-stack	AWS Directory Service sekarang mendukung upgrade jenis jaringan direktori dari IPv4 ke dual stack (IPv4 dan IPv6). Fitur ini menyediakan ruang alamat yang lebih besar dan memungkinkan IPv6 konektivitas untuk direktori Anda. Anda juga dapat memperbarui direktori AD Connector dan direktori Simple AD dengan dukungan dual stack .	September 30, 2025
Peran terkait AWS layanan baru	Directory Service menambahkan peran terkait AWS layanan baru, <code>AWSServiceRoleForDirectoryService</code> dan kebijakan <code>AWSManagedAWSDirectoryServiceServiceRolePolicy</code> . Kebijakan memungkinkan AWS untuk memantau pengontrol domain yang dikelola pelanggan.	Juli 30, 2025
AWS Microsoft AD yang Dikelola (Edisi Hybrid)	AWS Microsoft AD (Edisi Hybrid) yang dikelola sendiri menghubungkan Active Directory yang dikelola sendiri dengan AWS Directory	Juli 30, 2025

Service untuk Microsoft Active Directory, menciptakan lingkungan identitas terintegrasi yang mencakup infrastruktur dan jaringan. AWS Cloud

[Topik logging dan pemantauan yang diperbarui - bagian baru](#)

Termasuk bagian untuk AWS Directory Service dan AWS Directory Service Data dalam topik logging dan monitoring.

September 18, 2024

[API dan atribut Directory Service Data baru](#)

AWS Directory Service Data menyediakan manajemen objek bawaan. Sekarang Anda dapat menemukan dan memperbarui objek dengan [daftar atribut AD yang didukung](#).

September 18, 2024

[AWS kebijakan terkelola - kebijakan baru](#)

AWS Directory Service Data menambahkan kebijakan AWS terkelola baru: AWSDirectoryServiceDataFullAccess dan AWSDirectoryServiceDataReadOnlyAccess. Kebijakan memberikan akses ke manajemen objek Directory Service Data.

September 18, 2024

[Pengaturan otentikasi berbasis sertifikat](#)

Menambahkan konten tentang dua pengaturan keamanan baru untuk Microsoft AD yang AWS Dikelola.

11 April 2023

[AWS PrivateLink](#)

Menambahkan konten tentang AWS PrivateLink.

31 Maret 2023

Titik Akhir VPC AD Sederhana	Menambahkan konten tentang titik akhir VPC mana yang tidak boleh dikonfigurasi.	25 Agustus 2021
Titik Akhir VPC Konektor AD	Menambahkan konten tentang titik akhir VPC mana yang tidak boleh dikonfigurasi.	25 Agustus 2021
Dukungan kartu pintar	Menambahkan konten tentang dukungan untuk kartu pintar dan Amazon WorkSpace s Application Manager di Wilayah AWS GovCloud (AS-Barat)	1 Desember 2020
Reset kata sandi	Menambahkan konten tentang cara mengatur ulang kata sandi pengguna menggunakan Konsol Manajemen AWS, PowerShell dan AWS CLI.	2 Januari 2019
Berbagi direktori	Menambahkan konten tentang cara menggunakan berbagi direktori dengan Microsoft AD yang AWS Dikelola.	25 September 2018
Konten yang dimigrasi ke Panduan Pengembang Amazon Cloud Directory baru	Memindahkan konten Amazon Cloud Directory dari panduan ini ke Panduan Pengembang Amazon Cloud Directory yang baru.	21 Juni 2018
Perombakan lengkap panduan admin TOC	Menata ulang konten untuk lebih langsung memenuhi kebutuhan pelanggan. Juga menambahkan konten baru jika diperlukan.	5 April 2018

AWS kelompok yang didelegasikan	Menambahkan daftar grup AWS yang didelegasikan yang dapat ditetapkan ke pengguna lokal.	8 Maret 2018
Kebijakan kata sandi berbutir halus	Menambahkan konten tentang kebijakan kata sandi baru.	5 Juli 2017
Pengontrol domain tambahan	Menambahkan konten tentang cara menambahkan lebih banyak pengontrol domain ke direktori Anda di Microsoft AD yang AWS Dikelola.	30 Juni 2017
Tutorial	Menambahkan tutorial baru untuk menguji lingkungan lab Microsoft AD AWS Terkelola.	21 Juni 2017
MFA dengan AWS Microsoft AD yang Dikelola	Menambahkan konten tentang penggunaan MFA dengan AWS Microsoft AD yang Dikelola.	13 Februari 2017
Amazon Cloud Directory	Menambahkan konten tentang jenis direktori baru.	26 Januari 2017
Ekstensi skema	Menambahkan konten tentang ekstensi skema dengan AWS Directory Service untuk Microsoft Active Directory.	14 November 2016
Reorganisasi besar dari Panduan Directory Service Administrator	Menata ulang konten untuk lebih langsung memenuhi kebutuhan pelanggan.	14 November 2016
Pemberitahuan SNS	Menambahkan konten tentang notifikasi SNS.	25 Februari 2016

Otorisasi dan otentikasi	Menambahkan konten tentang cara menggunakan IAM dengan Directory Service.	25 Februari 2016
AWS Microsoft AD yang dikelola	Menambahkan konten tentang Microsoft AD yang AWS Dikelola dan panduan gabungan ke dalam satu panduan.	17 November 2015
Izinkan instance Linux untuk digabungkan ke direktori Simple AD	Menambahkan konten tentang cara menggabungkan instance Linux ke direktori Simple AD.	23 Juli 2015
Pemisahan panduan	Pisahkan Panduan Directory Service Administrasi menjadi panduan terpisah.	14 Juli 2015
Dukungan masuk tunggal	Menambahkan konten tentang dukungan untuk sistem masuk tunggal.	31 Maret 2015
Panduan baru	Ini adalah rilis pertama dari AWS Directory Service Panduan Administrasi.	21 Oktober 2014

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.