Panduan Pengguna

VMware Layanan Elastis Amazon

VMware Layanan Elastis Amazon: Panduan Pengguna

Table of Contents

Apa itu Amazon Elastic VMware Service?

Anda dapat menggunakan Amazon Elastic VMware Service (Amazon EVS) untuk menerapkan dan menjalankan lingkungan VMware Cloud Foundation (VCF) secara langsung pada instans EC2 bare metal di dalam (VPC). Amazon Virtual Private Cloud

Topik

Fitur Amazon EVS

Berikut ini adalah fitur utama Amazon EVS:

Sederhanakan dan percepat migrasi Anda ke AWS

Hapus gesekan migrasi dan pastikan konsistensi operasional dengan portabilitas langganan dan penerapan otomatis VMware Cloud Foundation (VCF) di cloud. Memperluas jaringan lokal dan memigrasikan beban kerja tanpa harus mengubah alamat IP, melatih kembali staf, atau menulis ulang runbook operasional.

Pertahankan kontrol VMware arsitektur Anda di cloud

Pertahankan kontrol penuh atas VMware arsitektur Anda dan optimalkan tumpukan virtualisasi yang memenuhi tuntutan unik aplikasi Anda, termasuk add-on dan solusi pihak ketiga.

Mengelola sendiri atau memanfaatkan AWS Mitra untuk pengalaman terkelola

Buka pilihan dan fleksibilitas untuk mengelola sendiri, atau manfaatkan keahlian AWS Mitra untuk mengelola dan mengoperasikan lingkungan VCF Anda AWS untuk memenuhi tujuan bisnis Anda di seluruh bakat, waktu, dan biaya.

Skala dan lindungi bisnis Anda dari gangguan

Tingkatkan skalabilitas pada cloud yang paling aman, terukur, dan tangguh untuk memigrasi dan mengoperasikan beban kerja berbasis Anda. VMware

Merangkul AWS inovasi untuk mengubah aplikasi dan infrastruktur Anda

Sebagai layanan AWS asli, Amazon EVS menyederhanakan perluasan dan perluasan VMware lingkungan Anda dengan 200+ layanan (termasuk database terkelola, analitik, tanpa server dan wadah, dan AI generatif) untuk mengubah bisnis Anda.

Memulai Amazon EVS

Untuk membuat lingkungan Amazon EVS pertama Anda, lihatMulai menggunakan. Secara umum, memulai dengan Amazon EVS melibatkan menyelesaikan langkah-langkah berikut.

1. Prasyarat lengkap. Untuk informasi selengkapnya, lihat Menyiapkan VMware Layanan Elastis Amazon.
2. Buat lingkungan Amazon EVS. Selama pembuatan lingkungan, Amazon EVS membuat subnet VLAN yang diperlukan menggunakan rentang CIDR yang Anda tentukan dan menambahkan host ke lingkungan.
3. Sesuaikan VCF. Konfigurasikan lingkungan Anda di antarmuka pengguna vSphere sesuai dengan kebutuhan Anda. Ini mungkin termasuk menyiapkan login, kebijakan, pemantauan, dan banyak lagi.
4. Connect dan migrasi. Hubungkan lingkungan Anda ke pusat data lokal dan migrasi beban kerja VCF Anda ke Amazon EVS.

Mengakses Amazon EVS

Anda dapat menentukan dan mengonfigurasi penerapan Amazon EVS menggunakan antarmuka berikut:

- Konsol Amazon EVS - Menyediakan antarmuka web untuk membuat lingkungan Amazon EVS.
- AWS CLI - Menyediakan perintah untuk serangkaian luas Layanan AWS dan didukung pada Windows, macOS, dan Linux. Untuk informasi selengkapnya, lihat AWS Command Line Interface.
- AWS CloudFormation - Menyediakan spesifikasi untuk setiap jenis sumber daya, sepertiAWS::EVS::Environment. Anda membuat template menggunakan spesifikasi sumber daya, dan CloudFormation mengurus penyediaan dan konfigurasi sumber daya untuk Anda.

Konsep dan komponen Amazon EVS

Bagian ini menjelaskan beberapa konsep dan komponen Amazon EVS utama.

Lingkungan Amazon EVS

Lingkungan Amazon EVS adalah wadah logis untuk sumber daya VMware Cloud Foundation (VCF), seperti host vSphere, vSAN, NSX, dan Manajer SDDC. Lingkungan berisi domain VCF gabungan dengan sebuah klaster vSphere yang meng-host komponen untuk mengelola, memantau, dan menginisiasi tumpukan perangkat lunak VCF. Setiap lingkungan langsung memetakan ke alat Manajer SDDC. Untuk informasi selengkapnya, lihat the section called “Arsitektur ”.

Tuan rumah Amazon EVS

Host Amazon EVS adalah host VMware ESX yang berjalan pada instans Amazon EC2 bare metal. Host Amazon EVS menggunakan volume penyimpanan NVMe instans lokal untuk datastores vSAN, yang menyimpan mesin virtual manajemen dan beban kerja Anda.

> **Warning**
>
> Volume penyimpanan instans bersifat fana. Data yang disimpan pada volume ini tidak bertahan jika instans EC2 yang mendasarinya dihentikan atau dihentikan. Menghentikan atau menghentikan Amazon EC2 instans yang digunakan oleh Amazon EVS tanpa dekomisi dalam VCF dapat mengakibatkan kehilangan data.
> Untuk informasi selengkapnya tentang pemeliharaan host, lihatthe section called “Pemeliharaan host”.

Subnet akses layanan

Subnet akses layanan adalah subnet VPC standar yang memungkinkan Amazon EVS mengakses penyebaran VCF. Selama pembuatan lingkungan Amazon EVS, Anda menentukan VPC dan subnet untuk Amazon EVS yang akan digunakan untuk akses layanan.

Saat Anda membuat lingkungan Amazon EVS, Amazon EVS menyediakan antarmuka jaringan elastis ke dalam subnet akses layanan untuk memfasilitasi konektivitas manajemen ke peralatan VCF dan host ESX. Konektivitas ini diperlukan agar Amazon EVS dapat menyebarkan, mengelola, dan memantau penyebaran VCF.

Amazon EVS VLAN subnet

Subnet Amazon EVS VLAN adalah subnet Amazon VPC yang dikelola oleh Amazon EVS. Subnet VLAN menyediakan konektivitas VPC untuk host Amazon EVS, dan peralatan VCF seperti NSX, HCX VMware , dan vCenter Server. VMware VMware Setiap subnet VLAN memiliki tag VLAN untuk memungkinkan lalu lintas jaringan VLAN tersegmentasi secara logis.

Amazon EVS membuat semua subnet VLAN yang digunakan layanan saat lingkungan Amazon EVS dibuat. Anda memberikan input blok CIDR yang digunakan subnet VLAN. Anda harus memastikan bahwa blok CIDR subnet VLAN Anda berukuran benar sesuai dengan jumlah host yang akan dikonfigurasi, dengan mempertimbangkan kebutuhan penskalaan masa depan. Blok CIDR harus memiliki ukuran minimum/28 netmask dan ukuran maksimum/24 netmask. Blok CIDR tidak boleh tumpang tindih dengan blok CIDR yang ada yang terkait dengan VPC.

Saat pembuatan, subnet VLAN secara implisit terkait dengan tabel rute utama VPC Anda. Pasca-penerapan Anda dapat secara eksplisit mengaitkan subnet VLAN dengan tabel rute khusus. Untuk informasi selengkapnya, lihat the section called “Pertimbangan jaringan Amazon EVS”.

Important

Subnet Amazon EVS VLAN hanya dapat dibuat selama pembuatan lingkungan Amazon EVS, dan tidak dapat dimodifikasi setelah lingkungan dibuat. Anda harus memastikan bahwa blok CIDR subnet VLAN berukuran benar sebelum membuat lingkungan. Anda tidak akan dapat menambahkan subnet VLAN setelah lingkungan digunakan.

Important

Aturan grup keamanan EC2 tidak diberlakukan pada antarmuka jaringan elastis Amazon EVS yang dilampirkan ke subnet VLAN. Untuk mengontrol lalu lintas ke dan dari subnet VLAN, Anda harus menggunakan daftar kontrol akses jaringan.

Manajemen host VLAN subnet

Subnet VLAN manajemen host memisahkan lalu lintas manajemen dari lalu lintas pengguna, dan memungkinkan manajemen host jarak jauh. Antarmuka jaringan vmkernel manajemen host EVS terhubung ke subnet ini.

VMotion VLAN subnet

Subnet VMotion VLAN secara logis menyegmentasikan lalu lintas VMware vMotion, dan digunakan selama proses vMotion untuk memindahkan mesin virtual antar host.

VSan VLAN subnet

Subnet VSAN VLAN digunakan oleh vSAN VMware untuk memisahkan lalu lintas yang terkait dengan operasi penyimpanan vSAN dari lalu lintas jaringan lainnya.

Subnet VTEP VLAN

Subnet VTEP VLAN menggunakan titik akhir terowongan virtual VMware NSX (VTEP) untuk merangkum dan mendekapsulasi lalu lintas jaringan overlay untuk host Amazon EVS ESX.

Tepi VTEP VLAN subnet

Subnet Edge VTEP VLAN adalah subnet VTEP VLAN khusus yang didedikasikan untuk lalu lintas overlay alat NSX Edge. VLAN ini digunakan untuk komunikasi overlay antara tepi NSX dan host ESX.

Manajemen VM VLAN subnet

Subnet Management VM VLAN digunakan untuk mengelola peralatan virtual, termasuk NSX Manager, vCenter Server, dan SDDC Manager.

Subnet VLAN uplink HCX

Subnet VLAN uplink HCX digunakan untuk komunikasi antara peralatan HCX Interconnect (HCX-IX) dan HCX Network Extension (HCX-NE), dan memungkinkan pembuatan uplink mesh layanan HCX.

Subnet VLAN uplink NSX

Subnet VLAN uplink NSX digunakan untuk menghubungkan jaringan overlay NSX Anda ke seluruh VPC Anda dan jaringan eksternal lainnya yang Anda konfigurasikan. Subnet VLAN uplink NSX dikonfigurasi pada uplink node NSX Edge.

Ekspansi VLAN subnet

Subnet VLAN ekspansi dapat digunakan untuk mengaktifkan fungsi tambahan yang didukung VCF, seperti Federasi NSX. Amazon EVS menciptakan dua subnet VLAN ekspansi selama pembuatan lingkungan.

VMware NSX

VMware NSX adalah platform software-defined networking (SDN) yang memungkinkan virtualisasi jaringan. Amazon EVS menggunakan VMware NSX untuk membuat dan mengelola jaringan overlay tempat peralatan dan beban kerja VMware Cloud Foundation (VCF) berjalan. Amazon EVS menyebarkan sepasang node Active/Standby NSX Edge, bersama dengan jaringan overlay NSX. Amazon EVS secara otomatis mengonfigurasi semua perutean dan uplink NSX atas nama Anda sebagai bagian dari penerapan. Untuk informasi lebih lanjut tentang konsep NSX umum, lihat Konsep Utama dalam Panduan Instalasi VMware NSX.

VMware Ekstensi Cloud Hybrid (HCX)

VMware Hybrid Cloud Extension (VMware HCX) adalah platform mobilitas aplikasi yang dirancang untuk menyederhanakan migrasi aplikasi, menyeimbangkan kembali beban kerja, dan mengoptimalkan pemulihan bencana di seluruh pusat data dan cloud. Anda dapat menggunakan HCX untuk memigrasikan beban kerja VMware berbasis Anda ke Amazon EVS.

Anda dapat mengonfigurasi konektivitas untuk VMware HCX menggunakan Direct Connect gateway transit terkait, atau menggunakan lampiran AWS Site-to-Site VPN ke gateway transit. Lihat informasi yang lebih lengkap di Migrasi.

Arsitektur Amazon EVS

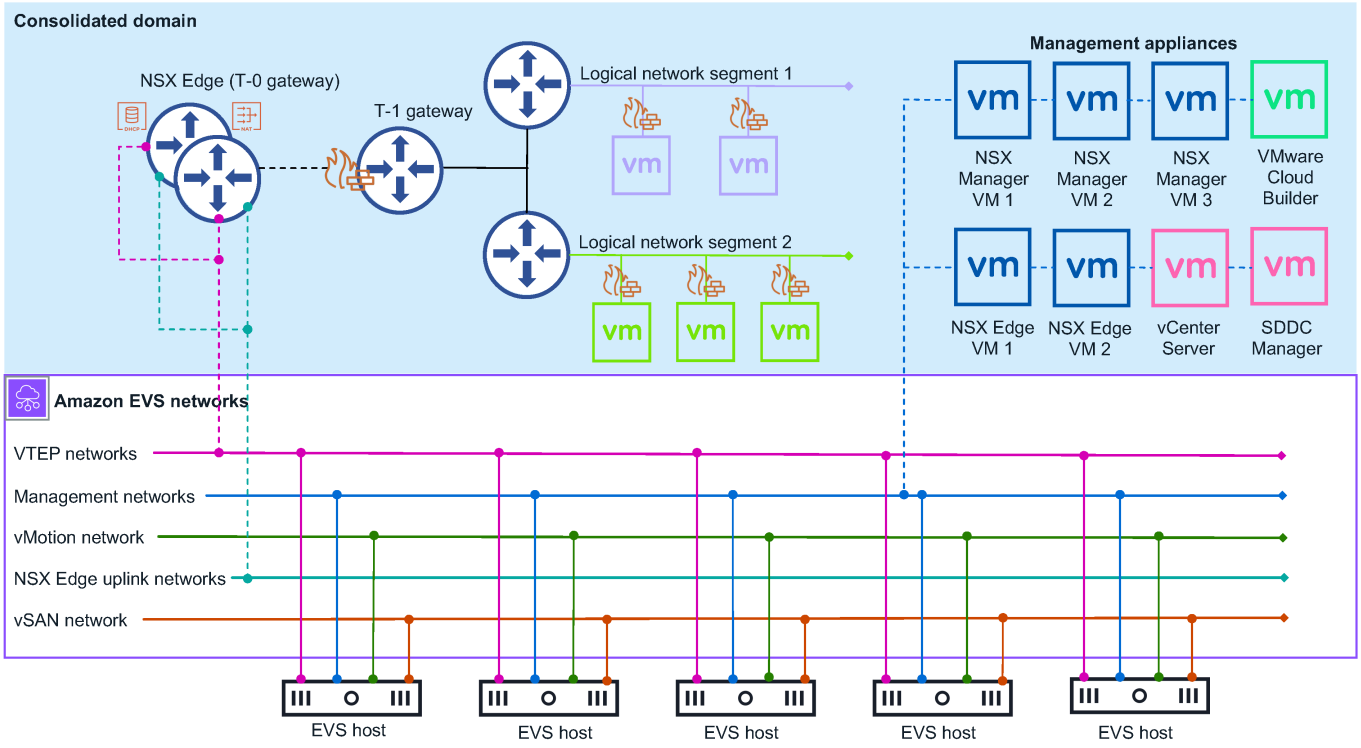
Amazon EVS mengimplementasikan model arsitektur terkonsolidasi VMware Cloud Foundation (VCF). Dalam model ini, komponen manajemen VCF dan beban kerja pelanggan berjalan bersama pada domain terkonsolidasi. Lingkungan Amazon EVS dikelola dari Server vCenter tunggal dengan kumpulan sumber daya vSphere yang menyediakan isolasi antara manajemen dan beban kerja pelanggan.

Domain konsolidasi yang digunakan Amazon EVS berisi komponen manajemen VCF berikut:

- Tuan rumah ESX
- vCenter Server contoh
- Manajer SDDC
- vSan Datastore
- Kluster Manajer NSX tiga simpul
- kluster vSphere

- Kluster Tepi NSX

Diagram berikut menunjukkan contoh arsitektur Amazon EVS yang telah diterapkan di lingkungan Amazon EVS, dan menunjukkan bagaimana komponen di lingkungan terhubung. Dalam diagram, lingkungan Amazon EVS dengan arsitektur domain terkonsolidasi diarsir dengan warna biru. Topologi jaringan Amazon EVS yang mendasari diilustrasikan dalam garis ungu solid.



Topologi jaringan

Lingkungan Amazon EVS memiliki dua lapisan jaringan manajemen terpisah:

Amazon VPC

VPC Amazon dan subnet Amazon EVS VLAN yang dibuat di VPC selama pembuatan lingkungan membentuk jaringan underlay untuk penyebaran VCF Anda. Infrastruktur ini menyediakan konektivitas untuk jaringan overlay NSX, manajemen host, vMotion, dan VSAN. Amazon VPC Route Server memungkinkan perutean dinamis antara jaringan underlay dan jaringan overlay. Untuk informasi selengkapnya, lihat the section called “Konsep dan komponen”.

> **Note**
>
> Subnet Amazon EVS VLAN digunakan untuk memfasilitasi komunikasi underlay VCF saja. Mesin virtual tamu yang menjalankan beban kerja pelanggan harus digunakan pada jaringan overlay NSX. Penyebaran mesin virtual tamu di jaringan underlay subnet Amazon EVS VLAN tidak didukung.

VMware Jaringan overlay NSX

Amazon EVS mengonfigurasi jaringan overlay NSX atas nama Anda sebagai bagian dari penerapan. Anda dapat mengonfigurasi jaringan overlay NSX tambahan untuk mencapai isolasi jaringan antara beban kerja atau aplikasi yang berbeda dalam lingkungan Amazon EVS Anda. Untuk informasi selengkapnya, lihat Desain Hamparan untuk VMware Cloud Foundation di dokumentasi produk VMware Cloud Foundation.

> **Note**
>
> Amazon EVS hanya mendukung satu gateway tingkat-0 untuk cluster NSX Edge dengan dua Active/Standby node NSX Edge. Gateway tier-0 ini terhubung ke dan mengiklankan semua jaringan overlay yang Anda konfigurasikan untuk digunakan dengan Amazon EVS.

Kedua lapisan jaringan dihubungkan oleh cluster Active/Standby NSX Edge dengan dua node NSX Edge. NSX Edge node memungkinkan komunikasi melalui VPC antara mesin virtual di VLANs, serta konektivitas internet, dan konektivitas pribadi Direct Connect menggunakan AWS Site-to-Site atau VPN dengan gateway transit.

Pertimbangan jaringan Amazon EVS

Jaringan manajemen memerlukan konfigurasi sumber daya jaringan berikut. Anda memberikan masukan ini selama pembuatan lingkungan Amazon EVS. Untuk informasi selengkapnya, lihat the section called “Konsep dan komponen”.

- VPC Amazon. Pastikan blok IPv4 CIDR VPC Anda berukuran tepat untuk mengakomodasi subnet VPC yang diperlukan dan subnet Amazon EVS VLAN yang disediakan Amazon EVS selama pembuatan lingkungan. Untuk informasi selengkapnya, lihat the section called “Amazon EVS VLAN subnet”.

> **Note**
>
> Amazon EVS tidak mendukung IPv6 saat ini.

- Subnet akses layanan di VPC Anda. Amazon EVS menggunakan subnet ini untuk mempertahankan koneksi persisten ke alat SDDC Manager Anda. Untuk informasi selengkapnya, lihat the section called “Subnet akses layanan”.

> **Note**
>
> Amazon EVS hanya mendukung penerapan Single-AZ saat ini. Semua subnet VPC yang digunakan Amazon EVS harus ada di Availability Zone tunggal di Wilayah tempat layanan tersedia.

> **Note**
>
> Semua subnet VPC memerlukan tabel rute terkait yang dikonfigurasi sesuai dengan kebutuhan jaringan organisasi Anda.

- Alamat IP server DNS primer dan alamat IP server DNS sekunder dalam opsi DHCP VPC diatur untuk menyelesaikan alamat IP host. Amazon EVS juga mengharuskan Anda membuat zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan server DNS”.
- Amazon EVS VLAN subnet CIDR memblokir untuk setiap subnet VLAN yang disediakan Amazon EVS untuk Anda selama pembuatan lingkungan. Blok CIDR harus memiliki ukuran minimum/28 netmask dan ukuran maksimum/24 netmask. Blok CIDR harus tidak tumpang tindih.
- Sebuah instance Amazon VPC Route Server dengan propagasi Route Server diaktifkan.
- Dua titik akhir Route Server di subnet akses layanan.
- Dua rekan Route Server yang mengintip node NSX Edge yang disediakan Amazon EVS dengan titik akhir Route Server.

Gerbang tingkat-0

Gateway tier-0 menangani semua lalu lintas utara-selatan antara jaringan logis dan fisik dan dibuat pada jaringan overlay NSX. Gateway tier-0 ini dibuat sebagai bagian dari penyebaran Amazon EVS.

> **Note**
>
> Amazon EVS hanya mendukung satu gateway tingkat-0 untuk cluster NSX Edge dengan dua Active/Standby node NSX Edge.

Gerbang tingkat-1

Gateway tier-1 menangani lalu lintas timur-barat antara segmen jaringan yang dirutekan dalam suatu lingkungan dan dibuat pada jaringan overlay NSX. Gateway tier-1 memiliki koneksi downlink ke segmen dan koneksi uplink ke gateway tier-0. Anda dapat membuat dan mengonfigurasi gateway Tier-1 tambahan jika Anda membutuhkannya.

Kluster Tepi NSX

Amazon EVS menggunakan antarmuka NSX Manager untuk menyebarkan cluster NSX Edge dengan dua node NSX Edge yang berjalan dalam mode. Active/Standby Cluster NSX Edge ini menyediakan platform tempat gateway Tier-0 dan Tier-1 berjalan, bersama dengan IPsec koneksi VPN dan mesin perutean BGP mereka.

Sumber daya Amazon EVS

Amazon EVS menyediakan AWS sumber daya berikut selama pembuatan lingkungan. Sumber daya ini muncul di VPC yang Anda izinkan Amazon EVS untuk diakses, dan terlihat di Konsol Manajemen AWS dan AWS CLI setelah dibuat.

> **Important**
>
> Modifikasi sumber daya ini di luar konsol dan API Amazon EVS dapat memengaruhi ketersediaan dan stabilitas lingkungan Amazon EVS Anda.

- Antarmuka jaringan elastis Amazon EVS yang memungkinkan konektivitas ke peralatan dan host VCF Anda.

- Host Amazon EVS ESX yang berjalan pada instans Amazon EC2 bare metal. Untuk informasi selengkapnya, lihat the section called “Tuan rumah Amazon EVS”.

  > **Important**
  >
  > Lingkungan Amazon EVS Anda harus memiliki minimal 4 host dan tidak lebih dari 16 host. Amazon EVS hanya mendukung lingkungan dengan 4-16 host.

- Subnet Amazon EVS VLAN yang menghubungkan VPC Anda ke peralatan VCF. Lihat informasi yang lebih lengkap di the section called “Amazon EVS VLAN subnet”.

Menyiapkan VMware Layanan Elastis Amazon

Untuk menggunakan Amazon EVS, Anda perlu mengonfigurasi AWS layanan lain, serta menyiapkan lingkungan Anda untuk memenuhi persyaratan VMware Cloud Foundation (VCF). Untuk daftar periksa ringkasan prasyarat penerapan, lihat. the section called “Daftar periksa penerapan”

Topik

Mendaftar untuk AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

1. Buka https://portal.aws.amazon.com/billing/ pendaftaran.
2. Ikuti petunjuk online.

Mmebuat pengguna IAM

1. Masuk ke konsol IAM sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat email AWS akun Anda. Di laman berikutnya, masukkan kata sandi.

   > **Note**
   >
   > Kami sangat menyarankan agar Anda mematuhi praktik terbaik menggunakan `Administrator` Pengguna IAM di bawah dan kunci kredensial pengguna akar secara aman. Masuk sebagai pengguna akar hanya untuk melakukan beberapa tugas manajemen layanan dan akun.

2. Di panel navigasi, pilih Pengguna dan kemudian pilih Buat pengguna.
3. Untuk Nama pengguna, masukkan `Administrator`.
4. Pilih kotak centang di samping akses AWS Management Console. Kemudian pilih Kata sandi khusus, lalu masukkan kata sandi baru Anda di kotak teks.
5. (Opsional) Secara default, AWS mengharuskan pengguna baru untuk membuat kata sandi baru saat pertama kali masuk. Anda dapat mengosongkan kotak centang di samping Pengguna harus membuat kata sandi baru saat masuk berikutnya agar pengguna baru dapat mengatur ulang kata sandi mereka setelah masuk.
6. Pilih Next: Permissions (Selanjutnya: Izin).
7. Di Bagian Set permissions (Atur izin), pilih Add user to group (Tambahkan pengguna ke grup).
8. Pilih Create group (Buat kelompok).
9. Di kotak dialog Buat kelompok, untuk Nama kelompok masukkan `Administrators`.
10. Pilih Filter kebijakan, lalu pilih fungsi -job AWS terkelola untuk memfilter isi tabel.
11. Dalam daftar kebijakan, pilih kotak centang untuk AdministratorAccess. Lalu, pilih Create group (Buat grup).

    > **Note**
    >
    > Anda harus mengaktifkan akses pengguna dan peran IAM ke Penagihan sebelum dapat menggunakan `AdministratorAccess` izin untuk mengakses konsol AWS Billing and Cost Management. Untuk melakukannya, ikuti petunjuk di langkah 1 dari tutorial tentang pendelegasian akses ke konsol penagihan.

12. Kembali ke daftar grup, pilih kotak centang untuk grup baru Anda. Pilih Refresh (Segarkan) jika diperlukan untuk melihat kelompok dalam daftar.
13. Pilih Next: Tags (Selanjutnya: Tanda).
14. (Opsional) Tambahkan metadata ke pengguna dengan melampirkan tanda sebagai pasangan nilai kunci. Untuk informasi selengkapnya tentang penggunaan tanda di IAM, lihat Menandai Entitas IAM dalam Panduan Pengguna IAM.
15. Pilih Next: Review (Selanjutnya: Tinjauan) untuk melihat daftar keanggotaan grup yang akan ditambahkan ke pengguna baru. Saat Anda siap untuk melanjutkan, pilih Create user (Buat pengguna).

Anda dapat menggunakan proses yang sama ini untuk membuat lebih banyak grup dan pengguna dan memberi pengguna akses ke sumber daya AWS akun Anda. Untuk mempelajari cara menggunakan kebijakan yang membatasi izin pengguna ke AWS sumber daya tertentu, lihat Manajemen Akses dan Kebijakan Contoh.

Membuat peran IAM untuk mendelegasikan izin Amazon EVS ke pengguna IAM

Anda dapat menggunakan peran untuk mendelegasikan akses ke AWS sumber daya Anda. Dengan peran IAM, Anda dapat membangun hubungan kepercayaan antara akun kepercayaan Anda dan akun AWS tepercaya lainnya. Akun kepercayaan memiliki sumber daya yang akan diakses, dan akun tepercaya berisi pengguna yang membutuhkan akses ke sumber daya.

Setelah Anda membuat hubungan kepercayaan, pengguna IAM atau aplikasi dari akun tepercaya dapat menggunakan operasi `AssumeRole` API AWS Security Token Service (AWS STS). Operasi ini menyediakan kredensil keamanan sementara yang memungkinkan akses ke AWS sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke pengguna IAM di Panduan Pengguna. AWS Identity and Access Management

Ikuti langkah-langkah ini untuk membuat peran IAM dengan kebijakan izin yang memungkinkan akses ke operasi Amazon EVS.

> **Note**
>
> Amazon EVS tidak mendukung penggunaan profil instans untuk meneruskan peran IAM ke instance EC2 .

Example

IAM console

1. Buka konsol IAM.
2. Di menu sebelah kiri, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Di editor kebijakan, buat kebijakan izin yang memungkinkan operasi Amazon EVS. Untuk contoh kebijakan, lihat the section called “Membuat dan mengelola lingkungan Amazon EVS”. Untuk melihat semua tindakan, sumber daya, dan kunci kondisi Amazon EVS yang tersedia, lihat Tindakan di Referensi Otorisasi Layanan.
5. Pilih Berikutnya.
6. Di bawah nama Kebijakan, masukkan nama kebijakan yang berarti untuk mengidentifikasi kebijakan ini.
7. Tinjau izin yang ditentukan dalam kebijakan ini.
8. (Opsional) Tambahkan tag untuk membantu mengidentifikasi, mengatur, atau mencari sumber daya ini.
9. Pilih Buat kebijakan.
10. Di menu sebelah kiri, pilih Peran.
11. Pilih Buat peran.
12. Untuk jenis entitas Tepercaya, pilih Akun AWS.
13. Di bawah An Akun AWS , tentukan akun yang ingin Anda lakukan tindakan Amazon EVS dan pilih Berikutnya.
14. Pada halaman Tambahkan izin, pilih kebijakan izin yang sebelumnya Anda buat dan pilih Berikutnya.
15. Di bawah Nama peran, masukkan nama yang bermakna untuk mengidentifikasi peran ini.
16. Tinjau kebijakan kepercayaan dan pastikan bahwa yang Akun AWS benar terdaftar sebagai kepala sekolah.
17. (Opsional) Tambahkan tag untuk membantu mengidentifikasi, mengatur, atau mencari sumber daya ini.
18. Pilih Buat peran.

AWS CLI

1. Salin konten berikut ke file JSON kebijakan kepercayaan. Untuk ARN utama, ganti contoh Akun AWS ID dan `service-user` nama dengan ID Anda sendiri dan nama Akun AWS pengguna IAM.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/service-user"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Buat peran. Ganti `evs-environment-role-trust-policy.json` dengan nama file kebijakan kepercayaan Anda.

```
aws iam create-role \
  --role-name myAmazonEVSEnvironmentRole \
  --assume-role-policy-document file://"evs-environment-role-trust-policy.json"
```

3. Buat kebijakan izin yang memungkinkan operasi Amazon EVS dan lampirkan kebijakan ke peran. Ganti `myAmazonEVSEnvironmentRole` dengan nama peran Anda. Untuk contoh kebijakan, lihat the section called “Membuat dan mengelola lingkungan Amazon EVS”. Untuk melihat semua tindakan, sumber daya, dan kunci kondisi Amazon EVS yang tersedia, lihat Tindakan di Referensi Otorisasi Layanan.

```
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:policy/AmazonEVSEnvironmentPolicy \
  --role-name myAmazonEVSEnvironmentRole
```

Mendaftar untuk paket AWS Business, AWS Enterprise On-Ramp, atau Enterprise AWS Support

Amazon EVS mengharuskan pelanggan terdaftar dalam paket AWS Business, AWS Enterprise On-Ramp, atau Enterprise AWS Support untuk menerima akses berkelanjutan ke dukungan teknis dan panduan arsitektur. AWS Business Support adalah tingkat AWS Support minimum yang memenuhi persyaratan Amazon EVS. Jika Anda memiliki beban kerja yang penting bagi bisnis, kami sarankan untuk mendaftar di paket Enterprise On-Ramp atau AWS Enterprise Support. AWS Untuk informasi selengkapnya, lihat Bandingkan Paket AWS Dukungan.

> **Important**
>
> Pembuatan lingkungan Amazon EVS gagal jika Anda tidak mendaftar untuk paket AWS Bisnis, AWS Enterprise On-Ramp, atau Enterprise AWS Support.

Periksa kuota

Untuk mengaktifkan pembuatan lingkungan Amazon EVS, pastikan akun Anda memiliki kuota tingkat akun minimum yang diperlukan. Untuk informasi selengkapnya, lihat Kuota layanan.

> **Important**
>
> Pembuatan lingkungan Amazon EVS gagal jika jumlah host per nilai kuota lingkungan EVS tidak minimal 4.

Paket ukuran VPC CIDR

Saat membuat lingkungan Amazon EVS, Anda harus menentukan blok CIDR VPC. Blok VPC CIDR tidak dapat diubah setelah lingkungan dibuat, dan perlu memiliki cukup ruang yang disediakan untuk mengakomodasi subnet dan host EVS yang diperlukan yang dibuat Amazon EVS selama penerapan lingkungan. Akibatnya, sangat penting untuk merencanakan ukuran blok CIDR dengan hati-hati, dengan mempertimbangkan persyaratan Amazon EVS dan kebutuhan penskalaan masa depan Anda sebelum penerapan. Amazon EVS memerlukan blok VPC CIDR dengan ukuran minimum /22 netmask untuk memungkinkan ruang yang cukup untuk subnet dan host EVS yang diperlukan. Untuk informasi selengkapnya, lihat the section called “Pertimbangan jaringan Amazon EVS”.

> **Important**
>
> Pastikan Anda memiliki ruang alamat IP yang cukup untuk subnet VPC Anda dan subnet VLAN yang dibuat Amazon EVS untuk peralatan VCF. Blok VPC CIDR harus memiliki ukuran minimum /22 netmask untuk memungkinkan ruang yang cukup untuk subnet dan host EVS yang diperlukan.

> **Note**
>
> Amazon EVS tidak mendukung IPv6 saat ini.

Buat VPC dengan subnet

Amazon EVS menyebarkan lingkungan Anda ke dalam VPC yang Anda sediakan. VPC ini harus berisi subnet untuk Amazon EVS service access (). the section called “Subnet akses layanan” Untuk langkah-langkah membuat VPC dengan subnet untuk Amazon EVS, lihat. the section called “Buat VPC dengan subnet dan tabel rute”

Konfigurasikan tabel rute utama VPC

Subnet Amazon EVS VLAN secara implisit terkait dengan tabel rute utama VPC. Untuk mengaktifkan konektivitas ke layanan dependen seperti DNS atau sistem lokal agar penerapan lingkungan berhasil, Anda harus mengonfigurasi tabel rute utama untuk memungkinkan lalu lintas ke sistem ini. Untuk informasi selengkapnya, lihat the section called “Secara eksplisit mengaitkan subnet Amazon EVS VLAN ke tabel rute VPC”.

> **Important**
>
> Amazon EVS mendukung penggunaan tabel rute khusus hanya setelah lingkungan Amazon EVS dibuat. Tabel rute khusus tidak boleh digunakan selama pembuatan lingkungan Amazon EVS, karena hal ini dapat mengakibatkan masalah konektivitas.

Persyaratan rute gateway

Konfigurasikan rute untuk jenis gateway ini berdasarkan persyaratan konektivitas Anda:

- Gerbang NAT (NGW)
  - Opsional untuk akses internet outbound saja.
  - Harus berada di subnet publik dengan akses gateway internet.
  - Tambahkan rute dari subnet pribadi dan subnet EVS VLAN ke gateway NAT.
  - Untuk informasi selengkapnya, lihat Bekerja dengan gateway NAT di Panduan Pengguna Amazon VPC.
- Gerbang transit (TGW)
  - Diperlukan untuk konektivitas lokal melalui AWS Direct Connect dan AWS Site-to-Site VPN.
  - Tambahkan rute untuk rentang jaringan lokal.
  - Konfigurasikan propagasi rute jika menggunakan BGP.
  - Untuk informasi selengkapnya, lihat Gateway transit di Gateway Transit VPC Amazon di Panduan Pengguna Amazon VPC.

Praktik terbaik

- Dokumentasikan semua konfigurasi tabel rute.
- Gunakan konvensi penamaan yang konsisten.
- Audit tabel rute Anda secara teratur.
- Uji konektivitas setelah melakukan perubahan.
- Cadangkan konfigurasi tabel rute.
- Pantau kesehatan dan propagasi rute.

Untuk informasi selengkapnya tentang bekerja dengan tabel rute, lihat Mengonfigurasi tabel rute di Panduan Pengguna Amazon VPC.

Konfigurasikan set opsi DHCP VPC Anda

> **Important**
>
> Penerapan lingkungan Anda gagal jika Anda tidak memenuhi persyaratan Amazon EVS ini:
>
> - Sertakan alamat IP server DNS primer dan alamat IP server DNS sekunder dalam set opsi DHCP.

- Sertakan zona pencarian maju DNS dengan catatan A untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda.
- Sertakan zona pencarian terbalik DNS dengan catatan PTR untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda.
- Konfigurasikan tabel rute utama VPC untuk memastikan rute ke server DNS Anda ada.
- Pastikan pendaftaran nama domain Anda valid dan belum kedaluwarsa, dan tidak ada duplikat nama host atau alamat IP.
- Konfigurasikan grup keamanan dan daftar kontrol akses jaringan (ACLs) agar Amazon EVS dapat berkomunikasi dengan:
  - Server DNS melalui TCP/UDP port 53.
  - Manajemen host VLAN subnet melalui HTTPS dan SSH.
  - Manajemen VLAN subnet melalui HTTPS dan SSH.

Untuk informasi selengkapnya, lihat the section called “Mengonfigurasi server DNS dan NTP menggunakan set opsi DHCP VPC”.

Membuat dan mengkonfigurasi infrastruktur VPC Route Server

Amazon EVS menggunakan Amazon VPC Route Server untuk mengaktifkan perutean dinamis berbasis BGP ke jaringan underlay VPC Anda. Anda harus menentukan server rute yang berbagi rute ke setidaknya dua titik akhir server rute di subnet akses layanan. ASN peer yang dikonfigurasi pada peer server rute harus cocok, dan alamat IP peer harus unik.

Important

Penerapan lingkungan Anda gagal jika Anda tidak memenuhi persyaratan Amazon EVS ini untuk konfigurasi Server Rute VPC:

- Anda harus mengkonfigurasi setidaknya dua titik akhir server rute di subnet akses layanan.
- Saat mengonfigurasi Border Gateway Protocol (BGP) untuk gateway Tier-0, nilai ASN rekan VPC Route Server harus sesuai dengan nilai ASN peer NSX Edge.
- Saat membuat dua rekan server rute, Anda harus menggunakan alamat IP unik dari VLAN uplink NSX untuk setiap titik akhir. Kedua alamat IP ini akan ditetapkan ke tepi NSX selama penyebaran lingkungan Amazon EVS.

- Saat mengaktifkan propagasi Route Server, Anda harus memastikan bahwa semua tabel rute yang disebarkan memiliki setidaknya satu asosiasi subnet eksplisit. Iklan rute BGP gagal jika tabel rute yang disebarkan tidak memiliki asosiasi subnet eksplisit.

> **Note**
>
> Untuk deteksi keaktifan rekan Route Server, Amazon EVS hanya mendukung mekanisme keepalive BGP default. Amazon EVS tidak mendukung Deteksi Penerusan Dua Arah (BFD) multi-hop.

Prasyarat

Sebelum memulai, Anda memerlukan:

- Subnet VPC untuk server rute Anda.
- Izin IAM untuk mengelola sumber daya Server Rute VPC.
- Nilai BGP ASN untuk server rute (ASN sisi Amazon). Nilai ini harus berada di kisaran 1-4294967295.
- ASN peer untuk mengintip server rute Anda dengan gateway NSX Tier-0. Nilai ASN rekan yang dimasukkan di server rute dan gateway NSX Tier-0 harus cocok. ASN default untuk alat NSX Edge adalah 65000.

Langkah-langkah

Untuk langkah-langkah untuk mengatur VPC Route Server, lihat tutorial Route Server memulai.

> **Note**
>
> Jika Anda menggunakan gateway NAT atau gateway transit, pastikan server rute Anda dikonfigurasi dengan benar untuk menyebarkan rute NSX ke tabel rute VPC.

> **Note**
>
> Kami menyarankan Anda mengaktifkan rute persisten untuk instance server rute dengan durasi bertahan antara 1-5 menit. Jika diaktifkan, rute akan dipertahankan dalam database routing server rute bahkan jika semua sesi BGP berakhir.

> **Note**
>
> Status konektivitas BGP akan turun hingga lingkungan Amazon EVS digunakan dan beroperasi.

Membuat gateway transit untuk konektivitas lokal

Anda dapat mengonfigurasi konektivitas untuk pusat data lokal ke AWS infrastruktur Anda menggunakan Direct Connect gateway transit terkait, atau menggunakan lampiran AWS Site-to-Site VPN ke gateway transit. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan konektivitas jaringan lokal (opsional)”.

Buat Reservasi EC2 Kapasitas Amazon

Amazon EVS meluncurkan instans Amazon EC2 i4i.metal yang mewakili host ESX di lingkungan Amazon EVS Anda. Untuk memastikan bahwa Anda memiliki kapasitas instans i4i.metal yang cukup tersedia saat Anda membutuhkannya, kami sarankan Anda meminta Reservasi Kapasitas Amazon EC2 . Anda dapat membuat Reservasi Kapasitas kapan saja, dan Anda dapat memilih kapan dimulai. Anda dapat meminta Reservasi Kapasitas untuk penggunaan segera, atau Anda dapat meminta Reservasi Kapasitas untuk tanggal yang akan datang. Untuk informasi selengkapnya, lihat Cadangan kapasitas komputasi dengan Reservasi Kapasitas EC2 Sesuai Permintaan di Panduan Pengguna Amazon Elastic Compute Cloud.

Mengatur AWS CLI

AWS CLI Ini adalah alat baris perintah untuk bekerja dengan Layanan AWS, termasuk Amazon EVS. Ini juga digunakan untuk mengautentikasi pengguna IAM atau peran untuk akses ke lingkungan virtualisasi Amazon EVS dan AWS sumber daya lain dari mesin lokal Anda. Untuk menyediakan

AWS sumber daya dari baris perintah, Anda perlu mendapatkan ID kunci AWS akses dan kunci rahasia untuk digunakan di baris perintah. Maka Anda perlu mengkonfigurasi kredensional ini di. AWS CLI Untuk informasi selengkapnya, lihat Mengatur AWS CLI dalam Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Buat Amazon EC2 key pair

Amazon EVS menggunakan Amazon EC2 key pair yang Anda sediakan selama pembuatan lingkungan untuk terhubung ke host Anda. Untuk membuat key pair, ikuti langkah-langkah pada Create a key pair untuk Amazon EC2 instance Anda di Panduan Amazon Elastic Compute Cloud Pengguna.

Persiapkan lingkungan Anda untuk VMware Cloud Foundation (VCF)

Sebelum menerapkan lingkungan Amazon EVS, lingkungan Anda harus memenuhi persyaratan infrastruktur VMware Cloud Foundation (VCF). Untuk prasyarat VCF terperinci, lihat Buku Kerja Perencanaan dan Persiapan di dokumentasi produk Cloud Foundation. VMware

Anda juga harus membiasakan diri dengan persyaratan VCF 5.2.x. Lihat catatan rilis VCF 5.2.x untuk informasi rilis yang relevan.

> **Note**
>
> Untuk informasi tentang versi VCF yang disediakan oleh Amazon EVS, lihat. the section called “Versi dan instance VCF EC2 ”

Mendapatkan kunci lisensi VCF

Untuk menggunakan Amazon EVS, Anda perlu memberikan kunci solusi VCF dan kunci lisensi vSAN. Kunci solusi VCF harus memiliki setidaknya 256 core. Kunci lisensi vSAN harus memiliki setidaknya 110 TiB kapasitas vSAN. Untuk informasi selengkapnya tentang lisensi VCF, lihat Mengelola Kunci Lisensi di Cloud Foundation di VMware Panduan Administrasi VMware Cloud Foundation.

> **Important**
>
> Gunakan antarmuka pengguna SDDC Manager untuk mengelola solusi VCF dan kunci lisensi vSAN. Amazon EVS mengharuskan Anda mempertahankan solusi VCF yang valid dan kunci lisensi vSAN di SDDC Manager agar layanan berfungsi dengan baik.

> **Note**
>
> Lisensi VCF Anda akan tersedia untuk Amazon EVS di semua AWS Wilayah untuk kepatuhan lisensi. Amazon EVS tidak memvalidasi kunci lisensi. Untuk memvalidasi kunci lisensi, kunjungi dukungan Broadcom.

VMware Prasyarat HCX

Anda dapat menggunakan VMware HCX untuk memigrasikan beban kerja VMware berbasis yang ada ke Amazon EVS. Sebelum Anda menggunakan VMware HCX dengan Amazon EVS, pastikan bahwa tugas-tugas prerequiste berikut telah selesai.

> **Note**
>
> VMware HCX tidak diinstal di lingkungan EVS secara default.

- Sebelum Anda dapat menggunakan VMware HCX dengan Amazon EVS, persyaratan dasar jaringan minimum harus dipenuhi. Untuk informasi selengkapnya, lihat Persyaratan Minimum Underlay Jaringan di Panduan Pengguna VMware HCX.
- Konfirmasikan bahwa VMware NSX diinstal dan dikonfigurasi di lingkungan. Untuk informasi lebih lanjut, lihat Panduan Instalasi VMware NSX.
- Pastikan VMware HCX diaktifkan dan dipasang di lingkungan. Untuk informasi selengkapnya tentang mengaktifkan dan menginstal VMware HCX, lihat Tentang Memulai dengan VMware HCX di Panduan Memulai dengan HCX. VMware
- Jika Anda membutuhkan konektivitas internet HCX, Anda harus menyelesaikan tugas-tugas prasyarat berikut:
  - Pastikan kuota IPAM Anda untuk panjang netmask blok IPv4 CIDR publik bersebelahan yang disediakan Amazon adalah /28 atau lebih besar.

> **Important**
>
> Untuk konektivitas internet HCX, Amazon EVS memerlukan penggunaan blok IPv4 CIDR dari kolam IPAM publik dengan panjang netmask /28 atau lebih besar. Penggunaan blok CIDR apa pun dengan panjang netmask lebih kecil dari /28 akan mengakibatkan masalah konektivitas HCX. Untuk informasi lebih lanjut tentang meningkatkan kuota IPAM, lihat Kuota untuk IPAM Anda.

- Buat IPAM dan kolam IPv4 IPAM publik dengan CIDR yang memiliki panjang netmask minimal /28.
- Alokasikan setidaknya dua alamat IP Elastis (EIPs) dari kolam IPAM untuk peralatan HCX Manager dan HCX Interconnect (HCX-IX). Alokasikan alamat IP Elastis tambahan untuk setiap perangkat jaringan HCX yang perlu Anda gunakan.
- Tambahkan blok IPv4 CIDR publik sebagai CIDR tambahan ke VPC Anda.

Untuk informasi selengkapnya tentang pengaturan HCX, lihat the section called “Pilih opsi konektivitas HCX Anda” dan. the section called “Opsi konektivitas HCX”

Daftar periksa prasyarat penerapan Amazon EVS

Bagian ini berisi daftar prasyarat yang harus diselesaikan untuk mengaktifkan penerapan lingkungan Amazon EVS yang berhasil.

Informasi kunci lisensi VCF

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
ID Situs	ID situs disediakan oleh Broadcom untuk akses ke portal dukungan Broadcom.	Harus memberikan ID Situs dari Broadcom dalam permintaan pembuatan lingkungan EVS.	01234567
Kunci solusi VCF	Kunci lisensi VCF tunggal yang membuka fitur dari seluruh tumpukan	Harus menyediakan kunci solusi VCF aktif yang valid dalam permintaan	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
	VCF, termasuk vSphere, NSX, SDDC Manager, dan vCenter Server.	pembuatan lingkungan EVS. Kunci tidak dapat digunakan oleh lingkungan EVS yang ada.	
Kunci lisensi vSAN	Kunci lisensi vSAN memungkinkan Anda untuk mengaktifkan dan menggunakan perangkat lunak vSAN dalam lingkungan VCF.	Harus memberikan kunci lisensi vSAN aktif yang valid dalam permintaan pembuatan lingkungan EVS. Kunci tidak dapat digunakan oleh lingkungan EVS yang ada.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

AWS akun dan informasi Wilayah

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
AWS nomor ID akun	AWS Akun ini memungkinkan Anda untuk membuat dan mengelola AWS sumber daya dan mengakses AWS layanan.	Harus memiliki akses ke AWS akun.	999999999999
AWS Wilayah	Area geografis fisik di mana AWS memelihara beberapa pusat data terisolasi yang disebut Availability Zones.	Harus menentukan AWS Wilayah untuk Amazon EVS untuk diterapkan. Untuk daftar Wilayah di mana Amazon EVS saat ini tersedia,	AS Barat (Oregon)

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
		lihat titik akhir dan kuota Amazon Elastic VMware Service di Panduan Referensi AWS Umum.	

AWS Transit Gateway untuk konektivitas pusat data lokal

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
ID gerbang transit	Gateway transit bertindak sebagai router virtual Regional untuk lalu lintas yang mengalir antara VPC Anda dan jaringan lokal.	Harus menggunakan gateway transit untuk menghubungkan lingkungan Amazon EVS ke jaringan lokal Anda.	TGW-0262A 0E521Contoh
Metode konektivitas	Untuk menghubun gkan jaringan lokal Anda ke lingkungan Amazon EVS, Anda harus menggunak an gateway transit dengan Direct AWS Connect atau AWS Site-to-Site VPN.	Tentukan apakah Anda akan menggunakan AWS Direct Connect, AWS Site-to-Site VPN, atau kombinasi keduanya. Untuk informasi selengkapnya tentang penggunaan Site-to-S ite VPN dengan Direct Connect, lihat Private IP AWS Site-to-Site VPN with AWS Direct Connect.	AWS Site-to-Site VPN dengan AWS Direct Connect

VPC untuk lingkungan Amazon EVS

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
VPC ID	VPC adalah jaringan virtual yang sangat mirip dengan jaringan tradisional yang akan Anda operasikan di pusat data Anda sendiri.	VPC Amazon apa pun dapat digunakan untuk penyebaran lingkungan.	vpc-0abcdef1234567890
Blok VPC CIDR	Di Amazon VPC, blok CIDR menentukan rentang alamat IP yang tersedia dalam VPC Anda.	Blok CIDR RFC 1918 dengan ukuran minimum/22 netmask. Blok CIDR VPC harus berukuran tepat untuk mengakomodasi semua subnet dan host EVS yang akan digunakan di VPC Anda. Blok CIDR ini harus unik di seluruh lingkungan Anda.	10.1.0.0/20

Subnet VPC untuk lingkungan EVS

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
akses layanan subnet ID	Subnet akses layanan adalah subnet VPC standar yang memungkinkan akses layanan Amazon EVS. Untuk informasi selengkapnya, lihat the section	Subnet VPC apa pun dapat digunakan, asalkan subnet berukuran sesuai dalam VPC. Kami menyarankan untuk menentukan blok	subnet-abcdef1234567890e

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
	called “Subnet akses layanan”.	CIDR subnet VPC dengan netmask /24.	
akses layanan subnet CIDR	blok CIDR subnet VPC adalah rentang alamat IP, didefinis ikan menggunak an notasi CIDR, yang dialokasikan ke subnet tertentu dalam VPC.	Subnet akses layanan harus berukuran tepat untuk juga mengakomodasi subnet dan host EVS lainnya yang akan digunakan di VPC Anda. Kami menyarankan untuk menentukan blok CIDR subnet VPC dengan netmask /24.	10.1.0.0/24
AWS ID Zona Ketersediaan di dalam Wilayah	Lokasi yang berbeda dalam suatu AWS Wilayah, dirancang untuk diisolasi dari kegagalan di wilayah lain AZs, dan terdiri dari satu atau lebih pusat data.	Anda dapat menentukan Availability Zone yang digunakan subnet VPC selama pembuatan subnet. Untuk informasi selengkapnya, lihat Membuat subnet di Panduan Pengguna Amazon VPC.	kami-barat-2a

Subnet EVS VLAN untuk lingkungan EVS

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
Manajemen host VLAN CIDR	Blok CIDR untuk subnet VLAN manajemen host.	Harus memiliki ukuran minimum /28 netmask dan ukuran	10.1.1.0/24

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
	Untuk informasi selengkapnya, lihat the section called “Manajemen host VLAN subnet”.	maksimum /24 netmask. Tidak boleh tumpang tindih dengan blok CIDR yang ada yang terkait dengan VPC.	
VMotion VLAN CIDR	Blok CIDR untuk subnet VMotion VLAN. Untuk informasi selengkapnya, lihat the section called “VMotion VLAN subnet”.	Harus berukuran sama dengan VLAN manajemen host.	10.1.2.0/24
VSAN VLAN CIDR	Blok CIDR untuk subnet VSAN VLAN. Untuk informasi selengkapnya, lihat the section called “VSan VLAN subnet”.	Harus berukuran sama dengan VLAN manajemen host.	10.1.3.0/24
VTEP VLAN CIDR	Blok CIDR untuk subnet VTEP VLAN. Untuk informasi selengkapnya, lihat the section called “Subnet VTEP VLAN”.	Harus berukuran sama dengan VLAN manajemen host.	10.1.4.0/24

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
Tepi VTEP VLAN CIDR	Blok CIDR untuk subnet VTEP VLAN tepi. Untuk informasi selengkapnya, lihat the section called “Tepi VTEP VLAN subnet”.	Harus memiliki ukuran minimum /28 netmask dan ukuran maksimum /24 netmask. Tidak boleh tumpang tindih dengan blok CIDR yang ada yang terkait dengan VPC.	10.1.5.0/24
Manajemen VM VLAN CIDR	Blok CIDR untuk subnet VM VLAN Manajemen. Untuk informasi selengkapnya, lihat the section called “Manajemen VM VLAN subnet”.	Harus memiliki ukuran minimum /28 netmask dan ukuran maksimum /24 netmask. Tidak boleh tumpang tindih dengan blok CIDR yang ada yang terkait dengan VPC.	10.1.6.0/24
HCX uplink VLAN CIDR	Blok CIDR untuk subnet VLAN uplink HCX. Untuk informasi selengkapnya, lihat the section called “Subnet VLAN uplink HCX”.	Harus memiliki ukuran minimum /28 netmask dan ukuran maksimum /24 netmask. Tidak boleh tumpang tindih dengan blok CIDR yang ada yang terkait dengan VPC.	10.1.7.0/24

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
NSX uplink VLAN CIDR	Blok CIDR untuk subnet VLAN uplink NSX. Untuk informasi selengkapnya, lihat the section called “Subnet VLAN uplink NSX”.	Harus memiliki ukuran minimum /28 netmask dan ukuran maksimum /24 netmask. Tidak boleh tumpang tindih dengan blok CIDR yang ada yang terkait dengan VPC.	10.1.8.0/24
Ekspansi VLAN 1 CIDR	Blok CIDR untuk subnet VLAN ekspansi. Untuk informasi selengkapnya, lihat the section called “Ekspansi VLAN subnet”.	Harus memiliki ukuran minimum /28 netmask dan ukuran maksimum /24 netmask. Tidak boleh tumpang tindih dengan blok CIDR yang ada yang terkait dengan VPC.	10.1.9.0/24
Ekspansi VLAN 2 CIDR	Blok CIDR untuk subnet VLAN ekspansi. Untuk informasi selengkapnya, lihat the section called “Ekspansi VLAN subnet”.	Harus memiliki ukuran minimum /28 netmask dan ukuran maksimum /24 netmask. Tidak boleh tumpang tindih dengan blok CIDR yang ada yang terkait dengan VPC.	10.1.10.0/24

Infrastruktur DNS dan NTP

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
Alamat IP server DNS utama	Server sistem nama domain utama (DNS) digunakan sebagai sumber kebenaran untuk semua catatan DNS domain.	Anda dapat menggunakan IPv4 alamat yang valid dan tidak terpakai dalam rentang host yang dapat digunakan.	10.1.1.10
Alamat IP server DNS sekunder	Server DNS cadangan untuk catatan DNS domain.	Anda dapat menggunakan IPv4 alamat yang valid dan tidak terpakai dalam rentang host yang dapat digunakan.	10.1.5.25
Alamat IP server NTP	Server Network Time Protocol (NTP) adalah perangkat atau aplikasi yang menyinkronkan jam dalam jaringan menggunakan standar NTP.	Anda dapat menggunakan Layanan Sinkronisasi Waktu Amazon default dengan alamat `169.254.169.123` IP lokal, atau alamat IP server NTP lainnya.	169.254.169.123 (Layanan Sinkronisasi Waktu Amazon)
FQDN untuk penyebaran VCF	Nama domain yang sepenuhnya memenuhi syarat (FQDN) adalah nama absolut perangkat di jaringan. FQDN terdiri dari nama host dan nama domain.	FQDN hanya dapat berisi karakter alfanumerik, tanda minus (-), dan periode yang digunakan sebagai pembatas antar label. Harus merupakan FQDN unik yang valid dan belum kedaluwarsa.	evs.lokal

Set opsi VPC DHCP

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
ID set opsi DHCP	Set opsi DHCP adalah sekelompok pengaturan jaringan yang digunakan oleh sumber daya di VPC Anda, EC2 seperti instance, untuk berkomunikasi melalui jaringan virtual Anda.	Harus berisi minimal 2 server DNS. Anda dapat menggunakan Route 53 atau server DNS khusus. Juga harus berisi nama domain DNS Anda dan server NTP.	dopt-0a1b2c3d

EC2 key pair

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
EC2 nama key pair	EC2 Key pair adalah sekumpulan kredenal keamanan yang digunakan untuk terhubung dengan aman ke instans Amazon. EC2	Nama pasangan kunci harus unik.	`my-ec2-key-pair`

Tabel rute VPC

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
ID tabel rute utama	Di Amazon VPC, tabel rute utama adalah tabel rute default yang dibuat secara otomatis dengan VPC, dan	Harus dikonfigurasi untuk mengaktif kan konektivitas ke layanan dependen seperti DNS atau sistem lokal agar	rtb-0123456789abcd ef0

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
	mengatur lalu lintas untuk subnet VPC apa pun yang tidak secara eksplisit terkait dengan tabel rute yang berbeda. Subnet EVS VLAN secara implisit terkait dengan tabel rute utama VPC Anda saat Amazon EVS membuatnya.	penerapan lingkungan berhasil.	

Daftar kontrol akses jaringan (ACL)

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
ID ACL Jaringan	Network Access Control List (ACL) memungkinkan atau menolak lalu lintas masuk atau keluar di tingkat subnet.	Harus mengizinkan Amazon EVS berkomunikasi dengan: • Server DNS melalui TCP/UDP port 53. • Manajemen host VLAN subnet melalui HTTPS dan SSH. • Manajemen VM VLAN subnet melalui HTTPS dan SSH.	acl-0f62c640e793a38a3

Catatan DNS untuk komponen VCF

Komponen	Deskripsi	Persyaratan minimum	Contoh alamat IP	Contoh nama host
Tuan rumah ESX 1	Alamat IP dan nama host didefinisikan dalam catatan A dan catatan PTR untuk host ESX 1.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap host ESX di setiap penyebaran EVS.	10.1.0.10	esxi01
Tuan rumah ESX 2	Alamat IP dan nama host didefinisikan dalam catatan A dan catatan PTR untuk host ESX 2.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap host ESX di setiap penyebaran EVS.	10.1.0.11	esxi02
Tuan rumah ESX 3	Alamat IP dan nama host didefinisikan	Amazon EVS memerlukan zona pencarian	10.1.0.12	esxi03

Komponen	Deskripsi	Persyaratan minimum	Contoh alamat IP	Contoh nama host
	dalam catatan A dan catatan PTR untuk host ESX 3.	maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap host ESX di setiap penyebaran EVS.		
Tuan rumah ESX 4	Alamat IP dan nama host didefinisikan dalam catatan A dan catatan PTR untuk host ESX 4.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap host ESX di setiap penyebaran EVS.	10.1.0.13	esxi04

Komponen	Deskripsi	Persyaratan minimum	Contoh alamat IP	Contoh nama host
alat vCenter Server	Alamat IP dan nama host didefinisikan dalam catatan A dan catatan PTR untuk alat vCenter Server.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.10	vc01
Kluster Manajer NSX	Alamat IP dan nama host didefinisikan dalam catatan A dan catatan PTR untuk cluster NSX Manager.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.11	nsx

Komponen	Deskripsi	Persyaratan minimum	Contoh alamat IP	Contoh nama host
Alat Manajer SDDC	Alamat IP dan nama host yang ditentukan dalam catatan A dan catatan PTR untuk alat SDDC Manager.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.12	sddcm01
Alat Cloud Builder	Alamat IP dan nama host yang ditentukan dalam catatan A dan catatan PTR untuk alat Cloud Builder.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.13	cb01

Komponen	Deskripsi	Persyaratan minimum	Contoh alamat IP	Contoh nama host
Alat NSX Edge 1	Alamat IP dan nama host yang ditentukan dalam catatan A dan catatan PTR untuk alat NSX Edge 1.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.14	edge01
Alat NSX Edge 2	Alamat IP dan nama host yang ditentukan dalam catatan A dan catatan PTR untuk alat NSX Edge 2.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.15	edge02

Komponen	Deskripsi	Persyaratan minimum	Contoh alamat IP	Contoh nama host
Alat NSX Manager 1	Alamat IP dan nama host yang ditentukan dalam catatan A dan catatan PTR untuk alat NSX Manager 1.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.16	nsx01
Alat NSX Manager 2	Alamat IP dan nama host yang ditentukan dalam catatan A dan catatan PTR untuk alat NSX Manager 2.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.17	nsx02

Komponen	Deskripsi	Persyaratan minimum	Contoh alamat IP	Contoh nama host
Alat NSX Manager 3	Alamat IP dan nama host yang ditentukan dalam catatan A dan catatan PTR untuk alat NSX Manager 3.	Amazon EVS memerlukan zona pencarian maju DNS dengan catatan A dan zona pencarian terbalik dengan catatan PTR yang dibuat untuk setiap alat manajemen VCF di setiap penerapan EVS.	10.1.5.18	nsx03

Infrastruktur Server Rute VPC

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
ID server rute	Amazon EVS menggunakan Amazon VPC Route Server untuk mengaktifkan perutean dinamis berbasis BGP ke jaringan underlay VPC Anda.	Anda harus menentukan server rute yang berbagi rute ke setidaknya dua titik akhir server rute di subnet akses layanan. ASN peer yang dikonfigurasi pada server rute dan rekan NSX Edge harus cocok, dan alamat IP peer harus unik.	rs-0a1b2c3d4e5f67890

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
asosiasi server rute	Koneksi antara server rute dan VPC.	Server rute Anda harus terkait dengan VPC Anda.	{ "RouteServerAssociation": { "RouteServerId": "rs-0a1b2c3d4e5f67890", "VpcId": "vpc-1", "State": "associating" } }
BGP ASN dari sisi Server Rute VPC (ASN sisi Amazon)	ASN sisi Amazon mewakili AWS sisi sesi BGP antara server rute VPC dan rekan NSX Edge. Anda menentukan BGP ASN ini saat membuat server rute. Untuk informasi selengkapnya, lihat Membuat server rute di Panduan Pengguna Amazon VPC.	Nilai ini harus unik, dan dalam kisaran 1-4294967295. AWS merekomendasikan penggunaan ASN pribadi dalam kisaran 64512-65534 (ASN 16-bit) atau 4200000000—4294967294 (ASN 32-bit).	65001

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
titik akhir server rute 1 ID	Titik akhir server rute adalah komponen yang AWS dikelola di dalam subnet yang memfasilitasi koneksi BGP (Border Gateway Protocol) antara server rute Anda dan rekan BGP Anda.	Harus menyebarkan titik akhir server rute ke subnet akses layanan.	rse-0123456789abcdef0
rute server peer 1 ID	Peer server rute adalah sesi peering BGP antara titik akhir server rute dan perangkat yang digunakan di (NSX Edge). AWS	Nilai ASN peer yang ditentukan dalam peer server rute harus sesuai dengan nilai ASN peer yang digunakan untuk gateway NSX Edge Tier-0.	rsp-0123456789abcdef0
rute server peer 1 alamat IP (EVS NSX Edge 1 sisi)	Alamat IP dari server rute peer (`PeerAddress`).	Harus menggunakan alamat IP unik yang tidak digunakan dari VLAN uplink NSX. Amazon EVS akan menerapkan alamat IP ini ke NSX Edge 1 sebagai bagian dari penerapan dan peer dengan rekan titik akhir server rute.	10.1.7.10
rute server peer 1 alamat ENI titik akhir	Alamat IP ENI titik akhir dari server rute peer ()`EndpointEniAddress` .	Secara otomatis dihasilkan oleh server rute pada pembuatan rekan.	10.1.7.11

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
titik akhir server rute 2 ID	Titik akhir server rute adalah komponen yang AWS dikelola di dalam subnet yang memfasilitasi koneksi BGP (Border Gateway Protocol) antara server rute Anda dan rekan BGP Anda.	Harus menyebarkan titik akhir server rute ke subnet akses layanan.	rse-fedcba9876543210f
rute server peer 2 ID (EVS NSX Edge 2 sisi)	Peer server rute adalah sesi peering BGP antara titik akhir server rute dan perangkat yang digunakan di (NSX Edge). AWS	Nilai ASN peer yang ditentukan dalam peer server rute harus sesuai dengan nilai ASN peer yang digunakan untuk gateway NSX Edge Tier-0.	rsp-fedcba9876543210f
rute server peer 2 alamat IP	Alamat IP dari server rute peer (`PeerAddress`).	Harus menggunakan alamat IP unik dari VLAN uplink NSX. Amazon EVS akan menerapkan alamat IP ini ke NSX Edge 2 sebagai bagian dari penyebaran dan peer dengan rekan titik akhir server rute.	10.1.7.200
rute server peer 2 alamat ENI titik akhir	Alamat IP ENI titik akhir dari server rute peer ()`EndpointEniAddress` .	Secara otomatis dihasilkan oleh server rute pada pembuatan rekan.	10.1.7.201

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh

propagasi server rute	Propagasi server rute menginstal rute di FIB pada tabel rute yang telah Anda tentukan.	Harus menentukan tabel rute yang terkait dengan subnet akses layanan Anda. Amazon EVS hanya mendukung IPv4 jaringan saat ini.	<pre>{
			"RouteServerEndpoint": {
			"RouteServerId": "rs-1",
			"RouteServerEndpointId": "rse-1",
			"VpcId": "vpc-1",
			"SubnetId": "subnet-1",
			"State": "pending"
			}
			}</pre>

BGP ASN dari sisi rekan NSX	BGP ASN untuk sisi koneksi NSX.	Sarankan menggunakan ASN 65000 default NSX	65000

Sumber daya akses internet HCX (Opsional)

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
IPAM ID	Amazon VPC IP Address Manager (IPAM) digunakan untuk mengelola alamat IP untuk akses internet HCX.	Harus dikonfigurasi untuk memberikan IPv4 alamat publik. Diperlukan hanya untuk konfigurasi akses internet HCX.	ipam-0123456789abcdef0
ID kolam IPAM	Kolam IPv4 IPAM publik milik Amazon yang menyediakan alamat untuk komponen HCX.	Harus dikonfigurasi sebagai kolam IPv4 renang umum. Diperlukan hanya	ipam-kolam-0123456789abcdef0

Komponen	Deskripsi	Persyaratan minimum	Nilai contoh
		untuk konfigurasi akses internet HCX.	
Blok CIDR VLAN publik HCX	Blok IPv4 CIDR publik sekunder yang dialokasikan dari kolam IPAM untuk subnet VLAN publik HCX.	Harus memiliki netmask /28 dan dialokasikan dari kolam renang umum IPAM milik Amazon. Diperlukan hanya untuk konfigurasi akses internet HCX.	18.97.137.0/28
Alamat IP elastis	Alamat IP Elastis Berurutan dialokasikan dari kolam IPAM untuk komponen HCX.	Minimal 3 EIPs dari kolam IPAM yang sama untuk HCX Manager, HCX Interconnect Appliance (HCX-IX), dan HCX Network Extension (HCX-NE). Diperlukan hanya untuk konfigurasi akses internet HCX.	eipalloc-0123456789abcdef0, eipalloc-0123456789abcdef1, eipalloc-0123456789abcdef2

Memulai dengan Amazon Elastic VMware Service

Gunakan panduan ini untuk memulai Amazon Elastic VMware Service (Amazon EVS). Anda akan mempelajari cara membuat lingkungan Amazon EVS dengan host dalam Amazon Virtual Private Cloud (VPC) Anda sendiri.

Setelah selesai, Anda akan memiliki lingkungan Amazon EVS yang dapat Anda gunakan untuk memigrasikan beban kerja VMware berbasis vSphere Anda ke file. AWS Cloud

Important

Untuk memulai sesederhana dan secepat mungkin, topik ini mencakup langkah-langkah untuk membuat VPC, dan menentukan persyaratan minimum untuk konfigurasi server DNS dan pembuatan lingkungan Amazon EVS. Sebelum membuat sumber daya ini, kami sarankan Anda merencanakan ruang alamat IP dan pengaturan catatan DNS yang memenuhi kebutuhan Anda. Anda juga harus membiasakan diri dengan persyaratan VCF 5.2.x. Lihat catatan rilis VCF 5.2.x untuk informasi rilis yang relevan.

Important

Untuk informasi tentang versi VCF yang disediakan oleh Amazon EVS, lihat. the section called “Versi dan instance VCF EC2 ”

Topik

Prasyarat

Sebelum memulai, Anda harus menyelesaikan tugas prasyarat Amazon EVS. Untuk informasi selengkapnya, lihat Menyiapkan VMware Layanan Elastis Amazon.

Buat VPC dengan subnet dan tabel rute

> **Note**
>
> Lingkungan VPC, subnet, dan Amazon EVS semuanya harus dibuat di akun yang sama. Amazon EVS tidak mendukung berbagi lintas akun subnet VPC atau lingkungan Amazon EVS.

Example

Amazon VPC console

1. Buka konsol Amazon VPC.
2. Di dasbor VPC, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Biarkan pembuatan otomatis tag Nama dipilih untuk membuat tag Nama untuk sumber daya VPC, atau hapus untuk menyediakan tag Nama Anda sendiri untuk sumber daya VPC.
5. Untuk blok IPv4 CIDR, masukkan blok IPv4 CIDR. VPC harus memiliki blok IPv4 CIDR. Pastikan Anda membuat VPC yang berukuran cukup untuk mengakomodasi subnet Amazon EVS. Untuk informasi selengkapnya, lihat the section called “Pertimbangan jaringan Amazon EVS”.

> **Note**
>
> Amazon EVS tidak mendukung IPv6 saat ini.

6. Pertahankan Penyewaan sebagai`Default`. Dengan opsi ini dipilih, EC2 instance yang diluncurkan ke VPC ini akan menggunakan atribut penyewaan yang ditentukan saat instance diluncurkan. Amazon EVS meluncurkan EC2 instans bare metal atas nama Anda.
7. Untuk Jumlah Availability Zones (AZs), pilih 1.

> **Note**
>
> Amazon EVS hanya mendukung penerapan Single-AZ saat ini.

8. Perluas Kustomisasi AZs dan pilih AZ untuk subnet Anda.

> **Note**
>
> Anda harus menerapkan di AWS Wilayah tempat Amazon EVS didukung. Untuk informasi selengkapnya tentang ketersediaan Amazon EVS Region, lihat titik akhir dan kuota Amazon Elastic VMware Service di Panduan Referensi AWS Umum.

9. (Opsional) Jika Anda membutuhkan konektivitas internet, untuk Jumlah subnet publik, pilih 1.
10. Untuk Jumlah subnet pribadi, pilih 1. Subnet pribadi ini akan digunakan sebagai subnet akses layanan yang Anda berikan ke Amazon EVS selama langkah pembuatan lingkungan. Untuk informasi selengkapnya, lihat the section called “Subnet akses layanan”.
11. Untuk memilih rentang alamat IP untuk subnet Anda, perluas Sesuaikan subnet blok CIDR.

> **Note**
>
> Subnet Amazon EVS VLAN juga perlu dibuat dari ruang CIDR VPC ini. Pastikan Anda menyisakan cukup ruang di blok CIDR VPC untuk subnet VLAN yang dibutuhkan layanan. Untuk informasi selengkapnya, lihat the section called “Pertimbangan jaringan Amazon EVS”

12. (Opsional) Untuk memberikan akses internet IPv4 ke sumber daya, untuk gateway NAT, pilih Dalam 1 AZ. Perhatikan bahwa ada biaya yang terkait dengan gateway NAT. Untuk informasi selengkapnya, lihat Harga untuk gateway NAT.

> **Note**
>
> Amazon EVS memerlukan penggunaan gateway NAT untuk mengaktifkan konektivitas internet keluar.

13. Untuk titik akhir VPC, pilih Tidak Ada.

> **Note**
>
> Amazon EVS tidak mendukung titik akhir VPC gateway Amazon S3 untuk saat ini. Untuk mengaktifkan Amazon S3 konektivitas, Anda harus mengatur antarmuka VPC endpoint menggunakan for. AWS PrivateLink Amazon S3Untuk informasi selengkapnya, lihat AWS PrivateLinkAmazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

14. Untuk opsi DNS, tetap pilih default. Amazon EVS mengharuskan VPC Anda memiliki kemampuan resolusi DNS untuk semua komponen VCF.
15. (Opsional) Untuk menambahkan tag ke VPC Anda, perluas Tag tambahan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
16. Pilih Buat VPC.

> **Note**
>
> Selama pembuatan VPC, Amazon VPC secara otomatis membuat tabel rute utama dan secara implisit mengaitkan subnet ke dalamnya secara default.

AWS CLI

1. Buka sesi terminal.
2. Buat VPC dengan subnet pribadi dan subnet publik opsional dalam satu Availability Zone.

```
aws ec2 create-vpc \
  --cidr-block 10.0.0.0/16 \
  --instance-tenancy default \
  --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=evs-vpc}]'
---
```

```
. Store the VPC ID for use in subsequent commands.
+
[source,bash]
```

VPC_ID=$ (aws ec2 describe-vpcs\ --filters name=tag:name, values=evs-vpc\ --query 'Vpcs [0]. VpcId'\ --output teks) ---

3. Aktifkan nama host DNS dan dukungan DNS.

```
aws ec2 modify-vpc-attribute \
  --vpc-id $VPC_ID \
  --enable-dns-hostnames
aws ec2 modify-vpc-attribute \
  --vpc-id $VPC_ID \
  --enable-dns-support
```

4. Buat subnet pribadi di VPC.

```
aws ec2 create-subnet \
  --vpc-id $VPC_ID \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-west-2a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=evs-private-
subnet}]'
```

5. Simpan ID subnet pribadi untuk digunakan dalam perintah berikutnya.

```
PRIVATE_SUBNET_ID=$(aws ec2 describe-subnets \
  --filters Name=tag:Name,Values=evs-private-subnet \
  --query 'Subnets[0].SubnetId' \
  --output text)
```

6. (Opsional) Buat subnet publik jika konektivitas internet diperlukan.

```
aws ec2 create-subnet \
  --vpc-id $VPC_ID \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-west-2a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=evs-public-
subnet}]'
```

7. (Opsional) Simpan ID subnet publik untuk digunakan dalam perintah berikutnya.

```
PUBLIC_SUBNET_ID=$(aws ec2 describe-subnets \
  --filters Name=tag:Name,Values=evs-public-subnet \
  --query 'Subnets[0].SubnetId' \
  --output text)
```

8. (Opsional) Buat dan lampirkan gateway internet jika subnet publik dibuat.

```
aws ec2 create-internet-gateway \
  --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=evs-
igw}]'

IGW_ID=$(aws ec2 describe-internet-gateways \
  --filters Name=tag:Name,Values=evs-igw \
  --query 'InternetGateways[0].InternetGatewayId' \
  --output text)

aws ec2 attach-internet-gateway \
  --vpc-id $VPC_ID \
  --internet-gateway-id $IGW_ID
```

9. (Opsional) Buat gateway NAT jika konektivitas internet diperlukan.

```
aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-nat-
eip}]'

EIP_ID=$(aws ec2 describe-addresses \
  --filters Name=tag:Name,Values=evs-nat-eip \
  --query 'Addresses[0].AllocationId' \
  --output text)

aws ec2 create-nat-gateway \
  --subnet-id $PUBLIC_SUBNET_ID \
  --allocation-id $EIP_ID \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=evs-nat}]'
```

10. Buat dan konfigurasikan tabel rute yang diperlukan.

```
aws ec2 create-route-table \
  --vpc-id $VPC_ID \
```

```
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=evs-
private-rt}]'

PRIVATE_RT_ID=$(aws ec2 describe-route-tables \
  --filters Name=tag:Name,Values=evs-private-rt \
  --query 'RouteTables[0].RouteTableId' \
  --output text)

aws ec2 create-route-table \
  --vpc-id $VPC_ID \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=evs-public-
rt}]'

PUBLIC_RT_ID=$(aws ec2 describe-route-tables \
  --filters Name=tag:Name,Values=evs-public-rt \
  --query 'RouteTables[0].RouteTableId' \
  --output text)
```

11. Tambahkan rute yang diperlukan ke tabel rute.

```
aws ec2 create-route \
  --route-table-id $PUBLIC_RT_ID \
  --destination-cidr-block 0.0.0.0/0 \
  --gateway-id $IGW_ID

aws ec2 create-route \
  --route-table-id $PRIVATE_RT_ID \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id $NAT_GW_ID
```

12. Kaitkan tabel rute dengan subnet Anda.

```
aws ec2 associate-route-table \
  --route-table-id $PRIVATE_RT_ID \
  --subnet-id $PRIVATE_SUBNET_ID

aws ec2 associate-route-table \
  --route-table-id $PUBLIC_RT_ID \
  --subnet-id $PUBLIC_SUBNET_ID
```

> **Note**
>
> Selama pembuatan VPC, Amazon VPC secara otomatis membuat tabel rute utama dan secara implisit mengaitkan subnet ke dalamnya secara default.

Pilih opsi konektivitas HCX Anda

Pilih satu opsi konektivitas untuk lingkungan Amazon EVS Anda:

- Konektivitas pribadi: Menyediakan jalur jaringan berkinerja tinggi untuk HCX, mengoptimalkan keandalan dan konsistensi. Memerlukan penggunaan AWS Direct Connect atau Site-to-Site VPN untuk konektivitas jaringan eksternal.
- Konektivitas internet: Menggunakan internet publik untuk membuat jalur migrasi fleksibel yang cepat diatur. Memerlukan penggunaan VPC IP Address Manager (IPAM) dan alamat IP Elastis.

Untuk analisis terperinci, lihatthe section called “Opsi konektivitas HCX”.

Pilih opsi Anda:

- Opsi A: Hanya konektivitas pribadi → Lanjutkan kethe section called “Konfigurasikan tabel rute utama VPC”.
- Opsi B: Konektivitas internet → Lanjutkan kethe section called “Pengaturan konektivitas internet HCX”.

Pengaturan konektivitas internet HCX

> **Note**
>
> Lewati bagian ini jika Anda memilih konektivitas pribadi HCX dan lanjutkan ke. the section called “Konfigurasikan tabel rute utama VPC”

Untuk mengaktifkan konektivitas internet HCX untuk Amazon EVS, Anda harus:

- Pastikan kuota VPC IP Address Manager (IPAM) untuk blok CIDR publik IPv4 bersebelahan yang disediakan Amazon adalah /28 atau lebih besar.

> **Important**
>
> Penggunaan blok IPv4 CIDR publik bersebelahan yang disediakan Amazon dengan panjang netmask lebih kecil dari /28 akan mengakibatkan masalah konektivitas HCX. Untuk informasi lebih lanjut tentang meningkatkan kuota IPAM, lihat Kuota untuk IPAM Anda.

- Buat IPAM dan kolam IPv4 IPAM publik dengan CIDR yang memiliki panjang netmask minimal /28.
- Alokasikan setidaknya dua alamat IP Elastis (EIPs) dari kolam IPAM untuk peralatan HCX Manager dan HCX Interconnect (HCX-IX). Alokasikan alamat IP Elastis tambahan untuk setiap perangkat jaringan HCX yang perlu Anda gunakan.
- Tambahkan blok IPv4 CIDR publik sebagai CIDR tambahan ke VPC Anda.

Untuk informasi selengkapnya tentang mengelola konektivitas internet HCX setelah pembuatan lingkungan, lihat. the section called “Konektivitas publik HCX”

Buat IPAM

Ikuti langkah-langkah ini untuk membuat IPAM.

> **Note**
>
> Anda dapat menggunakan IPAM Tingkat Gratis untuk membuat sumber daya IPAM untuk digunakan dengan Amazon EVS. Meskipun IPAM sendiri gratis dengan Tingkat Gratis, Anda bertanggung jawab atas biaya AWS layanan lain yang digunakan bersama dengan IPAM seperti gateway NAT dan IPv4 alamat publik apa pun yang Anda gunakan yang berada di luar batas tingkat gratis. Untuk informasi selengkapnya tentang harga IPAM, lihat halaman Amazon VPC harga.

> **Note**
>
> Amazon EVS tidak mendukung IPv6 Global Unicast Address (GUA) pribadi CIDRs saat ini.

Buat kolam IPv4 IPAM publik

Ikuti langkah-langkah ini untuk membuat kolam IPv4 renang umum.

IPAM console

1. Buka konsol IPAM.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup publik. Untuk informasi selengkapnya tentang cakupan, lihat Cara kerja IPAM.
4. Pilih Buat kolam.
5. (Opsional) Tambahkan tag Nama untuk kolam dan Deskripsi untuk kolam.
6. Di bawah Alamat keluarga, pilih IPv4.
7. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih.
8. Di bawah Locale, pilih lokasi untuk kolam renang. Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Lokal yang Anda pilih harus cocok dengan AWS Wilayah tempat VPC Anda digunakan.
9. Di bawah Layanan, pilih EC2 (EIP/VPC). Ini akan mengiklankan yang CIDRs dialokasikan dari kumpulan ini untuk EC2 layanan Amazon (untuk alamat IP Elastis).
10. Di bawah Sumber IP Publik, pilih milik Amazon.
11. Di bawah CIDRs ketentuan, pilih Tambahkan CIDR publik milik Amazon.
12. Di bawah Netmask, pilih panjang netmask CIDR. /28 adalah panjang netmask minimum yang diperlukan.
13. Pilih Buat kolam.

AWS CLI

1. Buka sesi terminal.
2. Dapatkan ID lingkup publik dari IPAM Anda.

```
SCOPE_ID=$(aws ec2 describe-ipam-scopes \
  --filters Name=ipam-scope-type,Values=public \
  --query 'IpamScopes[0].IpamScopeId' \
  --output text)
```

3. Buat kolam IPAM di ruang lingkup publik.

```
aws ec2 create-ipam-pool \
  --ipam-scope-id $SCOPE_ID \
  --address-family ipv4 \
```

```
  --no-auto-import \
  --locale us-east-2 \
  --description "Public IPv4 pool for HCX" \
  --tag-specifications 'ResourceType=ipam-pool,Tags=[{Key=Name,Value=evs-hcx-
public-pool}]' \
  --public-ip-source amazon \
  --aws-service ec2
```

4. Simpan ID kolam untuk digunakan dalam perintah berikutnya.

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)
```

5. Menyediakan blok CIDR dari kolam dengan panjang netmask minimum /28.

```
aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id $POOL_ID \
  --netmask-length 28
```

Alokasikan alamat IP Elastis dari kolam IPAM

Ikuti langkah-langkah ini untuk mengalokasikan alamat IP Elastis (EIPs) dari kolam IPAM untuk peralatan HCX Service Mesh.

Amazon VPC console

1. Buka konsol Amazon VPC.
2. Di panel navigasi, pilih Elastic IPs.
3. Pilih Alokasi alamat IP elastis.
4. Pilih Alokasikan menggunakan kolam IPv4 IPAM.
5. Pilih IPv4 kolam umum milik Amazon yang sebelumnya Anda konfigurasikan.
6. Di bawah Alokasikan metode IPAM, pilih Input alamat secara manual dalam kolam IPAM.

> **Important**
>
> Anda tidak dapat mengaitkan dua EIP pertama EIPs atau terakhir dari blok CIDR IPAM publik ke subnet VLAN. Ini EIPs dicadangkan sebagai jaringan, gateway default, dan

alamat siaran. Amazon EVS memunculkan kesalahan validasi jika Anda mencoba mengaitkannya EIPs dengan subnet VLAN.

Important

Masukkan alamat secara manual dalam kumpulan IPAM untuk memastikan bahwa cadangan Amazon EVS tidak dialokasikan. EIPs Jika Anda mengizinkan IPAM untuk memilih EIP, IPAM dapat mengalokasikan EIP yang dicadangkan Amazon EVS, menyebabkan kegagalan selama asosiasi EIP ke subnet VLAN.

7. Tentukan EIP yang akan dialokasikan dari kolam IPAM.
8. Pilih Alokasikan.
9. Ulangi proses ini untuk mengalokasikan sisa EIPs yang Anda butuhkan. Anda diharuskan mengalokasikan setidaknya dua EIPs dari kolam IPAM untuk peralatan HCX Manager dan HCX Interconnect (HCX-IX). Alokasikan EIP tambahan untuk setiap perangkat jaringan HCX yang perlu Anda gunakan.

AWS CLI

1. Buka sesi terminal.
2. Dapatkan ID kolam IPAM yang Anda buat sebelumnya.

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)
```

3. Alokasikan alamat IP elastis dari kolam IPAM. Anda diharuskan mengalokasikan setidaknya dua EIPs dari kolam IPAM untuk peralatan HCX Manager dan HCX Interconnect (HCX-IX). Alokasikan EIP tambahan untuk setiap perangkat jaringan HCX yang perlu Anda gunakan.

Important

Anda tidak dapat mengaitkan dua EIP pertama EIPs atau terakhir dari blok CIDR IPAM publik dengan subnet VLAN. Ini EIPs dicadangkan sebagai jaringan, gateway default,

dan alamat siaran. Amazon EVS memunculkan kesalahan validasi jika Anda mencoba mengaitkannya EIPs dengan subnet VLAN.

Important

Masukkan alamat secara manual dalam kumpulan IPAM untuk memastikan bahwa cadangan Amazon EVS tidak dialokasikan. EIPs Jika Anda mengizinkan IPAM untuk memilih EIP, IPAM dapat mengalokasikan EIP yang dicadangkan Amazon EVS, menyebabkan kegagalan selama asosiasi EIP ke subnet VLAN.

```
aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-
manager-eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.3

aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-ix-
eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.4

aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-ne-
eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.5
```

Tambahkan blok IPv4 CIDR publik dari kolam IPAM ke VPC untuk koneksi internet HCX

Untuk mengaktifkan konektivitas internet HCX, Anda harus menambahkan blok IPv4 CIDR publik dari kolam IPAM ke VPC Anda sebagai CIDR tambahan. Amazon EVS menggunakan blok CIDR ini untuk menghubungkan VMware HCX ke jaringan Anda. Ikuti langkah-langkah ini untuk menambahkan blok CIDR ke VPC Anda.

> **Important**
>
> Anda harus memasukkan blok IPv4 CIDR secara manual yang Anda tambahkan ke VPC Anda. Amazon EVS tidak mendukung penggunaan blok CIDR yang dialokasikan IPAM saat ini. Penggunaan blok CIDR yang dialokasikan IPAM dapat mengakibatkan kegagalan asosiasi EIP.

Amazon VPC console

1. Buka konsol Amazon VPC.
2. Di panel navigasi, pilih Your VPCs.
3. Pilih VPC yang sebelumnya Anda buat, dan pilih Tindakan, Edit. CIDRs
4. Pilih Tambahkan IPV4 CIDR baru.
5. Pilih input manual IPV4 CIDR.
6. Tentukan blok CIDR dari kolam IPAM publik yang sebelumnya Anda buat.

AWS CLI

1. Buka sesi terminal.
2. Dapatkan ID kolam IPAM dan blok CIDR yang disediakan.

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)

CIDR_BLOCK=$(aws ec2 get-ipam-pool-cidrs \
  --ipam-pool-id $POOL_ID \
  --query 'IpamPoolCidrs[0].Cidr' \
  --output text)
```

3. Tambahkan blok CIDR ke VPC Anda.

```
aws ec2 associate-vpc-cidr-block \
  --vpc-id $VPC_ID \
  --cidr-block $CIDR_BLOCK
```

Konfigurasikan tabel rute utama VPC

Subnet Amazon EVS VLAN secara implisit terkait dengan tabel rute utama VPC. Untuk mengaktifkan konektivitas ke layanan dependen seperti DNS atau sistem lokal agar penerapan lingkungan berhasil, Anda harus mengonfigurasi tabel rute utama untuk memungkinkan lalu lintas ke sistem ini. Tabel rute utama harus menyertakan rute untuk CIDR VPC. Penggunaan tabel rute utama hanya diperlukan untuk penerapan lingkungan Amazon EVS awal. Setelah penerapan lingkungan, Anda dapat mengonfigurasi lingkungan Anda untuk menggunakan tabel rute khusus. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan tabel rute khusus”.

Setelah penerapan lingkungan, Anda harus secara eksplisit mengaitkan setiap subnet Amazon EVS VLAN dengan tabel rute di VPC Anda. Konektivitas NSX gagal jika subnet VLAN Anda tidak secara eksplisit terkait dengan tabel rute VPC. Kami sangat menyarankan agar Anda secara eksplisit mengaitkan subnet Anda dengan tabel rute khusus setelah penerapan lingkungan. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan tabel rute utama VPC”.

Important

Amazon EVS mendukung penggunaan tabel rute khusus hanya setelah lingkungan Amazon EVS dibuat. Tabel rute khusus tidak boleh digunakan selama pembuatan lingkungan Amazon EVS, karena hal ini dapat mengakibatkan masalah konektivitas.

Mengonfigurasi server DNS dan NTP menggunakan set opsi DHCP VPC

Important

Penerapan lingkungan Anda gagal jika Anda tidak memenuhi persyaratan Amazon EVS ini:

- Sertakan alamat IP server DNS primer dan alamat IP server DNS sekunder dalam set opsi DHCP.
- Sertakan zona pencarian maju DNS dengan catatan A untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda.
- Sertakan zona pencarian terbalik DNS dengan catatan PTR untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda.
- Konfigurasikan tabel rute utama VPC untuk memastikan rute ke server DNS Anda ada.

- Pastikan pendaftaran nama domain Anda valid dan belum kedaluwarsa, dan tidak ada duplikat nama host atau alamat IP.
- Konfigurasikan grup keamanan dan daftar kontrol akses jaringan (ACLs) agar Amazon EVS dapat berkomunikasi dengan:
  - Server DNS melalui TCP/UDP port 53.
  - Manajemen host VLAN subnet melalui HTTPS dan SSH.
  - Manajemen VLAN subnet melalui HTTPS dan SSH.

Amazon EVS menggunakan opsi DHCP VPC Anda yang disetel untuk mengambil yang berikut:

- Domain Name System (DNS) server untuk resolusi alamat IP host.
- Nama domain untuk resolusi DNS.
- Server Network Time Protocol (NTP) untuk sinkronisasi waktu.

Anda dapat membuat set opsi DHCP menggunakan Amazon VPC konsol atau AWS CLI. Untuk informasi selengkapnya, lihat Membuat opsi DHCP yang diatur dalam Panduan Amazon VPC Pengguna.

Konfigurasikan server DNS

Konfigurasi DNS memungkinkan resolusi nama host di lingkungan Amazon EVS Anda. Agar berhasil menerapkan lingkungan Amazon EVS, set opsi DHCP VPC Anda harus memiliki pengaturan DNS berikut:

- Alamat IP server DNS primer dan alamat IP server DNS sekunder di set opsi DHCP.
- Zona pencarian maju DNS dengan catatan A untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda.
- Zona pencarian terbalik dengan catatan PTR untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda. Untuk konfigurasi NTP, Anda dapat menggunakan alamat NTP Amazon default`169.254.169.123`, atau IPv4 alamat lain yang Anda inginkan.

Untuk informasi selengkapnya tentang mengonfigurasi server DNS dalam set opsi DHCP, lihat Membuat set opsi DHCP.

Konfigurasikan DNS untuk konektivitas lokal

Untuk konektivitas lokal, kami merekomendasikan penggunaan zona host pribadi Route 53 dengan resolver masuk. Pengaturan ini memungkinkan resolusi DNS hybrid, di mana Anda dapat menggunakan Route 53 untuk DNS internal dalam VPC Anda dan mengintegrasikannya dengan infrastruktur DNS lokal yang ada. Hal ini memungkinkan sumber daya dalam VPC Anda untuk menyelesaikan nama domain yang dihosting di jaringan lokal Anda, dan sebaliknya, tanpa memerlukan konfigurasi yang rumit. Jika diperlukan, Anda juga dapat menggunakan server DNS Anda sendiri dengan resolver keluar Route 53. Untuk langkah-langkah untuk mengonfigurasi, lihat Membuat zona yang dihosting pribadi dan Meneruskan kueri DNS masuk ke VPC Anda di Panduan Pengembang Amazon Route 53.

> **Note**
>
> Menggunakan Route 53 dan server Sistem Nama Domain (DNS) kustom di set opsi DHCP dapat menyebabkan perilaku yang tidak terduga.

> **Note**
>
> Jika Anda menggunakan nama domain DNS kustom yang ditentukan di zona host pribadi di Route 53, atau menggunakan DNS pribadi dengan titik akhir VPC antarmuka (AWS PrivateLink), Anda harus menyetel atribut dan ke. `enableDnsHostnames` `enableDnsSupport` `true` Untuk informasi selengkapnya, lihat atribut DNS untuk VPC Anda.

Memecahkan masalah jangkauan DNS

Amazon EVS memerlukan koneksi persisten ke SDDC Manager dan server DNS di opsi DHCP VPC Anda yang disetel untuk mencapai catatan DNS. Jika koneksi persisten ke SDDC Manager menjadi tidak tersedia, Amazon EVS tidak akan lagi dapat memvalidasi status lingkungan, dan Anda mungkin kehilangan akses lingkungan. Untuk langkah-langkah untuk memecahkan masalah ini, lihat. the section called “Pemeriksaan jangkauan gagal”

Konfigurasikan server NTP

Server NTP menyediakan waktu untuk jaringan Anda. Referensi waktu yang konsisten dan akurat pada EC2 instans Amazon Anda sangat penting untuk banyak tugas dan proses lingkungan VCF. Sinkronisasi waktu sangat penting untuk:

- Pencatatan dan audit sistem
- Operasi keamanan
- Manajemen sistem terdistribusi
- Pemecahan masalah

Anda dapat memasukkan IPv4 alamat hingga empat server NTP di set opsi DHCP VPC Anda. Anda dapat menentukan Layanan Sinkronisasi Waktu Amazon di IPv4 alamat`169.254.169.123`. Secara default, EC2 instans Amazon yang digunakan Amazon EVS menggunakan Layanan Sinkronisasi Waktu Amazon di alamat. IPv4 `169.254.169.123`

Untuk informasi selengkapnya tentang server NTP, lihat RFC 2123. Untuk informasi selengkapnya tentang Layanan Sinkronisasi Waktu Amazon, lihat Sinkronisasi jam dan waktu presisi di EC2 instans Anda dan Mengonfigurasi NTP di Host VMware Cloud Foundation dalam dokumentasi VMware Cloud Foundation.

Untuk mengkonfigurasi pengaturan NTP

1. Pilih sumber NTP Anda:
   - Layanan Sinkronisasi Waktu Amazon (disarankan)
   - Server NTP khusus
2. Tambahkan server NTP ke set opsi DHCP Anda. Untuk informasi selengkapnya, lihat Membuat opsi DHCP yang disetel di Panduan Pengguna Amazon VPC.
3. Verifikasi sinkronisasi waktu. Untuk informasi selengkapnya tentang konfigurasi set opsi DHCP, lihatthe section called “Konfigurasikan set opsi DHCP VPC Anda”.

Konfigurasikan konektivitas jaringan lokal (opsional)

Anda dapat mengonfigurasi konektivitas untuk pusat data lokal ke AWS infrastruktur Anda menggunakan Direct Connect gateway transit terkait, atau menggunakan lampiran AWS Site-to-Site VPN ke gateway transit.

Untuk mengaktifkan konektivitas ke sistem lokal agar penerapan lingkungan berhasil, Anda harus mengonfigurasi tabel rute utama VPC untuk memungkinkan lalu lintas ke sistem ini. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan tabel rute utama VPC”.

Setelah lingkungan Amazon EVS dibuat, Anda harus memperbarui tabel rute gateway transit dengan CIDRs VPC yang dibuat dalam lingkungan Amazon EVS. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan tabel rute gateway transit dan awalan Direct Connect untuk konektivitas lokal (opsional)”.

Untuk informasi selengkapnya tentang pengaturan Direct Connect koneksi, lihat Direct Connect gateway dan asosiasi gateway transit. Untuk informasi selengkapnya tentang penggunaan AWS Site-to-Site VPN dengan AWS Transit Gateway, lihat lampiran AWS Site-to-Site VPN di Gateway Amazon VPC Transit di Panduan Pengguna Gateway Amazon VPC Transit.

> **Note**
>
> Amazon EVS tidak mendukung konektivitas melalui antarmuka virtual pribadi AWS Direct Connect (VIF), atau melalui koneksi AWS Site-to-Site VPN yang berakhir langsung ke VPC underlay.

Siapkan instance VPC Route Server dengan titik akhir dan rekan

Amazon EVS menggunakan Amazon VPC Route Server untuk mengaktifkan perutean dinamis berbasis BGP ke jaringan underlay VPC Anda. Anda harus menentukan server rute yang berbagi rute ke setidaknya dua titik akhir server rute di subnet akses layanan. ASN peer yang dikonfigurasi pada peer server rute harus cocok, dan alamat IP peer harus unik.

Jika Anda mengonfigurasi Route Server untuk konektivitas internet HCX, Anda harus mengonfigurasi propagasi Route Server untuk subnet akses layanan dan subnet publik yang Anda buat pada langkah pertama prosedur ini.

> **Important**
>
> Penerapan lingkungan Anda gagal jika Anda tidak memenuhi persyaratan Amazon EVS ini untuk konfigurasi Server Rute VPC:
>
> - Anda harus mengkonfigurasi setidaknya dua titik akhir server rute di subnet akses layanan.

- Saat mengonfigurasi Border Gateway Protocol (BGP) untuk gateway Tier-0, nilai ASN rekan VPC Route Server harus sesuai dengan nilai ASN peer NSX Edge.
- Saat membuat dua rekan server rute, Anda harus menggunakan alamat IP unik dari VLAN uplink NSX untuk setiap titik akhir. Kedua alamat IP ini akan ditetapkan ke tepi NSX selama penyebaran lingkungan Amazon EVS.
- Saat mengaktifkan propagasi Route Server, Anda harus memastikan bahwa semua tabel rute yang disebarkan memiliki setidaknya satu asosiasi subnet eksplisit. Iklan rute BGP gagal jika tabel rute yang disebarkan tidak memiliki asosiasi subnet eksplisit.

Untuk informasi selengkapnya tentang pengaturan VPC Route Server, lihat tutorial memulai Route Server.

Important

Saat mengaktifkan propagasi Route Server, pastikan bahwa semua tabel rute yang disebarkan memiliki setidaknya satu asosiasi subnet eksplisit. Iklan rute BGP gagal jika tabel rute memang memiliki asosiasi subnet eksplisit.

Note

Untuk deteksi keaktifan rekan Route Server, Amazon EVS hanya mendukung mekanisme keepalive BGP default. Amazon EVS tidak mendukung Deteksi Penerusan Dua Arah (BFD) multi-hop.

Note

Kami menyarankan Anda mengaktifkan rute persisten untuk instance server rute dengan durasi bertahan antara 1-5 menit. Jika diaktifkan, rute akan dipertahankan dalam database routing server rute bahkan jika semua sesi BGP berakhir. Untuk informasi selengkapnya, lihat Membuat server rute di Panduan Amazon VPC Pengguna.

> **Note**
>
> Jika Anda menggunakan gateway NAT atau gateway transit, pastikan server rute Anda dikonfigurasi dengan benar untuk menyebarkan rute NSX ke tabel rute VPC.

Pemecahan masalah

Jika Anda mengalami masalah:

- Verifikasi bahwa setiap tabel rute memiliki asosiasi subnet eksplisit.
- Periksa apakah nilai ASN peer dimasukkan untuk server rute dan gateway NSX Tier-0 cocok.
- Konfirmasikan bahwa alamat IP titik akhir Route Server unik.
- Tinjau status propagasi rute di tabel rute Anda.
- Gunakan peer logging VPC Route Server untuk memantau kesehatan sesi BGP dan memecahkan masalah koneksi. Untuk informasi selengkapnya, lihat Route server peer logging di Panduan Pengguna Amazon VPC.

Buat ACL jaringan untuk mengontrol lalu lintas subnet Amazon EVS VLAN

Amazon EVS menggunakan daftar kontrol akses jaringan (ACL) untuk mengontrol lalu lintas ke dan dari subnet Amazon EVS VLAN. Anda dapat menggunakan ACL jaringan default untuk VPC Anda, atau Anda dapat membuat ACL jaringan khusus untuk VPC Anda dengan aturan yang mirip dengan aturan untuk grup keamanan Anda untuk menambahkan lapisan keamanan ke VPC Anda. Untuk informasi selengkapnya, lihat Membuat ACL jaringan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Jika Anda berencana untuk mengonfigurasi konektivitas internet HCX, pastikan bahwa aturan ACL jaringan yang Anda konfigurasikan memungkinkan koneksi masuk dan keluar yang diperlukan untuk komponen HCX. Untuk informasi selengkapnya tentang persyaratan port HCX, lihat Panduan Pengguna VMware HCX.

Important

Jika Anda terhubung melalui internet, mengaitkan alamat IP Elastis dengan VLAN menyediakan akses internet langsung ke semua sumber daya di subnet VLAN tersebut. Pastikan Anda memiliki daftar kontrol akses jaringan yang sesuai yang dikonfigurasi untuk membatasi akses sesuai kebutuhan untuk persyaratan keamanan Anda.

Important

EC2 grup keamanan tidak berfungsi pada antarmuka jaringan elastis yang dilampirkan ke subnet Amazon EVS VLAN. Untuk mengontrol lalu lintas ke dan dari subnet Amazon EVS VLAN, Anda harus menggunakan daftar kontrol akses jaringan.

Buat lingkungan Amazon EVS

Important

Untuk memulai sesederhana dan secepat mungkin, topik ini mencakup langkah-langkah untuk membuat lingkungan Amazon EVS dengan pengaturan default. Sebelum membuat lingkungan, kami sarankan Anda membiasakan diri dengan semua pengaturan dan menerapkan lingkungan dengan pengaturan yang memenuhi persyaratan Anda. Lingkungan hanya dapat dikonfigurasi selama pembuatan lingkungan awal. Lingkungan tidak dapat dimodifikasi setelah Anda membuatnya. Untuk gambaran umum tentang semua kemungkinan pengaturan lingkungan Amazon EVS, lihat Panduan Referensi Amazon EVS API.

Note

ID lingkungan Anda akan tersedia untuk Amazon EVS di semua AWS Wilayah untuk kebutuhan kepatuhan lisensi VCF.

> **Note**
>
> Lingkungan Amazon EVS harus disebarkan ke Wilayah dan Zona Ketersediaan yang sama dengan subnet VPC dan VPC.

Selesaikan langkah ini untuk membuat lingkungan Amazon EVS dengan host dan subnet VLAN.

Example

Amazon EVS console

1. Buka konsol Amazon EVS.

   > **Note**
   >
   > Pastikan bahwa AWS Wilayah yang ditampilkan di kanan atas konsol Anda adalah AWS Wilayah tempat Anda ingin membuat lingkungan Anda. Jika tidak, pilih dropdown di sebelah nama AWS Region dan pilih AWS Region yang ingin Anda gunakan.

2. Pada panel navigasi, pilih Lingkungan.
3. Pilih Buat lingkungan.
4. Pada halaman Validasi persyaratan Amazon EVS, periksa apakah persyaratan layanan telah terpenuhi. Untuk informasi selengkapnya, lihat Menyiapkan VMware Layanan Elastis Amazon.
   a. (Opsional) Untuk Nama, masukkan nama lingkungan.
   b. Untuk versi Lingkungan, pilih versi VCF Anda. Untuk informasi tentang versi VCF yang disediakan oleh Amazon EVS, lihat. the section called “Versi dan instance VCF EC2 ”
   c. Untuk ID Situs, masukkan ID Situs Broadcom Anda.
   d. Untuk kunci Solusi VCF, masukkan kunci solusi VCF (VMware vSphere 8 Enterprise Plus untuk VCF). Kunci lisensi ini tidak dapat digunakan oleh lingkungan yang ada.

      > **Note**
      >
      > Kunci solusi VCF harus memiliki setidaknya 256 core.

> **Note**
>
> Lisensi VCF Anda akan tersedia untuk Amazon EVS di semua AWS Wilayah untuk kepatuhan lisensi. Amazon EVS tidak memvalidasi kunci lisensi. Untuk memvalidasi kunci lisensi, kunjungi dukungan Broadcom.

> **Note**
>
> Amazon EVS mengharuskan Anda mempertahankan kunci solusi VCF yang valid di SDDC Manager agar layanan berfungsi dengan baik. Jika Anda mengelola kunci solusi VCF menggunakan pasca-penyebaran Klien vSphere, Anda harus memastikan bahwa kunci juga muncul di layar lisensi antarmuka pengguna SDDC Manager.

e. Untuk kunci lisensi vSAN, masukkan kunci lisensi vSAN. Kunci lisensi ini tidak dapat digunakan oleh lingkungan yang ada.

> **Note**
>
> Kunci lisensi vSAN harus memiliki setidaknya 110 TiB kapasitas vSAN.

> **Note**
>
> Lisensi VCF Anda akan tersedia untuk Amazon EVS di semua AWS Wilayah untuk kepatuhan lisensi. Amazon EVS tidak memvalidasi kunci lisensi. Untuk memvalidasi kunci lisensi, kunjungi dukungan Broadcom.

> **Note**
>
> Amazon EVS mengharuskan Anda mempertahankan kunci lisensi vSAN yang valid di Manajer SDDC untuk memilih layanan agar berfungsi dengan baik. Jika Anda mengelola kunci lisensi vSAN menggunakan pasca-penyebaran Klien vSphere,

Anda harus memastikan bahwa kunci juga muncul di layar lisensi antarmuka pengguna SDDC Manager.

f. Untuk persyaratan lisensi VCF, centang kotak untuk mengonfirmasi bahwa Anda telah membeli dan akan terus mempertahankan jumlah lisensi perangkat lunak VCF yang diperlukan untuk mencakup semua inti prosesor fisik di lingkungan Amazon EVS. Informasi tentang perangkat lunak VCF Anda di Amazon EVS akan dibagikan dengan Broadcom untuk memverifikasi kepatuhan lisensi.

g. Pilih Berikutnya.

5. Pada halaman Tentukan detail host, selesaikan langkah-langkah berikut empat kali untuk menambahkan empat host ke lingkungan. Lingkungan Amazon EVS memerlukan empat host untuk penerapan awal.

a. Pilih Tambahkan detail host.

b. Untuk nama host DNS, masukkan nama host untuk host.

c. Misalnya jenis, pilih jenis EC2 instance.

d. Untuk versi host ESX, selama pembuatan lingkungan versi ESX default untuk versi VCF yang dipilih akan digunakan. Untuk informasi selengkapnya, lihat the section called “Versi dan instance VCF EC2 ”.

> **Important**
>
> Jangan menghentikan atau menghentikan EC2 instance yang diterapkan Amazon EVS. Tindakan ini mengakibatkan hilangnya data.

> **Note**
>
> Amazon EVS hanya mendukung EC2 instans i4i.metal saat ini.

e. Untuk key pair SSH, pilih key pair SSH untuk akses SSH ke host.

f. Pilih Tambahkan host.

6. Pada halaman Konfigurasi jaringan dan konektivitas, lakukan hal berikut.

a. Untuk persyaratan konektivitas HCX, pilih apakah Anda ingin menggunakan HCX dengan konektivitas pribadi atau melalui internet.

b. Untuk VPC, pilih VPC yang sebelumnya Anda buat.

c. (Hanya untuk koneksi internet HCX) Untuk jaringan HCX ACL, pilih ACL jaringan mana yang akan dikaitkan dengan VLAN HCX Anda.

> **Important**
>
> Kami sangat menyarankan Anda membuat ACL jaringan khusus yang didedikasikan untuk HCX VLAN. Untuk informasi selengkapnya, lihat the section called "Konfigurasikan ACL jaringan".

d. Untuk subnet akses Layanan, pilih subnet pribadi yang dibuat saat Anda membuat VPC.

e. Untuk grup Keamanan - opsional, Anda dapat memilih hingga dua grup keamanan yang mengontrol komunikasi antara bidang kontrol Amazon EVS dan VPC. Amazon EVS menggunakan grup keamanan default jika tidak ada grup keamanan yang dipilih.

> **Note**
>
> Pastikan bahwa grup keamanan yang Anda pilih menyediakan konektivitas ke server DNS dan subnet Amazon EVS VLAN Anda.

f. Di bawah konektivitas Manajemen, masukkan blok CIDR yang akan digunakan untuk subnet Amazon EVS VLAN. Untuk blok VLAN CIDR uplink HCX, jika mengkonfigurasi VLAN HCX publik, Anda harus menentukan blok CIDR dengan panjang netmask tepatnya /28. Amazon EVS memunculkan kesalahan validasi jika ukuran blok CIDR lainnya ditentukan untuk VLAN HCX publik. Untuk VLAN HCX pribadi dan semua blok VLANs CIDR lainnya, panjang netmask minimum yang dapat Anda gunakan adalah/28 dan maksimumnya adalah /24.

> **Important**
>
> Subnet Amazon EVS VLAN hanya dapat dibuat selama pembuatan lingkungan Amazon EVS, dan tidak dapat dimodifikasi setelah lingkungan dibuat. Anda harus memastikan bahwa blok CIDR subnet VLAN berukuran benar sebelum membuat lingkungan. Anda tidak akan dapat menambahkan subnet VLAN setelah lingkungan digunakan. Untuk informasi selengkapnya, lihat the section called "Pertimbangan jaringan Amazon EVS".

g. Di bawah Ekspansi VLANs, masukkan blok CIDR untuk subnet Amazon EVS VLAN tambahan yang dapat digunakan untuk memperluas kemampuan VCF dalam Amazon EVS, seperti mengaktifkan Federasi NSX.

h. Di bawah konektivitas beban kerja/VCF, masukkan blok CIDR untuk VLAN uplink NSX, dan pilih dua rekan Server Rute VPC yang mengintip titik akhir Server IDs Route melalui uplink NSX.

> **Note**
>
> Amazon EVS memerlukan instance VPC Route Server yang dikaitkan dengan dua titik akhir Route Server dan dua rekan Server Route sebelum penerapan EVS. Konfigurasi ini memungkinkan perutean berbasis BGP dinamis melalui uplink NSX. Untuk informasi selengkapnya, lihat the section called “Siapkan instance VPC Route Server dengan titik akhir dan rekan”.

i. Pilih Berikutnya.

7. Pada halaman Tentukan nama host DNS Manajemen, lakukan hal berikut.

a. Di bawah nama host DNS alat Manajemen, masukkan nama host DNS untuk mesin virtual untuk meng-host peralatan manajemen VCF. Jika menggunakan Route 53 sebagai penyedia DNS Anda, pilih juga zona yang dihosting yang berisi catatan DNS Anda.

b. Di bawah Credentials, pilih apakah Anda ingin menggunakan kunci KMS AWS terkelola untuk Secrets Manager atau kunci KMS yang dikelola pelanggan yang Anda berikan. Kunci ini digunakan untuk mengenkripsi kredensi VCF yang diperlukan untuk menggunakan SDDC Manager, NSX Manager, dan peralatan vCenter.

> **Note**
>
> Ada biaya penggunaan yang terkait dengan kunci KMS yang dikelola pelanggan. Untuk informasi lebih lanjut, lihat halaman harga AWS KMS.

c. Pilih Berikutnya.

8. (Opsional) Pada halaman Tambahkan tag, tambahkan tag apa pun yang ingin Anda tetapkan ke lingkungan ini dan pilih Berikutnya.

> **Note**
>
> Host yang dibuat sebagai bagian dari lingkungan ini akan menerima tag berikut:`DoNotDelete-EVS-<environmentid>-<hostname>`.

> **Note**
>
> Tag yang terkait dengan lingkungan Amazon EVS tidak menyebar ke AWS sumber daya dasar seperti EC2 instance. Anda dapat membuat tag pada AWS sumber daya yang mendasarinya menggunakan konsol layanan masing-masing atau AWS CLI.

9. Pada halaman Tinjau dan buat, tinjau konfigurasi Anda dan pilih Buat lingkungan.

> **Important**
>
> Selama penerapan lingkungan, Amazon EVS membuat subnet EVS VLAN dan secara implisit mengaitkannya dengan tabel rute utama. Setelah penerapan selesai, Anda harus secara eksplisit mengaitkan subnet Amazon EVS VLAN dengan tabel rute untuk tujuan konektivitas NSX. Untuk informasi selengkapnya, lihat the section called “Secara eksplisit mengaitkan subnet Amazon EVS VLAN ke tabel rute VPC”.

> **Note**
>
> Amazon EVS menerapkan versi paket VMware Cloud Foundation terbaru yang mungkin tidak menyertakan pembaruan produk individual, yang dikenal sebagai tambalan asinkron. Setelah menyelesaikan penerapan ini, kami sangat menyarankan Anda meninjau dan memperbarui produk individual menggunakan Broadcom's Async Patch Tool (AP Tool) atau otomatisasi LCM dalam produk Manajer SDDC. Upgrade NSX harus dilakukan di luar SDDC Manager.

> **Note**
>
> Penciptaan lingkungan bisa memakan waktu beberapa jam.

AWS CLI

1. Buka sesi terminal.
2. Buat lingkungan Amazon EVS. Di bawah ini adalah contoh `aws evs create-environment` permintaan.

> **Important**
>
> Sebelum menjalankan `aws evs create-environment` perintah, periksa apakah semua prasyarat Amazon EVS telah terpenuhi. Penerapan lingkungan gagal jika prasyarat belum terpenuhi. Untuk informasi selengkapnya, lihat Menyiapkan VMware Layanan Elastis Amazon.

> **Important**
>
> Selama penerapan lingkungan, Amazon EVS membuat subnet EVS VLAN dan secara implisit mengaitkannya dengan tabel rute utama. Setelah penerapan selesai, Anda harus secara eksplisit mengaitkan subnet Amazon EVS VLAN dengan tabel rute untuk tujuan konektivitas NSX. Untuk informasi selengkapnya, lihat the section called “Secara eksplisit mengaitkan subnet Amazon EVS VLAN ke tabel rute VPC”.

> **Note**
>
> Amazon EVS menerapkan versi paket VMware Cloud Foundation terbaru yang mungkin tidak menyertakan pembaruan produk individual, yang dikenal sebagai tambalan asinkron. Setelah menyelesaikan penerapan ini, kami sangat menyarankan Anda meninjau dan memperbarui produk individual menggunakan Broadcom's Async Patch Tool (AP Tool) atau otomatisasi LCM dalam produk Manajer SDDC. Upgrade NSX harus dilakukan di luar SDDC Manager.

> **Note**
>
> Penyebaran lingkungan bisa memakan waktu beberapa jam.

- Untuk `--vpc-id`, tentukan VPC yang sebelumnya Anda buat dengan rentang IPv4 CIDR minimum/22.
- Untuk `--service-access-subnet-id`, tentukan ID unik subnet pribadi yang dibuat saat Anda membuat VPC.
- Untuk `--vcf-version`, Lihat the section called “Versi dan instance VCF EC2 ” untuk versi VCF yang disediakan oleh Amazon EVS,
- Dengan `--terms-accepted`, Anda mengonfirmasi bahwa Anda telah membeli dan akan terus mempertahankan jumlah lisensi perangkat lunak VCF yang diperlukan untuk mencakup semua inti prosesor fisik di lingkungan Amazon EVS. Informasi tentang perangkat lunak VCF Anda di Amazon EVS akan dibagikan dengan Broadcom untuk memverifikasi kepatuhan lisensi.
- Untuk `--license-info`, masukkan kunci solusi VCF Anda (VMware vSphere 8 Enterprise Plus untuk VCF) dan kunci lisensi vSAN.

> **Note**
>
> Kunci solusi VCF harus memiliki setidaknya 256 core. Kunci lisensi vSAN harus memiliki setidaknya 110 TiB kapasitas vSAN.

> **Note**
>
> Amazon EVS mengharuskan Anda mempertahankan kunci solusi VCF yang valid dan kunci lisensi vSAN di SDDC Manager agar layanan berfungsi dengan baik. Jika Anda mengelola kunci lisensi ini menggunakan pasca-penyebaran Klien vSphere, Anda harus memastikan bahwa kunci tersebut juga muncul di layar lisensi antarmuka pengguna SDDC Manager.

> **Note**
>
> Kunci solusi VCF dan kunci lisensi vSAN tidak dapat digunakan oleh lingkungan Amazon EVS yang ada.

- Untuk `--initial-vlans` tentukan rentang CIDR untuk subnet Amazon EVS VLAN yang dibuat Amazon EVS atas nama Anda. Ini VLANs digunakan untuk menyebarkan peralatan manajemen VCF. Jika mengkonfigurasi VLAN HCX publik, Anda harus menentukan blok CIDR dengan panjang netmask persis /28. Amazon EVS memunculkan kesalahan validasi jika ukuran blok CIDR lainnya ditentukan untuk VLAN HCX publik. Untuk VLAN HCX pribadi dan semua blok VLANs CIDR lainnya, panjang netmask minimum yang dapat Anda gunakan adalah/28 dan maksimumnya adalah /24.
- `hcxNetworkAclId`digunakan jika mengkonfigurasi konektivitas internet HCX. Tentukan ACL jaringan khusus untuk VLAN HCX publik.

> **Important**
>
> Kami sangat menyarankan Anda membuat ACL jaringan khusus yang didedikasikan untuk HCX VLAN. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan ACL jaringan”.

> **Important**
>
> Subnet Amazon EVS VLAN hanya dapat dibuat selama pembuatan lingkungan Amazon EVS, dan tidak dapat dimodifikasi setelah lingkungan dibuat. Anda harus memastikan bahwa blok CIDR subnet VLAN berukuran benar sebelum membuat lingkungan. Anda tidak akan dapat menambahkan subnet VLAN setelah lingkungan digunakan. Untuk informasi selengkapnya, lihat the section called “Pertimbangan jaringan Amazon EVS”.

- Untuk`--hosts`, tentukan detail host untuk host yang diperlukan Amazon EVS untuk penerapan lingkungan. Sertakan nama host DNS, nama kunci EC2 SSH, dan jenis EC2 instance untuk setiap host. ID host khusus adalah opsional.

> **Important**
>
> Jangan menghentikan atau menghentikan EC2 instance yang diterapkan Amazon EVS. Tindakan ini mengakibatkan hilangnya data.

> **Note**
>
> Amazon EVS hanya mendukung EC2 instans i4i.metal saat ini.

- Untuk `--connectivity-info`, tentukan 2 VPC Route Server peer IDs yang Anda buat pada langkah sebelumnya.

> **Note**
>
> Amazon EVS memerlukan instance VPC Route Server yang dikaitkan dengan dua titik akhir Route Server dan dua rekan Server Route sebelum penerapan EVS. Konfigurasi ini memungkinkan perutean berbasis BGP dinamis melalui uplink NSX. Untuk informasi selengkapnya, lihat the section called “Siapkan instance VPC Route Server dengan titik akhir dan rekan”.

- Untuk `--vcf-hostnames`, masukkan nama host DNS untuk mesin virtual untuk meng-host peralatan manajemen VCF.
- Untuk `--site-id`, masukkan ID situs Broadcom unik Anda. ID ini memungkinkan akses ke portal Broadcom dan diberikan kepada Anda oleh Broadcom saat kontrak perangkat lunak Anda berakhir atau diperpanjang.
- (Opsional) Untuk `--region`, masukkan Wilayah tempat lingkungan Anda akan digunakan. Jika Region tidak ditentukan, Region default Anda akan digunakan.

```
aws evs create-environment \
--environment-name testEnv \
--vpc-id vpc-1234567890abcdef0 \
--service-access-subnet-id subnet-01234a1b2cde1234f \
--vcf-version VCF-5.2.2 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"isHcxPublic\": true,
      \"hcxNetworkAclId\": \"nacl-abcd1234\",
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
```

```
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
        \"cidr\": \"10.10.3.0/24\"
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07879acf49EXAMPLE\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07878bde50EXAMPLE\"
    },
    {
      \"hostName\": \"esx03\",
```

```
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07877eio51EXAMPLE\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07863ghi52EXAMPLE\"
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

Berikut ini adalah contoh respon.

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATING",
        "stateDetails": "The environment is being initialized, this operation
 may take some time to complete.",
        "createdAt": "2025-04-13T12:03:39.718000+00:00",
        "modifiedAt": "2025-04-13T12:03:39.718000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-1234567890abcdef0",
```

```
        "serviceAccessSubnetId": "subnet-01234a1b2cde1234f",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-1234567890abcdef0",
                "rsp-abcdef01234567890"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        }
    }
}
```

Verifikasi pembuatan lingkungan Amazon EVS

Example

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Pada panel navigasi, pilih Lingkungan.
3. Pilih lingkungan.
4. Pilih tab Detail.

5. Periksa apakah status Lingkungan Lulus dan status Lingkungan Dibuat. Ini memberi tahu Anda bahwa lingkungan siap digunakan.

> **Note**
>
> Penciptaan lingkungan bisa memakan waktu beberapa jam. Jika status Lingkungan masih menunjukkan Membuat, segarkan halaman.

AWS CLI

1. Buka sesi terminal.
2. Jalankan perintah berikut, menggunakan ID lingkungan untuk lingkungan Anda dan nama Wilayah yang berisi sumber daya Anda. Lingkungan siap digunakan saat `environmentState` ada`CREATED`.

> **Note**
>
> Penciptaan lingkungan bisa memakan waktu beberapa jam. Jika `environmentState` masih muncul`CREATING`, jalankan perintah lagi untuk menyegarkan output.

```
aws evs get-environment  --environment-id env-abcde12345
```

Berikut ini adalah contoh respon.

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATED",
        "createdAt": "2025-04-13T13:39:49.546000+00:00",
        "modifiedAt": "2025-04-13T13:40:39.355000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-0c6def5b7b61c9f41",
        "serviceAccessSubnetId": "subnet-06a3c3b74d36b7d5e",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
```

```
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "checks": [],
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-056b2b1727a51e956",
                "rsp-07f636c5150f171c3"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        },
        "credentials": []
    }
}
```

Secara eksplisit mengaitkan subnet Amazon EVS VLAN ke tabel rute VPC

Secara eksplisit mengaitkan setiap subnet Amazon EVS VLAN dengan tabel rute di VPC Anda. Tabel rute ini digunakan untuk memungkinkan AWS sumber daya berkomunikasi dengan mesin virtual di segmen jaringan NSX, berjalan dengan Amazon EVS. Jika Anda telah membuat VLAN HCX publik, pastikan untuk secara eksplisit mengaitkan subnet VLAN HCX publik dengan tabel rute publik di VPC Anda yang merutekan ke gateway internet.

Example

Amazon VPC console

1. Pergi ke konsol VPC.
2. Di panel navigasi, pilih Tabel rute.
3. Pilih tabel rute yang ingin Anda kaitkan dengan subnet Amazon EVS VLAN.
4. Pilih tab Asosiasi Subnet.
5. Di bawah Asosiasi subnet eksplisit, pilih Edit asosiasi subnet.
6. Pilih semua subnet Amazon EVS VLAN.
7. Pilih Simpan pengaitan.

AWS CLI

1. Buka sesi terminal.
2. Identifikasi subnet Amazon EVS VLAN. IDs

```
aws ec2 describe-subnets
```

3. Kaitkan subnet Amazon EVS VLAN Anda dengan tabel rute di VPC Anda.

```
aws ec2 associate-route-table \
--route-table-id rtb-0123456789abcdef0 \
--subnet-id subnet-01234a1b2cde1234f
```

Kaitkan EIPs dengan subnet VLAN publik HCX (Untuk konektivitas internet HCX)

Ikuti langkah-langkah ini untuk mengaitkan alamat IP Elastic (EIPs) dari kolam IPAM ke VLAN publik HCX untuk konektivitas internet HCX. Anda diharuskan untuk mengaitkan setidaknya dua EIPs untuk peralatan HCX Manager dan HCX Interconnect (HCX-IX). Kaitkan EIP tambahan untuk setiap perangkat jaringan HCX yang perlu Anda gunakan. Anda dapat memiliki hingga 13 EIPs dari kolam IPAM yang terkait dengan VLAN publik HCX.

Important

Konektivitas internet publik HCX gagal jika Anda tidak mengaitkan setidaknya dua EIPs dari kolam IPAM dengan subnet VLAN publik HCX.

Note

Amazon EVS hanya mendukung asosiasi EIPs dengan HCX VLAN saat ini.

Note

Anda tidak dapat mengaitkan dua EIP pertama EIPs atau terakhir dari blok CIDR IPAM publik dengan subnet VLAN. Ini EIPs dicadangkan sebagai jaringan, gateway default, dan alamat siaran. Amazon EVS memunculkan kesalahan validasi jika Anda mencoba mengaitkannya EIPs dengan subnet VLAN.

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Pada menu navigasi, pilih Lingkungan.
3. Pilih lingkungan.
4. Di bawah tab Jaringan dan konektivitas, pilih VLAN publik HCX.
5. Pilih Associate EIP ke VLAN.
6. Pilih alamat IP Elastis untuk dikaitkan dengan VLAN publik HCX.
7. Pilih Kaitkan EIPs.
8. Periksa asosiasi EIP untuk mengonfirmasi bahwa EIPs telah dikaitkan dengan VLAN publik HCX.

AWS CLI

1. Untuk mengaitkan alamat IP elastis dengan VLAN, gunakan `associate-eip-to-vlan` perintah contoh.

- `environment-id`- ID lingkungan Amazon EVS Anda.
- `vlan-name`- Nama VLAN untuk dikaitkan dengan alamat IP Elastis.
- `allocation-id`- ID alokasi alamat IP Elastis.

```
aws evs associate-eip-to-vlan \
  --environment-id "env-605uove256" \
  --vlan-name "hcx" \
  --allocation-id "eipalloc-0429268f30c4a34f7"
```

Perintah mengembalikan detail tentang VLAN, termasuk asosiasi EIP baru:

```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [
            {
                "associationId": "eipassoc-09e966faad7ecc58a",
                "allocationId": "eipalloc-0429268f30c4a34f7",
                "ipAddress": "18.97.137.2"
            }
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

`eipAssociations`Array menunjukkan asosiasi baru, termasuk:

- `associationId`- ID unik untuk asosiasi EIP ini, digunakan untuk disasosiasi.
- `allocationId`- ID alokasi alamat IP Elastis terkait.
- `ipAddress`- Alamat IP yang ditetapkan ke VLAN.

2. Ulangi langkah ini untuk mengaitkan tambahan EIPs.

Konfigurasikan tabel rute gateway transit dan awalan Direct Connect untuk konektivitas lokal (opsional)

Jika Anda mengonfigurasi konektivitas jaringan lokal menggunakan Direct Connect atau AWS Site-to-Site VPN dengan gateway transit, Anda harus memperbarui tabel rute gateway transit dengan VPC yang dibuat CIDRs dalam lingkungan Amazon EVS. Untuk informasi selengkapnya, lihat Tabel rute gateway transit di Amazon VPC Transit Gateways.

Jika Anda menggunakan AWS Direct Connect, Anda mungkin perlu juga memperbarui awalan Direct Connect untuk mengirim dan menerima rute terbaru dari VPC. Untuk informasi selengkapnya, lihat Mengizinkan interaksi awalan untuk gateway Direct AWS Connect.

Ambil kredensi VCF dan akses peralatan manajemen VCF

Amazon EVS menggunakan AWS Secrets Manager untuk membuat, mengenkripsi, dan menyimpan rahasia terkelola di akun Anda. Rahasia ini berisi kredensi VCF yang diperlukan untuk menginstal dan mengakses peralatan manajemen VCF seperti vCenter Server, NSX, dan SDDC Manager, serta kata sandi root ESX. Untuk informasi selengkapnya tentang mengambil rahasia, lihat Mendapatkan AWS rahasia dari Secrets Manager di Panduan Pengguna AWS Secrets Manager.

> **Note**
>
> Amazon EVS tidak menyediakan rotasi terkelola untuk rahasia Anda. Kami sarankan Anda rutin merotasi rahasia Anda dengan jadwal rotasi yang ditentukan untuk memastikan rahasia tidak berlaku lama.

Setelah Anda mengambil kredensi VCF Anda dari Secrets AWS Manager, Anda dapat menggunakannya untuk masuk ke peralatan manajemen VCF Anda. Untuk informasi selengkapnya, lihat Masuk ke Antarmuka Pengguna SDDC Manager dan Cara Menggunakan dan Mengkonfigurasi Klien vSphere Anda dalam dokumentasi produk. VMware

Konfigurasikan Konsol EC2 Serial (opsional)

Secara default, Amazon EVS mengaktifkan ESX Shell pada host Amazon EVS yang baru digunakan. Konfigurasi ini memungkinkan akses ke port serial EC2 instans Amazon melalui konsol EC2 serial, yang dapat Anda gunakan untuk memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya. Konsol serial tidak memerlukan instans Anda untuk memiliki kemampuan jaringan. Dengan

konsol serial, Anda dapat memasukkan perintah ke EC2 instance yang sedang berjalan seolah-olah keyboard dan monitor Anda langsung terpasang ke port serial instance.

Konsol EC2 serial dapat diakses menggunakan EC2 konsol atau AWS CLI. Untuk informasi selengkapnya, lihat Konsol EC2 Serial untuk instance di Panduan EC2 Pengguna Amazon.

> **Note**
>
> Konsol EC2 serial adalah satu-satunya mekanisme yang didukung Amazon EVS untuk mengakses Antarmuka Pengguna Konsol Langsung (DCUI) untuk berinteraksi dengan host ESX secara lokal.

> **Note**
>
> Amazon EVS menonaktifkan SSH jarak jauh secara default. Untuk informasi selengkapnya tentang mengaktifkan SSH mengakses ESX Shell jarak jauh, lihat Akses Shell ESX Jarak Jauh dengan SSH di dokumentasi produk vSphere. VMware

Connect ke Konsol EC2 Serial

Untuk terhubung ke konsol EC2 serial dan menggunakan alat yang Anda pilih untuk pemecahan masalah, tugas prasyarat tertentu harus diselesaikan. Untuk informasi selengkapnya, lihat Prasyarat untuk EC2 Konsol Serial dan Connect ke Konsol EC2 Serial di Panduan Pengguna Amazon. EC2

> **Note**
>
> Untuk terhubung ke konsol EC2 serial, status EC2 instans Anda harus`running`.
> Anda tidak dapat terhubung ke konsol serial jika instance dalam`pending`,,`stopping`, `stopped`shutting-down, atau `terminated` status. Untuk informasi selengkapnya tentang perubahan status instans, lihat perubahan status EC2 instans Amazon di Panduan EC2 Pengguna Amazon.

Konfigurasikan akses ke Konsol EC2 Serial

Untuk mengonfigurasi akses ke konsol EC2 serial, Anda atau administrator harus memberikan akses konsol serial di tingkat akun dan kemudian mengonfigurasi kebijakan IAM untuk memberikan akses

ke pengguna Anda. Untuk instance Linux, Anda juga harus mengonfigurasi pengguna berbasis kata sandi pada setiap instance sehingga pengguna Anda dapat menggunakan konsol serial untuk pemecahan masalah. Untuk informasi selengkapnya, lihat Mengonfigurasi akses ke Konsol EC2 Serial di Panduan EC2 Pengguna Amazon.

Bersihkan

Ikuti langkah-langkah ini untuk menghapus AWS sumber daya yang dibuat.

Hapus host dan lingkungan Amazon EVS

Ikuti langkah-langkah ini untuk menghapus host dan lingkungan Amazon EVS. Tindakan ini menghapus instalasi VMware VCF yang berjalan di lingkungan Amazon EVS Anda.

> **Note**
>
> Untuk menghapus lingkungan Amazon EVS, Anda harus menghapus semua host di lingkungan terlebih dahulu. Lingkungan tidak dapat dihapus jika ada host yang terkait dengan lingkungan.

Example

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Di panel navigasi, pilih Lingkungan.
3. Pilih lingkungan yang berisi host untuk dihapus.
4. Pilih tab Hosts.
5. Pilih host dan pilih Hapus dalam tab Hosts. Ulangi langkah ini untuk setiap host di lingkungan.
6. Di bagian atas halaman Lingkungan, pilih Hapus dan kemudian Hapus lingkungan.

> **Note**
>
> Penghapusan lingkungan juga menghapus subnet Amazon EVS VLAN dan AWS rahasia Secrets Manager yang dibuat Amazon EVS. AWS sumber daya yang Anda buat tidak dihapus. Sumber daya ini dapat terus mengeluarkan biaya.

7. Jika Anda memiliki Reservasi EC2 Kapasitas Amazon di tempat yang tidak lagi Anda perlukan, pastikan Anda telah membatalkannya. Untuk informasi selengkapnya, lihat Membatalkan Reservasi Kapasitas di Panduan EC2 Pengguna Amazon.

AWS CLI

1. Buka sesi terminal.
2. Identifikasi lingkungan yang berisi host untuk dihapus.

```
aws evs list-environments
```

Berikut ini adalah contoh respon.

```
{
    "environmentSummaries": [
        {
            "environmentId": "env-abcde12345",
            "environmentName": "testEnv",
            "vcfVersion": "VCF-5.2.2",
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T14:42:41.430000+00:00",
            "modifiedAt": "2025-04-13T14:43:33.412000+00:00",
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345"
        },
        {
            "environmentId": "env-edcba54321",
            "environmentName": "testEnv2",
            "vcfVersion": "VCF-5.2.2",
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T13:39:49.546000+00:00",
            "modifiedAt": "2025-04-13T13:52:13.342000+00:00",
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
edcba54321"
        }
    ]
}
```

3. Hapus host dari lingkungan. Di bawah ini adalah contoh `aws evs delete-environment-host` permintaan.

> **Note**
>
> Untuk dapat menghapus lingkungan, Anda harus terlebih dahulu menghapus semua host yang ada di lingkungan.

```
aws evs delete-environment-host \
--environment-id env-abcde12345 \
--host esx01
```

4. Ulangi langkah sebelumnya untuk menghapus host yang tersisa di lingkungan Anda.
5. Hapus lingkungan.

```
aws evs delete-environment --environment-id env-abcde12345
```

> **Note**
>
> Penghapusan lingkungan juga menghapus subnet Amazon EVS VLAN dan AWS rahasia Secrets Manager yang dibuat Amazon EVS. AWS Sumber daya lain yang Anda buat tidak dihapus. Sumber daya ini dapat terus mengeluarkan biaya.

6. Jika Anda memiliki Reservasi EC2 Kapasitas Amazon di tempat yang tidak lagi Anda perlukan, pastikan Anda telah membatalkannya. Untuk informasi selengkapnya, lihat Membatalkan Reservasi Kapasitas di Panduan EC2 Pengguna Amazon.

Hapus sumber daya IPAM (Untuk konektivitas internet HCX)

Jika Anda telah mengonfigurasi konektivitas internet HCX, ikuti langkah-langkah berikut untuk menghapus sumber daya IPAM Anda.

1. Melepaskan alokasi EIP dari kolam IPAM publik. Untuk informasi selengkapnya, lihat Melepaskan alokasi di Panduan Pengguna Manajer Alamat IP VPC.
2. Pembatalan IPv4 CIDR publik dari kolam IPAM. Untuk informasi selengkapnya, lihat Pembatalan CIDRs dari kumpulan di Panduan Pengguna Manajer Alamat IP VPC.
3. Hapus kolam IPAM publik. Untuk informasi selengkapnya, lihat Menghapus kumpulan di Panduan Pengguna Pengelola Alamat IP VPC.

4. Hapus IPAM. Untuk informasi selengkapnya, lihat Menghapus IPAM di Panduan Pengguna Manajer Alamat IP VPC.

Hapus komponen VPC Route Server

Untuk langkah-langkah menghapus komponen Amazon VPC Route Server yang Anda buat, lihat Pembersihan Server Rute di Panduan Pengguna Amazon VPC.

Hapus daftar kontrol akses jaringan (ACL)

Untuk langkah-langkah menghapus daftar kontrol akses jaringan, lihat Menghapus ACL jaringan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Putuskan dan hapus tabel rute subnet

Untuk langkah-langkah untuk memisahkan dan menghapus tabel rute subnet, lihat Tabel rute subnet di Panduan Pengguna Amazon VPC.

Hapus subnet

Hapus subnet VPC, termasuk subnet akses layanan. Untuk langkah-langkah menghapus subnet VPC, lihat Menghapus subnet di Panduan Pengguna Amazon VPC.

> **Note**
>
> Jika Anda menggunakan Route 53 untuk DNS, hapus titik akhir masuk sebelum Anda mencoba menghapus subnet akses layanan. Jika tidak, Anda tidak akan dapat menghapus subnet akses layanan.

> **Note**
>
> Amazon EVS menghapus subnet VLAN atas nama Anda saat lingkungan dihapus. Subnet Amazon EVS VLAN hanya dapat dihapus ketika lingkungan dihapus.

Hapus VPC

Untuk langkah-langkah menghapus VPC, lihat Menghapus VPC Anda di Panduan Pengguna Amazon VPC.

Langkah selanjutnya

Migrasikan beban kerja Anda ke Amazon EVS menggunakan VMware Hybrid Cloud Extension (VMware HCX). Lihat informasi yang lebih lengkap di Migrasi.

Migrasikan beban kerja ke Amazon EVS menggunakan HCX VMware

Setelah Amazon EVS diterapkan, Anda dapat menerapkan VMware HCX dengan konektivitas internet pribadi atau publik untuk memfasilitasi migrasi beban kerja ke Amazon EVS. Untuk informasi selengkapnya, lihat Memulai VMware HCX di Panduan Pengguna VMware HCX.

Important

Migrasi berbasis internet HCX umumnya tidak disarankan untuk:

- Aplikasi sensitif terhadap jitter jaringan atau latensi.
- Operasi vMotion kritis waktu.
- Migrasi skala besar dengan persyaratan kinerja yang ketat.

Untuk skenario ini, kami sarankan menggunakan konektivitas pribadi HCX. Koneksi khusus pribadi menawarkan kinerja yang lebih andal dibandingkan dengan koneksi berbasis internet.

Opsi konektivitas HCX

Anda dapat memigrasikan beban kerja ke Amazon EVS menggunakan konektivitas pribadi dengan koneksi Direct AWS Connect atau Site-to-Site VPN, atau menggunakan konektivitas publik.

Tergantung pada situasi dan opsi konektivitas Anda, Anda mungkin lebih suka menggunakan konektivitas publik atau pribadi dengan HCX. Misalnya, beberapa situs mungkin memiliki konektivitas pribadi dengan konsistensi kinerja yang lebih besar, tetapi throughput yang lebih rendah karena enkripsi VPN atau kecepatan tautan terbatas. Demikian juga, Anda mungkin memiliki konektivitas internet publik throughput tinggi yang memiliki lebih banyak variasi dalam kinerja. Dengan Amazon EVS, Anda memiliki pilihan untuk menggunakan opsi konektivitas mana pun yang paling cocok untuk Anda.

Tabel berikut membandingkan perbedaan antara konektivitas pribadi dan publik HCX.

Konektivitas pribadi	Konektivitas publik
Ikhtisar	Ikhtisar
Hanya menggunakan koneksi pribadi dalam VPC. Anda dapat secara opsional menggunakan AWS Direct Connect atau Site-to-Site VPN dengan gateway transit untuk konektivitas jaringan eksternal.	Menggunakan konektivitas internet publik dengan alamat IP Elastic, memungkinkan migrasi tanpa koneksi pribadi khusus.
Paling cocok untuk	Paling cocok untuk
• Operasi vMotion yang sensitif terhadap waktu. • Migrasi skala besar. • Aplikasi sensitif terhadap latensi/jitter. • Transfer data volume tinggi. • Organizations dengan AWS Direct Connect/VPN AWS Site-to-Site yang sudah ada.	• Lokasi tanpa AWS Koneksi Langsung/VPN AWS Site-to-Site . • Proyek yang sensitif terhadap biaya.
Manfaat utama	Manfaat utama
• Konektivitas latensi rendah yang konsisten. • Alokasi bandwidth khusus. • Kinerja jaringan yang lebih andal. • Enkripsi HCX default dapat dinonaktifkan untuk lingkungan pribadi untuk mengoptimalkan kinerja. • Tidak diperlukan manajemen IP publik.	• Pengaturan lebih cepat daripada konektivitas pribadi. • Hemat biaya untuk migrasi yang lebih kecil.
Pertimbangan utama	Pertimbangan utama
• Pengaturan awal yang lebih kompleks. • Biaya infrastruktur di muka yang lebih tinggi. • Garis waktu implementasi yang lebih lama.	• Kinerja jaringan yang lebih bervariasi. • Keterbatasan bandwidth dimungkinkan. • Latensi lebih tinggi dari konektivitas pribadi.

Konektivitas pribadi	Konektivitas publik
• Tidak ada konektivitas internet langsung untuk komponen HCX apa pun.	• Setiap komponen memerlukan alamat IP Elastis khusus yang dialokasikan dari kolam IPAM publik. • Asosiasi EIP memungkinkan konektivitas internet langsung untuk setiap komponen HCX.

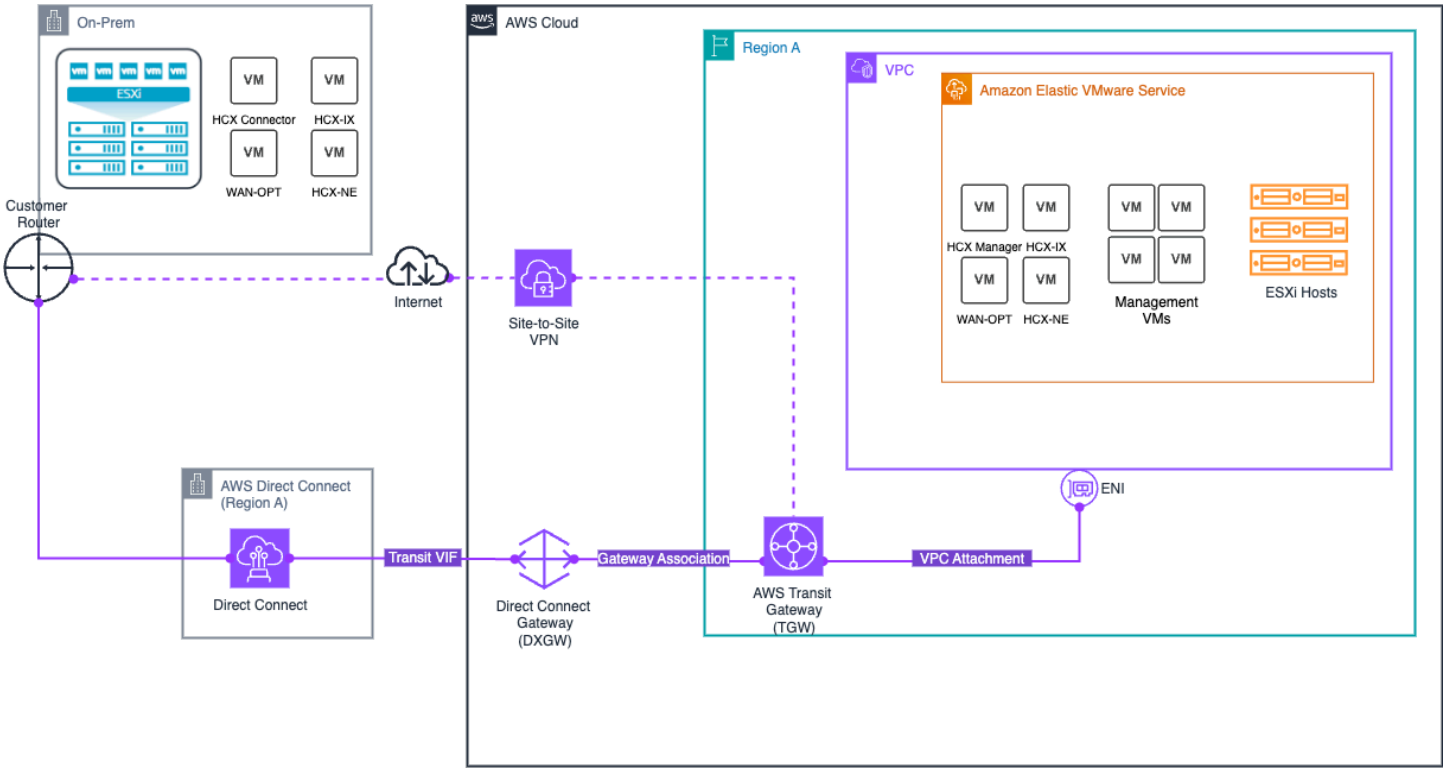
Arsitektur konektivitas pribadi HCX

Solusi konektivitas pribadi HCX mengintegrasikan beberapa komponen:

- Komponen jaringan Amazon EVS
  - Hanya menggunakan subnet VLAN pribadi untuk komunikasi yang aman, termasuk VLAN HCX pribadi.
  - Mendukung jaringan ACLs untuk kontrol lalu lintas.
  - Mendukung propagasi rute BGP dinamis melalui server rute VPC pribadi.
- AWS opsi transit jaringan terkelola untuk konektivitas lokal
  - AWS Direct Connect + AWS Transit Gateway memungkinkan Anda menghubungkan jaringan lokal ke Amazon EVS melalui koneksi khusus pribadi. Untuk informasi selengkapnya, lihat AWS Direct Connect + AWS Transit Gateway.
  - AWS Site-to-Site VPN + AWS Transit Gateway menyediakan opsi untuk membuat koneksi IPsec VPN antara jaringan jarak jauh Anda dan gateway transit melalui internet. Untuk informasi selengkapnya, lihat AWS Transit Gateway + AWS Site-to-Site VPN.

> **Note**
>
> Amazon EVS tidak mendukung konektivitas melalui antarmuka virtual pribadi AWS Direct Connect (VIF), atau melalui koneksi AWS Site-to-Site VPN yang berakhir langsung ke VPC underlay.

Diagram berikut menggambarkan arsitektur konektivitas pribadi HCX, menunjukkan bagaimana Anda dapat menggunakan Direct AWS Connect dan Site-to-Site VPN dengan gateway transit untuk mengaktifkan migrasi beban kerja yang aman melalui koneksi khusus pribadi.



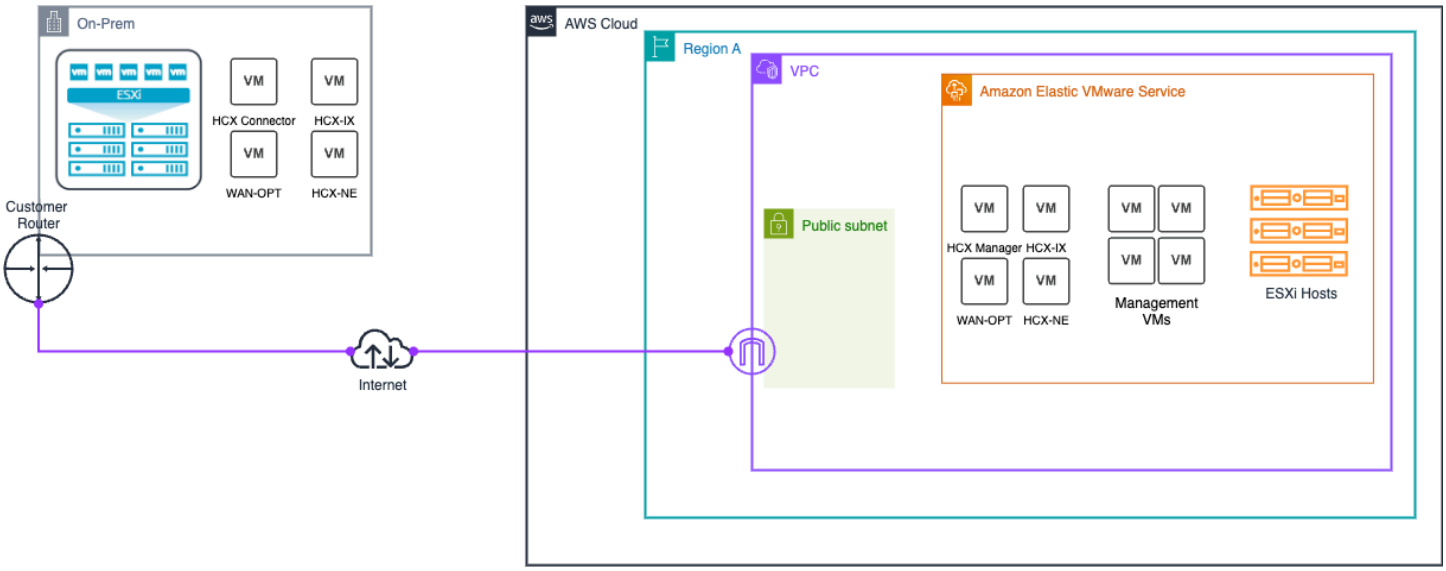
Arsitektur konektivitas internet HCX

Solusi konektivitas internet HCX terdiri dari beberapa komponen yang bekerja sama:

- Komponen jaringan Amazon EVS
  - Menggunakan subnet VLAN HCX publik yang terisolasi untuk mengaktifkan konektivitas internet antara Amazon EVS dan peralatan HCX lokal Anda.
  - Mendukung jaringan ACLs untuk kontrol lalu lintas.
  - Mendukung propagasi rute BGP dinamis melalui server rute VPC publik.
- IPAM dan manajemen IP publik
  - Amazon VPC IP Address Manager (IPAM) mengelola alokasi IPv4 alamat publik dari kolam IPAM publik milik Amazon.
  - Blok CIDR VPC sekunder (/28) dialokasikan dari kolam IPAM, menciptakan subnet publik terisolasi yang terpisah dari CIDR VPC utama.

Untuk informasi selengkapnya, lihat the section called “Konektivitas publik HCX”.

Diagram berikut menggambarkan arsitektur konektivitas internet HCX.



Pengaturan migrasi HCX

Tutorial ini menjelaskan cara mengonfigurasi VMware HCX untuk memigrasikan beban kerja Anda ke Amazon EVS.

Prasyarat

Sebelum menggunakan VMware HCX dengan Amazon EVS, pastikan bahwa prasyarat HCX telah terpenuhi. Untuk informasi selengkapnya, lihat the section called “VMware Prasyarat HCX”.

> **Important**
>
> Amazon EVS memiliki persyaratan unik untuk konektivitas internet publik HCX.
> Jika Anda membutuhkan konektivitas publik HCX, Anda harus memenuhi persyaratan berikut:
>
> - Buat IPAM dan kolam IPv4 IPAM publik dengan CIDR yang memiliki panjang netmask minimal /28.
> - Alokasikan setidaknya dua alamat IP Elastis (EIPs) dari kolam IPAM untuk peralatan HCX Manager dan HCX Interconnect (HCX-IX). Alokasikan alamat IP Elastis tambahan untuk setiap alat jaringan HCX yang perlu Anda gunakan.
> - Tambahkan blok IPv4 CIDR publik sebagai CIDR tambahan ke VPC Anda.

Untuk informasi selengkapnya, lihat the section called “Pengaturan konektivitas internet HCX”.

Periksa status subnet HCX VLAN

VLAN dibuat untuk HCX sebagai bagian dari penerapan EVS Amazon standar. Ikuti langkah-langkah ini untuk memeriksa apakah subnet HCX VLAN dikonfigurasi dengan benar.

Example

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Pada panel navigasi, pilih Lingkungan.
3. Pilih lingkungan Amazon EVS.
4. Pilih tab Jaringan dan konektivitas.
5. Di bawah VLANs, identifikasi VLAN HCX dan periksa apakah Negara Dibuat dan Publik benar.

AWS CLI

1. Jalankan perintah berikut, menggunakan ID lingkungan untuk lingkungan Anda dan nama Wilayah yang berisi sumber daya Anda.

```
aws evs list-environment-vlans  --region <region-name> --environment-id env-
abcde12345
```

2. Dalam output respons, identifikasi VLAN dengan `functionName` dari `hcx` dan periksa apakah `vlanState` sudah `CREATED` dan `isPublic` disetel `ketrue`. Berikut ini adalah contoh respon.

```
{
    "environmentVlans": [{
            "vlanId": 50,
            "cidr": "10.10.4.0/24",
            "availabilityZone": "us-east-2b",
            "functionName": "vTep",
            "subnetId": "subnet-0ce640ac79e7f4dbc",
```

```
            "createdAt": "2025-09-09T12:09:37.526000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.596000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [],
            "isPublic": false
        },
        {
            "vlanId": 80,
            "cidr": "18.97.141.240/28",
            "availabilityZone": "us-east-2b",
            "functionName": "hcx",
            "subnetId": "subnet-0f080c94782cc74b4",
            "createdAt": "2025-09-09T12:09:37.675000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.359000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [{
                    "assocationId": "eipassoc-0be981accbbdf443a",
                    "allocationId": "eipalloc-0cef80396f4a0cc24",
                    "ipAddress": "18.97.141.245"
                },
                {
                    "assocationId": "eipassoc-0d5572f66b7952e9d",
                    "allocationId": "eipalloc-003fc9807d35d1ad3",
                    "ipAddress": "18.97.141.244"
                }
            ],
            "isPublic": true
        }
    ]
}
```


Periksa apakah subnet HCX VLAN dikaitkan dengan ACL jaringan

Ikuti langkah-langkah ini untuk memeriksa apakah subnet HCX VLAN dikaitkan dengan ACL jaringan. Untuk informasi selengkapnya tentang asosiasi ACL jaringan, lihatthe section called “Buat ACL jaringan untuk mengontrol lalu lintas subnet Amazon EVS VLAN”.

> **Important**
>
> Jika Anda terhubung melalui internet, mengaitkan alamat IP Elastis dengan VLAN menyediakan akses internet langsung ke semua sumber daya di VLAN itu. Pastikan Anda memiliki daftar kontrol akses jaringan yang sesuai yang dikonfigurasi untuk membatasi akses sesuai kebutuhan untuk persyaratan keamanan Anda.

> **Important**
>
> EC2 grup keamanan tidak berfungsi pada antarmuka jaringan elastis yang dilampirkan ke subnet Amazon EVS VLAN. Untuk mengontrol lalu lintas ke dan dari subnet Amazon EVS VLAN, Anda harus menggunakan daftar kontrol akses jaringan (ACL).

Example

Amazon VPC console

1. Pergi ke Amazon VPC konsol.
2. Di panel navigasi, pilih Jaringan ACLs.
3. Pilih ACL jaringan yang terkait dengan subnet VLAN Anda.
4. Pilih tab Asosiasi Subnet.
5. Periksa apakah subnet HCX VLAN terdaftar di antara subnet terkait.

AWS CLI

1. Jalankan perintah berikut, menggunakan ID subnet HCX VLAN di filter. `Values`

```
aws ec2 describe-network-acls --filters "Name=subnet-id,Values=subnet-
abcdefg9876543210"
```

2. Periksa apakah ACL jaringan yang benar dikembalikan dalam respons.

Periksa apakah subnet EVS VLAN secara eksplisit terkait dengan tabel rute

Amazon EVS mengharuskan semua subnet EVS VLAN secara eksplisit dikaitkan dengan tabel rute di VPC Anda. Untuk konektivitas internet HCX, subnet VLAN publik HCX Anda harus secara eksplisit dikaitkan dengan tabel rute publik di VPC Anda yang merutekan ke gateway internet. Ikuti langkah-langkah ini untuk memeriksa asosiasi tabel rute eksplisit.

Example

Amazon VPC console

1. Pergi ke konsol VPC.
2. Di panel navigasi, pilih Tabel rute.
3. Pilih tabel rute yang harus dikaitkan dengan subnet EVS VLAN Anda secara eksplisit.
4. Pilih tab Asosiasi Subnet.
5. Di bawah Asosiasi subnet eksplisit, periksa apakah semua subnet EVS VLAN terdaftar. Jika subnet VLAN tidak tercantum di sini, subnet VLAN secara implisit terkait dengan tabel rute utama. Agar Amazon EVS berfungsi dengan baik, Anda harus secara eksplisit mengaitkan semua subnet VLAN dengan tabel rute. Untuk subnet VLAN publik HCX, Anda harus memiliki tabel rute publik terkait dengan gateway internet sebagai target. Untuk mengatasi masalah ini, pilih Edit asosiasi subnet dan tambahkan subnet VLAN yang hilang.

AWS CLI

1. Buka sesi terminal.
2. Jalankan perintah contoh berikut untuk mengambil detail tentang semua subnet EVS VLAN Anda, termasuk asosiasi tabel rute. Jika subnet VLAN tidak tercantum di sini, subnet VLAN secara implisit terkait dengan tabel rute utama. Agar Amazon EVS berfungsi dengan baik, Anda harus secara eksplisit mengaitkan semua subnet VLAN dengan tabel rute. Untuk subnet VLAN publik HCX, Anda harus memiliki tabel rute publik terkait dengan gateway internet sebagai target.

```
aws ec2 describe-subnets
```

3. Hubungkan subnet EVS VLAN Anda secara eksplisit dengan tabel rute di VPC Anda. Di bawah ini adalah contoh perintah.

```
aws ec2 associate-route-table \
--route-table-id rtb-0123456789abcdef0 \
--subnet-id subnet-01234a1b2cde1234f
```

(Untuk konektivitas internet HCX) Periksa yang terkait dengan EIPs subnet HCX VLAN

Untuk setiap perangkat jaringan HCX yang Anda gunakan, Anda harus memiliki EIP dari kolam IPAM yang terkait dengan subnet VLAN publik HCX. Anda diharuskan untuk mengaitkan setidaknya dua EIPs dengan subnet VLAN publik HCX untuk peralatan HCX Manager dan HCX Interconnect (HCX-IX). Ikuti langkah-langkah ini untuk memeriksa apakah asosiasi EIP yang diperlukan ada.

Important

Konektivitas internet publik HCX gagal jika Anda tidak mengaitkan setidaknya dua EIPs dari kolam IPAM dengan subnet VLAN publik HCX.

Note

Anda tidak dapat mengaitkan dua EIP pertama EIPs atau terakhir dari blok CIDR IPAM publik dengan subnet VLAN. Ini EIPs dicadangkan sebagai jaringan, gateway default, dan alamat siaran. Amazon EVS memunculkan kesalahan validasi jika Anda mencoba mengaitkannya EIPs dengan subnet VLAN.

Example

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Pada menu navigasi, pilih Lingkungan.
3. Pilih lingkungan.
4. Di bawah tab Jaringan dan konektivitas, pilih VLAN publik HCX.
5. Periksa tab asosiasi EIP untuk mengonfirmasi bahwa EIPs telah dikaitkan dengan VLAN publik HCX.

AWS CLI

1. Untuk memeriksa mana EIPs yang terkait dengan subnet HCX VLAN, gunakan perintah. `list-environment-vlans` Untuk`environment-id`, gunakan ID unik untuk lingkungan EVS yang berisi HCX VLAN.

```
aws evs list-environment-vlans \
  --environment-id "env-605uove256" \
```

Perintah mengembalikan detail tentang Anda VLANs, termasuk asosiasi EIP:

```
{
  "environmentVlans": [
    {
      "vlanId": 80,
      "cidr": "18.97.137.0/28",
      "availabilityZone": "us-east-2c",
      "functionName": "hcx",
      "subnetId": "subnet-02f9a4ee9e1208cfc",
      "createdAt": "2025-08-26T22:15:00.200000+00:00",
      "modifiedAt": "2025-08-26T22:20:28.155000+00:00",
      "vlanState": "CREATED",
      "stateDetails": "VLAN successfully created",
      "eipAssociations": [
        {
          "associationId": "eipassoc-09876543210abcdef",
          "allocationId": "eipalloc-0123456789abcdef0",
          "ipAddress": "18.97.137.3"
        },
        {
          "associationId": "eipassoc-12345678901abcdef",
          "allocationId": "eipalloc-1234567890abcdef1",
          "ipAddress": "18.97.137.4"
        },
        {
          "associationId": "eipassoc-23456789012abcdef",
          "allocationId": "eipalloc-2345678901abcdef2",
          "ipAddress": "18.97.137.5"
        }
      ],
      "isPublic": true,
      "networkAclId": "acl-0123456789abcdef0"
```

```
    },
    ...
  ]
}
```

`eipAssociations`Array menunjukkan asosiasi EIP, termasuk:

- `associationId`- ID unik untuk asosiasi EIP ini.
- `allocationId`- ID alokasi alamat IP Elastis terkait.
- `ipAddress`- Alamat IP yang ditetapkan ke VLAN.

Buat grup port terdistribusi dengan ID VLAN uplink publik HCX

Pergi ke antarmuka Klien vSphere dan ikuti langkah-langkah dalam Tambahkan Grup Port Terdistribusi untuk menambahkan grup port terdistribusi ke Switch Terdistribusi vSphere.

Saat mengkonfigurasi failback dalam antarmuka Klien vSphere, pastikan bahwa uplink1 adalah uplink aktif dan uplink2 adalah uplink siaga untuk mengaktifkan failover. Active/Standby Untuk pengaturan VLAN di antarmuka Klien vSphere, masukkan ID VLAN HCX yang sebelumnya Anda identifikasi.

(Opsional) Mengatur Optimasi HCX WAN

> **Note**
>
> Fitur optimasi WAN tidak lagi tersedia di HCX 4.11.3. Untuk informasi selengkapnya, lihat Catatan Rilis HCX 4.11.3.

Layanan HCX WAN Optimization (HCX-WO) meningkatkan karakteristik kinerja jalur pribadi atau jalur internet dengan menerapkan teknik optimasi WAN seperti pengurangan data dan pengkondisian jalur WAN. Layanan Optimasi WAN HCX direkomendasikan pada penerapan yang tidak dapat mendedikasikan jalur 10Gbit untuk migrasi. Dalam 10Gbit, penerapan latensi rendah, menggunakan Optimasi WAN mungkin tidak menghasilkan peningkatan kinerja migrasi. Untuk informasi selengkapnya, lihat VMware Pertimbangan Penerapan HCX dan Praktik Terbaik.

Layanan HCX WAN Optimization digunakan bersama dengan HCX WAN Interconnect service appliance (HCX-IX). HCX-IX bertanggung jawab atas replikasi data antara lingkungan perusahaan dan lingkungan Amazon EVS.

Untuk menggunakan layanan HCX WAN Optimization dengan Amazon EVS, Anda perlu menggunakan grup port terdistribusi pada subnet HCX VLAN. Gunakan grup port terdistribusi yang dibuat pada langkah sebelumnya.

(Opsional) Aktifkan Jaringan yang Dioptimalkan Mobilitas HCX

HCX Mobility Optimized Networking (MON) adalah fitur dari Layanan Ekstensi Jaringan HCX. Ekstensi jaringan berkemampuan MON-enabled meningkatkan arus lalu lintas untuk mesin virtual yang dimigrasi dengan mengaktifkan perutean selektif dalam lingkungan Amazon EVS Anda. MON memungkinkan Anda mengonfigurasi jalur optimal untuk memigrasikan lalu lintas beban kerja ke Amazon EVS saat meregangkan jaringan Layer 2, menghindari jalur jaringan pulang-pergi yang panjang melalui gateway sumber. Fitur ini tersedia untuk semua penerapan Amazon EVS. Untuk informasi selengkapnya, lihat Mengonfigurasi Jaringan yang Dioptimalkan Mobilitas di Panduan VMware Pengguna HCX.

> **Important**
>
> Sebelum Anda mengaktifkan HCX MON, baca batasan berikut dan konfigurasi yang tidak didukung untuk Ekstensi Jaringan HCX.
> Pembatasan dan Batasan untuk Ekstensi Jaringan
> Pembatasan dan Batasan untuk Topologi Jaringan yang Dioptimalkan Mobilitas

> **Important**
>
> Sebelum Anda mengaktifkan HCX MON, pastikan bahwa di antarmuka NSX Anda telah mengonfigurasi redistribusi rute untuk CIDR jaringan tujuan. Untuk informasi selengkapnya, lihat Mengkonfigurasi BGP dan Redistribusi Rute dalam dokumentasi NSX. VMware

Verifikasi konektivitas HCX

VMware HCX mencakup alat diagnostik bawaan yang dapat digunakan untuk menguji konektivitas. Untuk informasi selengkapnya, lihat Pemecahan Masalah VMware HCX di Panduan Pengguna HCX. VMware

Konfigurasikan konektivitas internet publik HCX

Anda dapat mengonfigurasi akses internet publik untuk VLAN publik HCX Anda dengan mengaitkan alamat IP Elastis dengan VLAN Anda. Hal ini memungkinkan konektivitas internet langsung untuk peralatan VMware HCX dan beban kerja yang memerlukan akses internet untuk operasi migrasi.

Topik terkait

Topik ini mencakup pengelolaan akses internet untuk VLAN publik HCX. Untuk implementasi lengkap:

1. Prasyarat lengkap di. Menyiapkan VMware Layanan Elastis Amazon
2. Konfigurasikan pengaturan awal diMulai menggunakan.
3. Konfigurasikan akses internet (topik ini).

Tentang akses internet HCX VLAN

Anda dapat mengonfigurasi akses internet untuk peralatan VMware HCX, memungkinkan Anda melakukan migrasi HCX dari beban kerja Anda ke Amazon EVS melalui internet.

Pendekatan ini:

- Mengaktifkan migrasi mesin virtual tanpa memerlukan konektivitas pribadi khusus.
- Menyediakan solusi yang fleksibel dan hemat biaya untuk migrasi.

Important

Migrasi berbasis internet HCX umumnya tidak disarankan untuk:

- Aplikasi sensitif terhadap jitter jaringan atau latensi.
- Operasi vMotion kritis waktu.
- Migrasi skala besar dengan persyaratan kinerja yang ketat.

Untuk skenario ini, kami sarankan menggunakan konektivitas pribadi HCX. Koneksi khusus pribadi menawarkan kinerja yang lebih andal dibandingkan dengan koneksi berbasis internet.

Ikhtisar konektivitas internet

Tinjau pertimbangan berikut.

Persyaratan jaringan HCX dan DNAT

HCX memiliki kendala jaringan khusus yang memengaruhi cara Anda mengatur akses internet publik.

HCX tidak mendukung Terjemahan Alamat Jaringan Tujuan (DNAT). Sebagai gantinya, HCX membutuhkan jaringan uplink agar dapat dirutekan dengan alamat IP gateway default.

Subnet Amazon EVS VLAN menyertakan alamat IP gateway default seperti subnet VPC lainnya. Namun, subnet ini selalu subnet pribadi, bahkan ketika Anda menggunakan blok CIDR di luar rentang alamat. RFC1918

Mengaktifkan konektivitas internet HCX

Untuk mengaktifkan konektivitas internet tanpa DNAT, Amazon EVS menggunakan pendekatan konfigurasi CIDR tertentu:

- Persyaratan CIDR yang dapat dirutekan Internet: Amazon EVS memerlukan CIDR yang dapat dirutekan internet yang cocok dengan subnet CIDR HCX VLAN Anda.
- Alokasi IPAM: Amazon EVS menggunakan CIDR yang dialokasikan IPAM publik dengan panjang netmask minimum /28 sebagai CIDR yang dapat dirutekan internet.
- Konfigurasi VPC: Anda harus menambahkan CIDR yang dialokasikan IPAM publik secara manual ke VPC Anda sebagai CIDR VPC sekunder.
- Penyebaran subnet VLAN: Setelah IPAM dan VPC dikonfigurasi, Anda dapat menggunakan CIDR yang dialokasikan IPAM publik di subnet HCX VLAN selama penyebaran Amazon EVS.
- Konfigurasi IP elastis: Amazon EVS memerlukan konfigurasi berikut:
  - Alokasikan elastis IPs: Anda mengalokasikan elastis IPs dari CIDR yang dialokasikan IPAM. Anda harus mengalokasikan setidaknya dua alamat IP Elastis (EIPs) dari kolam IPAM untuk peralatan HCX Manager dan HCX Interconnect (HCX-IX). Alokasikan alamat IP Elastis tambahan untuk setiap perangkat jaringan HCX yang perlu Anda gunakan.
  - Kaitkan dengan VLAN: Anda mengaitkan setiap IP Elastis yang ingin Anda gunakan dengan alat HCX ke subnet HCX VLAN. Gunakan konsol Amazon EVS atau AWS CLI untuk asosiasi ini.
  - Konfigurasikan alamat gateway: Alamat pertama yang dapat digunakan dari CIDR menjadi alamat gateway yang Anda konfigurasikan di alat HCX Anda.

- Perutean lalu lintas: Lalu lintas untuk setiap rute IP Elastis terkait langsung ke alat HCX tujuan dengan alamat IP yang sama, tanpa DNAT.

Untuk langkah-langkah mengonfigurasi HCX dengan konektivitas internet untuk penyebaran lingkungan Amazon EVS, lihat dan. Menyiapkan VMware Layanan Elastis Amazon Mulai menggunakan

Pertimbangan operasi

- Blok CIDR VLAN publik HCX harus memiliki panjang netmask /28.
- EIPs dapat dikaitkan dengan atau dipisahkan dari VLAN publik HCX setelah penerapan menggunakan konsol Amazon EVS AWS CLI atau, tetapi mereka harus dari kumpulan IPAM yang sama.
- Setiap asosiasi EIP memiliki ID asosiasi uniknya sendiri.
- Anda dapat memiliki hingga 13 EIPs dari kolam IPAM publik yang terkait dengan/28 HCX VLAN publik. Anda tidak dapat mengaitkan dua EIP pertama EIPs atau terakhir dari blok CIDR yang dialokasikan IPAM publik dengan subnet VLAN publik HCX. Ini EIPs dicadangkan sebagai jaringan, gateway default, dan alamat siaran. Amazon EVS memunculkan kesalahan validasi jika Anda mencoba mengaitkannya EIPs dengan VLAN.

Pertimbangan keamanan

- Daftar kontrol akses jaringan (ACLs) masih berlaku untuk lalu lintas yang mengalir melalui subnet VLAN publik HCX.
- Aturan grup keamanan tidak berlaku untuk lalu lintas pada subnet VLAN publik HCX. Gunakan jaringan ACLs untuk kontrol lalu lintas.

Important

Jika Anda terhubung melalui internet, mengaitkan alamat IP Elastis dengan VLAN menyediakan akses internet langsung ke semua sumber daya di VLAN itu. Pastikan Anda memiliki daftar kontrol akses jaringan yang sesuai yang dikonfigurasi untuk membatasi akses sesuai kebutuhan untuk persyaratan keamanan Anda.

Mengelola alamat IP Elastis untuk VLANs

Anda dapat mengaitkan dan memisahkan alamat IP Elastis dengan VLAN publik HCX menggunakan konsol Amazon EVS atau. AWS CLI

> **Note**
>
> Amazon EVS hanya mendukung asosiasi dan pemutusan alamat IP Elastis dengan VLAN publik HCX saat ini.

Kaitkan alamat IP Elastis dengan VLAN

Prasyarat

Pastikan Anda memiliki yang berikut:

- Alamat IP elastis dialokasikan dari kolam IPAM publik milik Amazon.
- Lingkungan Amazon EVS sudah dibuat.

Example

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Pada menu navigasi, pilih Lingkungan.
3. Pilih lingkungan.
4. Di bawah tab Jaringan dan konektivitas, pilih VLAN publik HCX.

   > **Note**
   >
   > Amazon EVS hanya mendukung asosiasi EIPs dengan HCX VLAN saat ini.

5. Pilih Associate EIP ke VLAN.
6. Pilih alamat IP Elastis untuk dikaitkan dengan VLAN publik HCX.
7. Pilih Kaitkan EIPs. Anda dapat memiliki hingga 13 EIPs yang terkait dengan VLAN publik HCX.

> **Note**
>
> Anda tidak dapat mengaitkan dua yang pertama EIPs dari blok CIDR IPAM publik ke subnet VLAN. Ini EIPs dicadangkan sebagai alamat jaringan dan gateway default.

8. Periksa asosiasi EIP untuk mengonfirmasi bahwa EIPs telah dikaitkan dengan VLAN publik HCX.

AWS CLI

1. Untuk mengaitkan alamat IP elastis dengan VLAN, gunakan `associate-eip-to-vlan` perintah contoh.
   - `environment-id`- ID lingkungan Amazon EVS Anda.
   - `vlan-name`- Pastihcx. Amazon EVS hanya mendukung asosiasi EIP dengan HCX VLAN saat ini.
   - `allocation-id`- ID alokasi alamat IP Elastis.

   ```
   aws evs associate-eip-to-vlan \
     --environment-id "env-605uove256" \
     --vlan-name "hcx" \
     --allocation-id "eipalloc-0429268f30c4a34f7"
   ```

   Perintah mengembalikan detail tentang VLAN, termasuk asosiasi EIP baru:

   ```
   {
       "vlan": {
           "vlanId": 80,
           "cidr": "18.97.137.0/28",
           "availabilityZone": "us-east-2c",
           "functionName": "hcx",
           "subnetId": "subnet-02f9a4ee9e1208cfc",
           "createdAt": "2025-08-22T23:42:16.200000+00:00",
           "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
           "vlanState": "CREATED",
           "stateDetails": "VLAN successfully created",
           "eipAssociations": [
               {
                   "associationId": "eipassoc-09e966faad7ecc58a",
   ```

```
                "allocationId": "eipalloc-0429268f30c4a34f7",
                "ipAddress": "18.97.137.2"
            }
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

`eipAssociations`Array menunjukkan asosiasi baru, termasuk:

- `associationId`- ID unik untuk asosiasi EIP ini, digunakan untuk disasosiasi.
- `allocationId`- ID alokasi alamat IP Elastis terkait.
- `ipAddress`- Alamat IP yang ditetapkan ke VLAN.

2. Ulangi langkah ini untuk mengaitkan tambahan EIPs. Anda dapat memiliki hingga 13 EIPs yang terkait dengan VLAN publik HCX.

Putuskan alamat IP Elastis dari VLAN

Prasyarat

Pastikan Anda memiliki yang berikut:

- Lingkungan Amazon EVS sudah dibuat.
- EIP dikaitkan dengan lingkungan Amazon EVS.

Example

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Pada menu navigasi, pilih Lingkungan.
3. Pilih lingkungan.
4. Di bawah tab Jaringan dan konektivitas, pilih VLAN publik HCX.
5. Pilih Disassociate EIP dari VLAN.
6. Pilih alamat IP Elastis untuk memisahkan diri dari VLAN publik HCX.

> **Important**
>
> Disasosiasi EIPs dapat menyebabkan hilangnya konektivitas internet untuk peralatan yang menggunakan subnet VLAN publik.

7. Pilih Pisahkan EIPs.
8. Periksa asosiasi EIP untuk mengonfirmasi bahwa EIPs telah dipisahkan dari VLAN publik HCX.

AWS CLI

Untuk memisahkan alamat IP Elastis dari VLAN, gunakan perintah contoh`disassociate-eip-from-vlan`.

- `environment-id`- ID lingkungan Amazon EVS Anda.
- `vlan-name`- Pastihcx. Amazon EVS hanya mendukung asosiasi EIP dengan HCX VLAN saat ini.
- `association-id`- ID asosiasi asosiasi EIP untuk dihapus.

> **Important**
>
> Disasosiasi EIPs dapat menyebabkan hilangnya konektivitas internet untuk peralatan yang menggunakan subnet VLAN publik.

```
aws evs disassociate-eip-from-vlan \
  --environment-id "env-605uove256" \
  --vlan-name "hcx" \
  --association-id "eipassoc-09e966faad7ecc58a"
```

Perintah mengembalikan detail tentang VLAN dengan asosiasi EIP dihapus:

```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
```

```
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:48:49.846000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

`eipAssociations`Array kosong mengonfirmasi bahwa alamat IP Elastis telah berhasil dipisahkan dari VLAN.

Tentang HCX WAN Optimization untuk migrasi berbasis internet

> **Note**
>
> Fitur optimasi WAN tidak lagi tersedia di HCX 4.11.3. Untuk informasi selengkapnya, lihat Catatan Rilis HCX 4.11.3.

Saat melakukan migrasi melalui internet, HCX WAN Optimization (HCX-WO) dapat meningkatkan kinerja migrasi. Layanan ini bekerja bersama dengan alat Interkoneksi HCX (HCX-IX) untuk:

- Terapkan teknik reduksi data untuk meminimalkan penggunaan bandwidth.
- Menerapkan pengkondisian jalur WAN untuk mengoptimalkan kinerja jaringan.
- Tingkatkan kecepatan migrasi melalui koneksi internet latensi tinggi.
- Meningkatkan keandalan migrasi berbasis internet.

HCX WAN Optimization sangat berguna untuk migrasi berbasis internet di mana:

- Latensi jaringan mungkin lebih tinggi daripada opsi konektivitas pribadi.
- Bandwidth yang tersedia mungkin terbatas atau variabel.
- Kondisi jaringan dapat berfluktuasi karena pola lalu lintas internet.

Untuk petunjuk terperinci tentang pengaturan HCX WAN Optimization setelah mengonfigurasi konektivitas internet, lihat. the section called “(Opsional) Mengatur Optimasi HCX WAN”

> **Note**
>
> Meskipun Optimasi WAN dapat secara signifikan meningkatkan kinerja migrasi berbasis internet, ini mungkin tidak memberikan manfaat tambahan di lingkungan dengan koneksi 10Gbit, latensi rendah khusus. Pertimbangkan karakteristik jaringan Anda saat memutuskan apakah akan mengaktifkan fitur ini.

Mengelola lingkungan Amazon EVS

Bab ini mencakup topik-topik berikut untuk membantu Anda mengelola lingkungan Anda.

- the section called “Langganan VCF”- Menjelaskan bagaimana langganan VCF bekerja dengan Amazon EVS dan tanggung jawab pelanggan untuk manajemen langganan VCF.
- the section called “Versi dan instance VCF EC2 ”- Menjelaskan versi VCF dan ESX yang didukung dan cara memeriksa ketersediaan versi di Amazon EVS.
- the section called “Manajemen siklus hidup”- Menjelaskan tanggung jawab manajemen siklus hidup dalam lingkungan Amazon EVS, termasuk manajemen infrastruktur yang mendasarinya, manajemen peningkatan VCF, manajemen lifecyle host ESX.
- the section called “Pemeliharaan lingkungan”- Menjelaskan cara melakukan tugas pemeliharaan umum untuk lingkungan Amazon EVS Anda, termasuk konfigurasi jaringan, pemeliharaan host ESX, memeriksa status lingkungan, dan mengelola jadwal rotasi rahasia untuk kredenal VCF Anda.
- the section called “Buat host”- Menjelaskan cara membuat host Amazon EVS setelah lingkungan diterapkan dan menambahkan host ke cluster.
- the section called “Hapus host”- Menjelaskan cara menghapus host Amazon EVS dan menghapusnya dari cluster.

Langganan VCF

> **Note**
>
> Amazon EVS tidak mendukung lisensi vSphere abadi. Anda harus memiliki langganan VMware Cloud Foundation yang valid dan aktif untuk menggunakan Amazon EVS.

Amazon EVS menggunakan langganan VMware Cloud Foundation (VCF) dengan hak portabilitas lisensi yang Anda bawa (BYOS). AWS Agar berhasil menerapkan lingkungan Amazon EVS, Anda harus memberikan kunci solusi VCF yang valid dan kunci lisensi vSAN dalam permintaan pembuatan lingkungan. Kunci lisensi vSphere berfungsi sebagai kunci solusi untuk VCF. Setiap kunci lisensi VCF hanya dapat digunakan untuk satu lingkungan Amazon EVS. Pembuatan lingkungan gagal jika Anda mencoba menggunakan kunci lisensi VCF yang sudah digunakan di lingkungan lain.

Kunci solusi VCF Anda harus memiliki setidaknya 256 core untuk menyediakan kapasitas inti yang memadai untuk empat host EC2 i4i.metal awal yang digunakan Amazon EVS saat pembuatan lingkungan. Setiap host i4i.metal membutuhkan 64 core. Kunci lisensi vSAN harus memiliki setidaknya 110 TiB kapasitas vSAN. Pembuatan lingkungan gagal jika Anda mencoba menggunakan kunci lisensi berukuran kecil.

> **Note**
>
> Langganan VCF Anda akan tersedia untuk Amazon EVS di semua AWS Wilayah untuk kepatuhan lisensi. Amazon EVS tidak memvalidasi kunci lisensi. Untuk memvalidasi kunci lisensi, kunjungi dukungan Broadcom.

> **Note**
>
> Informasi tentang perangkat lunak VCF Anda di Amazon EVS akan dibagikan dengan Broadcom untuk memverifikasi kepatuhan lisensi.

Manajemen berlangganan

Anda bertanggung jawab untuk mengelola langganan VCF Anda. Langganan VCF Anda harus dikelola di SDDC Manager. Menghapus kunci lisensi Anda dari SDDC Manager atau menggantinya dengan kunci lisensi yang sedang digunakan akan mengakibatkan pemeriksaan status lingkungan gagal, mencegah Anda menambahkan host ke lingkungan Amazon EVS Anda. Untuk informasi lebih lanjut tentang pemeriksaan status lingkungan, the section called “Pantau status lingkungan” danthe section called “Memecahkan masalah pemeriksaan status lingkungan yang gagal”. Untuk informasi selengkapnya tentang kunci lisensi VCF, lihat Mengelola Kunci Lisensi di VMware Cloud Foundation di dokumentasi VMware Cloud Foundation.

> **Important**
>
> Gunakan antarmuka pengguna SDDC Manager untuk mengelola solusi VCF dan kunci lisensi vSAN. Amazon EVS mengharuskan Anda mempertahankan solusi VCF yang valid dan kunci lisensi vSAN di SDDC Manager agar layanan berfungsi dengan baik. Meskipun kunci harus ditetapkan ke host dan kluster vSAN Anda menggunakan Klien vSphere, Anda harus

memastikan bahwa kunci tersebut juga muncul di layar lisensi antarmuka pengguna SDDC Manager.

Menambahkan kunci lisensi VCF

Di portal dukungan Broadcom, Anda dapat membeli kunci lisensi VCF tambahan, membagi kunci lisensi jika Anda sudah memiliki kunci besar, atau menggabungkan beberapa kunci lisensi. Ini memungkinkan Anda untuk melisensikan host yang Anda tambahkan ke lingkungan Anda setelah penerapan awal, atau melisensikan lingkungan tambahan. Pastikan bahwa kunci lisensi yang dibeli ditambahkan dalam inventaris vCenter Sever dan SDDC Manager. Jika menambahkan host, pastikan lisensi Anda ditetapkan ke host yang benar di vSphere dan memiliki core dan kapasitas penyimpanan vSAN yang memadai. Amazon EVS tidak mendukung host yang tidak berlisensi. Untuk informasi selengkapnya, lihat Mengonfigurasi Pengaturan Lisensi untuk Aset di Klien vSphere dalam VMware dokumentasi.

Kunci lisensi baru yang belum kedaluwarsa harus ditetapkan ke vCenter Server sebelum periode evaluasi kunci lisensi berakhir untuk tetap aktif. Kunci lisensi aktif diperlukan untuk berhasil menyiapkan lingkungan Amazon EVS. Lingkungan Anda akan gagal menerapkan jika kunci lisensi kedaluwarsa disediakan. Untuk informasi selengkapnya tentang pembuatan kunci lisensi VCF, lihat Membuat Lisensi Baru dalam dokumentasi. VMware Jika Anda mengalami masalah dengan kunci lisensi yang ditambahkan, lihatthe section called “Pemeriksaan cakupan kunci gagal”.

Menghapus kunci lisensi VCF

Anda dapat menghapus kunci lisensi VCF dari inventaris SDDC Manager untuk mengurangi kapasitas inti dan vSAN Anda setelah menghapus host di lingkungan Anda. Agar tetap mematuhi model lisensi produk yang Anda gunakan dengan vSphere, Anda harus menghapus semua kunci lisensi yang tidak ditetapkan dari inventaris. Jika Anda telah membagi, menggabungkan, atau mengupgrade kunci lisensi di Broadcom Support Portal, Anda harus menghapus kunci lisensi lama. Untuk informasi selengkapnya, lihat Menghapus lisensi dalam VMware dokumentasi.

Versi VCF dan jenis EC2 instans yang disediakan oleh Amazon EVS

Amazon EVS menyediakan beberapa versi VMware Cloud Foundation (VCF), ESX, dan jenis EC2 instans yang dapat Anda pilih saat membuat lingkungan dan membuat host.

Memeriksa versi VCF yang disediakan, versi ESX, dan jenis instans EC2

AWS Konsol menampilkan daftar versi VCF yang disediakan oleh Amazon EVS di wizard buat lingkungan. Versi ESX yang tersedia akan terlihat saat Anda memilih jenis instans sambil menambahkan host ke lingkungan yang ada. Anda juga dapat melihat versi VCF, versi ESX, dan jenis EC2 instance menggunakan CLI.

Example

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Pada menu navigasi, pilih Lingkungan.
3. Lakukan salah satu tindakan berikut:

   Untuk memeriksa versi VCF:

   a. Pilih Buat Lingkungan.

   b. Di bawah persyaratan Validasi Amazon EVS, pilih versi VCF Anda untuk melihat apakah status tersedia atau dibatasi untuk Anda.

   Untuk memeriksa versi ESX:

   a. Pilih lingkungan yang ada.

   b. Pilih Buat host.

   c. Pilih jenis instans untuk melihat versi ESX yang tersedia.

AWS CLI

Jalankan perintah berikut untuk mengambil informasi tentang versi VCF dan ESX:

```
aws evs get-versions --region <region-name>
```

Contoh respons:

```
{
   "instanceTypeEsxVersions": [
      {
         "esxVersions": [ "ESXi-8.0U3b-24280767","ESXi-8.0U3g-24859861" ],
```

```
            "instanceType": "i4i.metal"
         }
      ],
      "vcfVersions": [
         {
               "vcfVersion": "VCF-5.2.1",
               "status": "RESTRICTED",
               "defaultEsxVersion": "ESXi-8.0U3b-24280767",
               "instanceTypes": ["i4i.metal"]
         },
         {
               "vcfVersion": "VCF-5.2.2",
               "status": "AVAILABLE",
               "defaultEsxVersion": "ESXi-8.0U3g-24859861",
               "instanceTypes": ["i4i.metal"]
         }
      ]
}
```

> **Note**
>
> Jika versi yang Anda butuhkan menunjukkan`RESTRICTED`, dan Anda memiliki kebutuhan tertentu, lihat the section called “Meminta akses ke versi VCF terbatas” untuk informasi lebih lanjut tentang cara mendapatkan akses ke versi itu.

Versi VCF saat ini di Amazon EVS

Amazon EVS saat ini menyediakan versi VCF berikut untuk pembuatan lingkungan:

Versi VCF	Versi ESX default	Status	EC2 jenis contoh
VCF-5.2.2	ESXi-8.0U3G-24859861	AVAILABLE	i4i.metal
VCF-5.2.1	ESXi-8.0U3b-24280767	TERBATAS	i4i.metal

> **Note**
>
> Saat membuat lingkungan Amazon EVS baru, Anda harus menentukan versi VCF.

Pertimbangan versi ESX

Setiap versi VCF memiliki versi ESX default berdasarkan Broadcom VCF Bill of Materials (BOM). Saat membuat lingkungan baru, Anda tidak dapat memilih versi ESX tertentu. Versi ESX default untuk versi VCF yang dipilih diterapkan secara otomatis.

Namun, saat menambahkan host ke lingkungan Anda, Anda dapat memilih versi ESX yang tersedia untuk jenis instans yang Anda pilih. Jika Anda tidak menentukannya, Amazon EVS menggunakan versi ESX default yang terkait dengan versi VCF lingkungan Anda.

Setelah host ditambahkan, versi ESX-nya hanya dapat ditingkatkan menggunakan vCenter Lifecycle Manager.

> **Note**
>
> Amazon EVS tidak menyediakan semua versi VCF dan ESX yang dirilis oleh Broadcom. Untuk informasi interoperabilitas perangkat lunak, lihat Matriks Interoperabilitas Broadcom. Untuk kompatibilitas perangkat keras penuh dengan AWS EC2 instance, lihat Panduan Kompatibilitas Broadcom.

Meminta akses ke versi VCF terbatas

Jika Anda memerlukan akses ke versi VCF yang `RESTRICTED` berstatus, hubungi AWS Support dengan informasi berikut:

- ID AWS akun Anda
- AWS Wilayah
- Versi VCF spesifik yang Anda butuhkan
- Kasus penggunaan dan pembenaran bisnis Anda (misalnya,security/compliance, compatibility/dependency, dan lainnya)

AWS Support akan meninjau permintaan Anda dan menyetujui atau meminta informasi tambahan. Setelah disetujui, status versi akan berubah menjadi `AVAILABLE` respons AWS konsol atau `get-versions` API.

Manajemen siklus hidup lingkungan Amazon EVS

Halaman ini menjelaskan tanggung jawab manajemen siklus hidup Anda dalam lingkungan Amazon EVS.

Manfaat utama Amazon EVS adalah Anda memiliki kendali penuh atas VMware arsitektur Anda di cloud. Anda dapat mengoptimalkan tumpukan perangkat lunak VMware Cloud Foundation (VCF) untuk memenuhi permintaan unik aplikasi Anda. Karena Amazon EVS adalah layanan yang dikelola sendiri, Anda bertanggung jawab atas manajemen siklus hidup dan pemeliharaan VMware perangkat lunak yang digunakan di lingkungan Amazon EVS, seperti ESX, vSphere, vSAN, NSX, dan SDDC Manager. Anda juga bertanggung jawab untuk menjaga integrasi pihak ketiga apa pun, seperti solusi perlindungan data yang Anda integrasikan ke dalam host Amazon EVS Anda.

Anda bertanggung jawab atas konfigurasi komponen AWS jaringan dasar yang digunakan Amazon EVS, termasuk tabel rute VPC, grup keamanan, dan aturan daftar kontrol akses jaringan (ACL), konfigurasi Server Rute VPC, gateway internet, gateway NAT, dan gateway transit (untuk konektivitas lokal).

AWS bertanggung jawab untuk menerapkan lingkungan Amazon EVS dengan konfigurasi jaringan yang Anda berikan. Penyebaran lingkungan meliputi yang berikut:

- Bootstrapping konfigurasi jaringan lingkungan Amazon EVS Anda.
- Mengaktifkan perutean utara-selatan dengan instance Server Rute VPC yang Anda berikan.
- Menyebarkan subnet EVS VLAN yang diperlukan, antarmuka jaringan elastis, dan empat host ESX awal.
- Mengkonfigurasi jaringan overlay NSX dengan gateway Tier-0 dan gateway Tier-1.
- Menyebarkan cluster NSX Edge dengan dua node NSX Edge dalam mode. Active/Standby
- Membuat dan mengonfigurasi cluster vSAN awal dan memasang datastore.

Anda bertanggung jawab atas konfigurasi VMware NSX, termasuk segmen jaringan, aturan firewall terdistribusi, dan penyeimbang beban. Anda juga bertanggung jawab atas konfigurasi solusi terintegrasi apa pun yang Anda terapkan dengan Amazon EVS setelah lingkungan EVS diterapkan, termasuk konfigurasi VMware HCX dan gateway NSX Tier-1 tambahan.

Untuk informasi selengkapnya tentang AWS dan tanggung jawab pelanggan, lihat model tanggung jawab AWS bersama.

> **Note**
>
> Gateway Tier-0 dan gateway Tier-1 dibuat dan dikonfigurasi sebagai bagian dari penerapan lingkungan Amazon EVS. Amazon EVS hanya mendukung satu gateway Tier-0 saat ini. Setiap modifikasi pada router logis ini atau node tepi NSX VMs dapat memengaruhi konektivitas dan harus dihindari.

VMware pembaruan perangkat lunak

> **Warning**
>
> Jika Anda telah memperbarui versi ESX Anda setelah penerapan lingkungan Amazon EVS, manajer SDDC mungkin gagal selama validasi host VCF di langkah host komisi. Untuk langkah-langkah untuk memecahkan masalah ini, lihat. the section called “Manajer SDDC gagal validasi host VCF selama komisioning host”

Untuk informasi tentang versi VCF yang disediakan oleh Amazon EVS, lihat. the section called “Versi dan instance VCF EC2 ” Sesuai model tanggung jawab AWS bersama, Anda bertanggung jawab untuk menerapkan tambalan, pembaruan, atau peningkatan apa pun ke perangkat lunak VCF, termasuk ESX, vCenter Server, vSAN, NSX, Manajer SDDC, dan solusi terintegrasi lainnya, di lingkungan EVS Anda. Pasca penerapan, kami menyarankan Anda meninjau versi perangkat lunak VCF yang digunakan oleh Amazon EVS dan memperbarui sesuai kebutuhan. Anda dapat memperoleh pembaruan VCF melalui portal dukungan Broadcom. Kami juga menyarankan Anda membuat dan mematuhi jadwal pemeliharaan rutin untuk pembaruan dan tambalan.

> **Note**
>
> Amazon EVS tidak mendukung VMware Cloud Foundation 9 saat ini.

> **Note**
>
> Amazon EVS tidak menyediakan semua versi VCF dan ESX yang dirilis oleh Broadcom. Untuk informasi interoperabilitas perangkat lunak, lihat Matriks Interoperabilitas Broadcom. Untuk kompatibilitas perangkat keras penuh dengan AWS EC2 instance, lihat Panduan Kompatibilitas Broadcom.

Tambalan, pembaruan, atau peningkatan tertentu mungkin berdampak pada beban kerja yang berjalan di lingkungan Anda. Sebelum menambal, memperbarui, atau meningkatkan perangkat lunak VCF Anda, kami sarankan Anda meninjau Panduan Manajemen Siklus Hidup VCF untuk memahami bagaimana perubahan ini akan berdampak pada lingkungan Anda. Kami juga menyarankan Anda menguji perubahan di lingkungan pementasan sebelum menerapkan ke produksi. Anda dapat meninjau catatan rilis VCF 5.2.x untuk memahami pembaruan VCF 5.2.x terbaru.

Proses hidup dan pemeliharaan host ESX

Anda bertanggung jawab atas pengelolaan dan pemeliharaan siklus hidup host ESX dalam lingkungan Amazon EVS, termasuk memantau kesehatan host dan memulihkan masalah host. Untuk informasi selengkapnya, lihat the section called “Pemeliharaan lingkungan”.

AWS melakukan pemeliharaan terjadwal pada EC2 instans i4i.metal yang mendasarinya untuk memastikan keandalan, ketersediaan, dan kinerja infrastruktur. Lihat informasi yang lebih lengkap di the section called “Tentang pemeliharaan AWS terjadwal untuk EC2 instans”.

Melakukan pemeliharaan di lingkungan Anda

Bagian ini menjelaskan cara melakukan tugas pemeliharaan umum untuk lingkungan Amazon EVS Anda.

Topik

- Pantau status dan sumber daya lingkungan Anda
- Pemeliharaan AMI
- Pemeliharaan host Amazon EVS
- Konfigurasikan tabel rute khusus untuk subnet Amazon EVS
- Konfigurasikan daftar kontrol akses jaringan untuk mengontrol lalu lintas subnet Amazon EVS VLAN

- Siklus hidup manajemen rahasia

Pantau status dan sumber daya lingkungan Anda

Anda dapat memantau berbagai aspek lingkungan Amazon EVS dan AWS sumber daya yang mendasarinya menggunakan konsol Amazon EVS atau. AWS CLI

> **Note**
>
> VMware Komponen Cloud Foundation (VCF) dipantau di SDDC Manager. Anda tidak dapat memantau komponen VCF menggunakan konsol Amazon EVS atau. AWS CLI Untuk informasi tentang penggunaan SDDC Manager untuk memantau komponen VMware Cloud Foundation (VCF), lihat Memulai SDDC Manager.

Lihat status lingkungan dan sumber daya

Status lingkungan membantu Anda menentukan apakah lingkungan Anda mengalami masalah yang membutuhkan perhatian. Ikuti prosedur ini untuk memeriksa status lingkungan Anda dan melihat sumber daya yang mendasarinya.

Example

Amazon EVS console

1. Buka konsol Amazon EVS.
2. Pada panel navigasi, pilih Lingkungan.
3. Pilih ID lingkungan Anda untuk membuka halaman detail lingkungan.
4. Di bawah Detail, lihat status Lingkungan.

   Jika lingkungan Anda sehat, statusnya ditampilkan sebagai Lulus. Jika ada masalah, status ditampilkan sebagai Gagal. Ketika status Gagal, Anda dapat melihat popover yang menunjukkan hasil dari empat pemeriksaan status lingkungan:

   - Penggunaan kembali kunci - Menunjukkan Lulus atau Gagal untuk menunjukkan apakah kunci lisensi VCF valid.
   - Jumlah host - Menunjukkan Tidak Dikenal, Lulus, atau Gagal untuk menunjukkan status konektivitas host.

- Cakupan kunci - Menunjukkan Lulus atau Gagal untuk menunjukkan apakah kunci lisensi VCF mencakup semua host.
- Reachability - Menunjukkan Lulus atau Gagal untuk menunjukkan jangkauan ke Manajer SDDC.

  Untuk informasi tentang kegagalan pemeriksaan status lingkungan pemecahan masalah, lihat. Pemecahan masalah

  Untuk melihat sumber daya di lingkungan Anda

  Pilih salah satu tab berikut:

- Host - Menunjukkan host di lingkungan Anda.
- Jaringan & konektivitas - Menunjukkan sumber daya VPC, subnet EVS, dan VPC Route Server yang terkait dengan lingkungan Anda.
- Peralatan manajemen - Menunjukkan peralatan manajemen VCF di lingkungan Anda dengan nama host DNS dan kredensialnya yang terkait.
- Tag - Menunjukkan tag yang terkait dengan lingkungan Anda.

AWS CLI

Anda dapat menggunakan AWS CLI untuk memeriksa status lingkungan dan sumber daya Anda.

Untuk membuat daftar semua lingkungan dan statusnya

```
aws evs list-environments
```

> **Tip**
>
> Gunakan `--query` parameter untuk memfilter output. Contoh:

```
aws evs list-environments --query 'Environments[*].[EnvironmentId,Status]'
```

Untuk membuat daftar host lingkungan

```
aws evs list-environment-hosts \
    --environment-id environment-id
```

Untuk membuat daftar lingkungan VLANs

```
aws evs list-environment-vlans \
    --environment-id environment-id
```

Untuk informasi selengkapnya tentang operasi API, lihat berikut ini di Panduan Referensi Amazon EVS API:

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

Pemeliharaan AMI

Amazon EVS menyebarkan host ESX dengan EVS Amazon Machine Image (AMI) khusus. AMI berisi add-on vendor khusus yang berisi paket yang diperlukan untuk menjalankan ESX di Amazon. EC2

Memecahkan masalah menambahkan kegagalan host karena gambar cluster yang tidak kompatibel

Saat Anda menambahkan host ke lingkungan Anda, host memiliki versi terbaru dari add-on vendor khusus EVS yang tersedia. Jika lingkungan Anda menggunakan host dengan versi add-on yang lebih lama, menambahkan host baru gagal dengan kesalahan bahwa host baru tidak kompatibel dengan gambar cluster Anda. Untuk langkah-langkah rinci untuk memperbaiki masalah ini, lihatthe section called “Tambahkan kegagalan host karena gambar cluster yang tidak kompatibel”.

Pemeliharaan host Amazon EVS

Karena Amazon EVS adalah layanan yang dikelola sendiri, Anda bertanggung jawab atas pemeliharaan perangkat lunak VMware Cloud Foundation (VCF) yang berjalan di host, memantau kesehatan host, dan memperbaiki masalah host, termasuk penggantian host jika terjadi kegagalan host. Untuk informasi selengkapnya tentang mengelola host ESX di VMware Cloud Foundation (VCF), lihat Manajemen Host di dokumentasi VMware Cloud Foundation.

Memeriksa kesehatan dari EC2 contoh yang mendasarinya

Amazon EC2 melakukan pemeriksaan otomatis pada setiap EC2 instans yang berjalan untuk mengidentifikasi masalah perangkat keras dan perangkat lunak. Anda dapat melihat hasil pemeriksaan status ini di EC2 konsol atau AWS CLI untuk mengidentifikasi masalah spesifik dan

terdeteksi. Untuk informasi selengkapnya, lihat Melihat pemeriksaan status untuk EC2 instans Amazon di Panduan EC2 Pengguna Amazon dan describe-instance-statusdi Referensi Baris AWS CLI Perintah.

Anda dapat membuat CloudWatch alarm untuk memperingatkan Anda jika pemeriksaan status gagal pada instance tertentu. Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm untuk EC2 instans Amazon yang gagal memeriksa status di Panduan Pengguna EC2 Amazon.

Tentang pemeliharaan AWS terjadwal untuk EC2 instans

AWS melakukan pemeliharaan terjadwal pada EC2 instans yang mendasarinya untuk memastikan keandalan, ketersediaan, dan kinerja. EC2 instans bare metal tunduk pada jenis acara terjadwal yang sama seperti contoh lainnya EC2 . AWS dapat menjadwalkan acara untuk reboot, menghentikan, dan menghentikan instans Anda karena masalah perangkat keras yang mendasarinya atau pemeliharaan terjadwal. Peristiwa ini tidak sering terjadi. Untuk informasi selengkapnya, lihat Jenis acara terjadwal di Panduan EC2 Pengguna Amazon.

> **Note**
>
> Anda harus menempatkan host Anda dalam mode pemeliharaan di Klien vSphere sebelum acara reboot terjadwal.

Jika salah satu contoh Anda akan terpengaruh oleh acara yang dijadwalkan, AWS beri tahu Anda terlebih dahulu melalui email, menggunakan alamat email yang terkait dengan Anda. Akun AWS AWS juga mengirimkan acara AWS Kesehatan, yang dapat Anda pantau dan kelola dengan menggunakan Amazon EventBridge. Untuk informasi selengkapnya, lihat Memantau peristiwa di AWS Kesehatan dengan Amazon EventBridge dan peristiwa Terjadwal untuk EC2 instans Amazon di Panduan EC2 Pengguna Amazon.

Kapan saja, Anda dapat menjadwal ulang acara sehingga terjadi pada tanggal dan waktu tertentu yang cocok untuk Anda. Peristiwa dapat dijadwalkan ulang hingga tanggal batas waktu. Untuk informasi selengkapnya, lihat Menjadwalkan ulang acara terjadwal untuk EC2 instans di Panduan EC2 Pengguna Amazon.

Menggunakan Reservasi Kapasitas EC2 Sesuai Permintaan

Anda dapat menggunakan Reservasi Kapasitas EC2 Sesuai Permintaan untuk memastikan bahwa klaster Anda memiliki kapasitas yang cukup selama periode pemeliharaan. Anda dapat memesan

kapasitas di Availabilty Zone tertentu untuk durasi berapa pun. Untuk informasi selengkapnya, lihat Cadangan kapasitas komputasi dengan Reservasi Kapasitas EC2 Sesuai Permintaan di Panduan Pengguna Amazon EC2 .

Untuk langkah-langkah untuk membuat Reservasi Kapasitas, lihat Membuat Reservasi Kapasitas di Panduan EC2 Pengguna Amazon.

> **Note**
>
> Jika Anda menggunakan Reservasi Kapasitas EC2 Sesuai Permintaan atau Tuan Rumah EC2 Khusus, kami sarankan Anda mempertahankan host cadangan untuk beban kerja yang sangat penting. Sementara Reservasi Kapasitas memastikan Anda memiliki akses ke sejumlah kapasitas EC2 instans tertentu di Availability Zone tertentu, memiliki host cadangan menyediakan lapisan redundansi tambahan yang sangat penting untuk beban kerja yang sangat penting. Untuk Host Khusus, memiliki host cadangan memastikan bahwa Anda menjaga lingkungan untuk beban kerja yang sangat penting, bahkan jika host utama memerlukan pemeliharaan atau mengalami masalah.

Mempersiapkan AWS jadwal **`system-maintenance`** dan **`instance-retirement`** acara

AWS menjadwalkan dua jenis `system-maintenance` acara: pemeliharaan jaringan dan pemeliharaan daya.

- Selama pemeliharaan jaringan, instans terjadwal kehilangan konektivitas jaringan dalam jangka waktu singkat. Konektivitas jaringan normal ke instans Anda akan dipulihkan setelah pemeliharaan selesai.
- Selama pemeliharaan daya, instans terjadwal akan offline dalam jangka waktu singkat, lalu di-boot ulang. Ketika reboot dilakukan pada instance EC2 bare metal, data volume penyimpanan instance tidak dipertahankan.

AWS menjadwalkan EC2 `instance-retirement` peristiwa saat degradasi perangkat keras yang mendasari hosting EC2 instans Anda terdeteksi.

Untuk memulihkan `system-maintenance` dan `instance-retirement` peristiwa, ganti host yang gagal dengan host baru menggunakan konsol Amazon EVS atau AWS CLI dan Manajer SDDC sebelum peristiwa pemeliharaan terjadi. Jika Anda menunggu peristiwa pemeliharaan terjadi dan

reboot EC2 instance diperlukan, Anda akan kehilangan data vSAN Anda yang disimpan pada volume penyimpanan instance. Untuk langkah mendetail, lihat the section called “Ganti host Amazon EVS”.

> **Important**
>
> EC2 Konsol tidak boleh digunakan untuk mengelola status host Amazon EVS Anda, termasuk, berhenti, mulai, dan penghentian. Jangan mencoba memulai, menghentikan, atau menghentikan EC2 instans yang digunakan Amazon EVS. Tindakan ini mengakibatkan kehilangan data vSAN.

Ganti host Amazon EVS

Ikuti prosedur ini untuk mengganti host Amazon EVS.

> **Warning**
>
> Host Amazon EVS menggunakan add-on vendor khusus untuk menyediakan fungsionalitas host yang penting. Saat Anda menambahkan host ke lingkungan Anda, itu akan memiliki versi terbaru dari add-on khusus Amazon EVS yang tersedia. Jika lingkungan Anda menggunakan host dengan versi add-on yang lebih lama, menambahkan host ke kluster vSphere Anda akan menyebabkan remediasi gambar cluster gagal. Untuk langkah-langkah untuk memecahkan masalah ini, lihat. the section called “Memecahkan masalah menambahkan kegagalan host karena gambar cluster yang tidak kompatibel”

> **Warning**
>
> Jika Anda telah memperbarui versi ESX pasca-penerapan, manajer SDDC mungkin gagal selama validasi host VCF di langkah host komisi. Untuk langkah-langkah untuk memecahkan masalah ini, lihat. the section called “Manajer SDDC gagal validasi host VCF selama komisioning host”

> **Note**
>
> Pastikan jumlah host Amazon EVS per kuota lingkungan EVS diatur dengan benar untuk memastikan pembuatan host berhasil. Pembuatan host gagal jika nilai kuota ini kurang dari

jumlah host yang Anda coba sediakan dalam satu lingkungan Amazon EVS. Anda mungkin perlu meminta peningkatan kuota untuk operasi pemeliharaan yang memerlukan penggantian host. Untuk informasi selengkapnya, lihat Kuota layanan.

Example

Amazon EVS console and SDDC Managuer UI

1. Buka konsol Amazon EVS.
2. Di panel navigasi, pilih Lingkungan.
3. Pilih lingkungan yang berisi host yang akan diganti.
4. Pilih tab Hosts.
5. Pilih Buat host.
6. Tentukan detail host dan pilih Buat host.
7. Untuk memverifikasi penyelesaian, periksa apakah status Host telah berubah menjadi Dibuat.
8. Ambil kredensi untuk kata sandi root ESX dari Secrets Manager. AWS Untuk informasi selengkapnya tentang mengambil rahasia, lihat Mendapatkan AWS rahasia dari Secrets Manager di Panduan Pengguna AWS Secrets Manager.
9. Pergi ke Manajer SDDC.
10. Komisi host baru di SDDC Manager, menggunakan kredenal root ESX yang Anda ambil pada langkah sebelumnya. Untuk informasi selengkapnya, lihat Host Komisi di dokumentasi VMware Cloud Foundation.
11. Tambahkan host baru ke cluster. Untuk informasi selengkapnya, lihat Cara Menambahkan Host ESX ke Cluster vSphere Anda dengan Menggunakan Alur Kerja Mulai Cepat di dokumentasi vSphere.
12. Nonaktifkan host lama di SDDC Manager yang ingin Anda hapus dari SDDC Manager. Untuk informasi selengkapnya, lihat Menonaktifkan Host di dokumentasi VMware Cloud Foundation.
13. Kembali ke konsol Amazon EVS.
14. Di bawah tab Hosts, pilih host yang gagal dan pilih Hapus > Hapus host.

AWS CLI and SDDC Manager UI

1. Buka sesi terminal baru.

2. Buat host baru. Lihat contoh perintah di bawah ini untuk referensi.

```
aws evs create-environment-host \
    --environment-id "env-abcde12345" \
    --host '{ \
        "hostName": "esxi-host-05", \
        "keyName": "your-ec2-keypair-name", \
        "instanceType": "i4i.metal" \
        "esxVersion": "ESXi-8.0U3g-24859861"\
    }'
```

3. Ambil kredensi untuk kata sandi root ESX dari Secrets Manager. AWS Untuk informasi selengkapnya tentang mengambil rahasia, lihat Mendapatkan AWS rahasia dari Secrets Manager di Panduan Pengguna AWS Secrets Manager.
4. Pergi ke Manajer SDDC.
5. Komisi host baru di SDDC Manager, menggunakan kredenal root ESX yang Anda ambil pada langkah sebelumnya. Untuk informasi selengkapnya, lihat Host Komisi di dokumentasi VMware Cloud Foundation.
6. Tambahkan host baru ke cluster yang berisi host yang rusak.
7. Nonaktifkan host yang terganggu di Manajer SDDC. Untuk informasi selengkapnya, lihat Menonaktifkan Host di dokumentasi VMware Cloud Foundation.
8. Kembali ke terminal.
9. Hapus host yang gagal. Lihat contoh perintah di bawah ini untuk referensi.

```
aws evs delete-environment-host --environment-id "env-abcde12345" --host-name
 "esxi-host-05"
```

Pemecahan masalah

Untuk panduan pemecahan masalah, lihat. Pemecahan masalah Jika Anda terus mengalami masalah setelah meninjau panduan pemecahan masalah, hubungi AWS Support untuk bantuan lebih lanjut.

Konfigurasikan tabel rute khusus untuk subnet Amazon EVS

Amazon EVS mendukung penggunaan tabel rute khusus hanya setelah lingkungan Amazon EVS dibuat. Untuk mengaktifkan pembuatan lingkungan yang berhasil, Anda harus mengonfigurasi tabel

rute utama untuk mengizinkan lalu lintas ke layanan dependen seperti DNS dan sistem lokal. Ini karena subnet Amazon EVS VLAN secara implisit terkait dengan tabel rute utama VPC kami selama penerapan lingkungan.

Setelah lingkungan Anda diterapkan, Anda harus secara eksplisit mengaitkan setiap subnet Amazon EVS VLAN dengan tabel rute di VPC Anda. Konektivitas NSX gagal jika subnet VLAN Anda tidak secara eksplisit terkait dengan tabel rute VPC. Kami sangat menyarankan agar Anda secara eksplisit mengaitkan subnet Anda dengan tabel rute khusus. Tabel rute khusus memberikan kontrol yang lebih terperinci atas perutean lalu lintas jaringan dalam VPC Anda, memungkinkan aturan perutean yang disesuaikan untuk subnet atau gateway tertentu. Untuk informasi selengkapnya tentang membuat tabel rute khusus, lihat Membuat tabel rute untuk VPC Anda di Panduan Pengguna Amazon VPC.

Konfigurasikan daftar kontrol akses jaringan untuk mengontrol lalu lintas subnet Amazon EVS VLAN

Daftar kontrol akses jaringan (ACL) memungkinkan atau menolak lalu lintas masuk atau keluar tertentu di tingkat subnet. Anda dapat menggunakan jaringan ACLs untuk mengontrol lalu lintas masuk dan keluar untuk subnet Amazon EVS VLAN Anda. Untuk informasi selengkapnya, lihat Membuat ACL jaringan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Important

EC2 grup keamanan tidak berfungsi pada antarmuka jaringan elastis yang dilampirkan ke subnet Amazon EVS VLAN. Untuk mengontrol lalu lintas ke dan dari subnet Amazon EVS VLAN, Anda harus menggunakan daftar kontrol akses jaringan.

Warning

Amazon EVS memerlukan akses ke penyebaran VCF Anda. Anda harus mengonfigurasi grup keamanan dan daftar kontrol akses jaringan (ACLs) agar Amazon EVS dapat berkomunikasi dengan:

- Server DNS melalui TCP/UDP port 53.
- Manajemen host VLAN subnet melalui HTTPS dan SSH.
- Manajemen VM VLAN subnet melalui HTTPS dan SSH.

Jika grup keamanan dan jaringan Anda ACLs tidak mengizinkan akses ini, penerapan lingkungan Amazon EVS akan gagal dan lingkungan yang ada mungkin memiliki status kepatuhan yang terdegradasi.

Siklus hidup manajemen rahasia

Amazon EVS menggunakan AWS Secrets Manager untuk membuat, mengenkripsi, dan menyimpan rahasia di akun Anda pada penerapan lingkungan awal. Rahasia ini berisi kredensi VCF yang diperlukan untuk menginstal dan mengakses peralatan manajemen VCF seperti vCenter Server, NSX, dan SDDC Manager, serta kata sandi root host ESX. Amazon EVS juga menghapus rahasia terkelola atas nama Anda saat lingkungan EVS dihapus.

Anda bertanggung jawab atas manajemen lifecyle rahasia, termasuk rotasi rahasia. Amazon EVS tidak menyediakan rotasi terkelola untuk rahasia Anda. Kami menyarankan Anda memutar rahasia secara teratur pada jendela rotasi yang ditetapkan untuk memastikan bahwa rahasia tidak berumur panjang. Untuk informasi selengkapnya, lihat Jadwal rotasi di Panduan Pengguna AWS Secrets Manager.

Buat host Amazon EVS

Setelah lingkungan Amazon EVS diterapkan, Anda dapat menambahkan host untuk meningkatkan kapasitas dan ketahanan beban kerja. Amazon EVS mendukung 4-16 host per lingkungan. Tindakan ini hanya dapat digunakan setelah lingkungan Amazon EVS diterapkan.

Note

Anda harus menetapkan dan menugaskan host dalam antarmuka pengguna SDDC Manager.

Untuk membuat host Amazon EVS

Ikuti langkah-langkah ini untuk membuat host Amazon EVS.

Warning

Host Amazon EVS menggunakan add-on vendor khusus untuk menyediakan fungsionalitas host yang penting. Saat Anda menambahkan host ke lingkungan Anda, itu akan memiliki

versi terbaru dari add-on khusus Amazon EVS yang tersedia. Jika lingkungan Anda menggunakan host dengan versi add-on yang lebih lama, menambahkan host ke kluster vSphere Anda akan menyebabkan remediasi gambar cluster gagal. Untuk langkah-langkah untuk memecahkan masalah ini, lihat. the section called “Memecahkan masalah menambahkan kegagalan host karena gambar cluster yang tidak kompatibel”

Warning

Jika Anda telah memperbarui versi ESX Anda setelah penerapan lingkungan Amazon EVS, manajer SDDC mungkin gagal selama validasi host VCF di langkah host komisi. Untuk langkah-langkah untuk memecahkan masalah ini, lihat. the section called “Manajer SDDC gagal validasi host VCF selama komisioning host”

Note

Pastikan jumlah host Amazon EVS per kuota lingkungan EVS diatur dengan benar untuk memastikan pembuatan host berhasil. Pembuatan host gagal jika nilai kuota ini kurang dari jumlah host yang Anda coba sediakan dalam satu lingkungan Amazon EVS. Untuk menaikkan kuota, Anda dapat meminta kenaikan kuota. Untuk informasi selengkapnya, lihat Kuota layanan.

Note

Jika Anda tidak menentukan versi ESX saat menambahkan host ke lingkungan Anda, Amazon EVS secara otomatis menggunakan versi ESX default yang terkait dengan versi VCF lingkungan Anda. Untuk informasi selengkapnya, lihat the section called “Versi dan instance VCF EC2 ”.

Important

Saat menambahkan host ESX, pilih versi ESX yang cocok dengan kluster vSphere target Anda. Jika versi yang sama tidak tersedia, gunakan versi yang lebih lama dan tingkatkan menggunakan vSphere Lifecycle Manager. Untuk informasi selengkapnya, lihat the section

called “Manajer SDDC gagal validasi host VCF selama komisioning host”. Peningkatan mungkin memerlukan reboot host dan meningkatkan waktu yang diperlukan untuk menugaskan host.
Host dengan versi ESX yang lebih baru dari versi ESX gambar kluster vSphere Anda tidak dapat diturunkan peringkatnya. Anda harus menghapus host dan membuatnya kembali dengan versi ESX yang benar.

Example

Amazon EVS console and SDDC Managuer UI

1. Buka konsol Amazon EVS.
2. Di panel navigasi, pilih Lingkungan.
3. Pilih lingkungan tempat Anda ingin membuat host.
4. Pilih tab Hosts.
5. Pilih Buat host.
6. Tentukan detail host dan pilih Buat host.
7. Untuk memverifikasi penyelesaian, periksa apakah status Host telah berubah menjadi Dibuat.
8. Pergi ke Manajer SDDC.
9. Komisi host baru di SDDC Manager. Untuk informasi selengkapnya, lihat Host Komisi di dokumentasi VMware Cloud Foundation.
10. Tambahkan host baru ke cluster, menggunakan SDDC Manager. Untuk informasi selengkapnya, lihat Cara Menambahkan Host ESX ke Cluster vSphere Anda dengan Menggunakan Alur Kerja Mulai Cepat di dokumentasi vSphere.

AWS CLI and SDDC Manager UI

1. Buka sesi terminal baru.
2. Buat host baru. Lihat contoh perintah di bawah ini untuk referensi.

```
aws evs create-environment-host \
    --environment-id "env-abcde12345" \
    --host '{ \
        "hostName": "esxi-host-05", \
        "keyName": "your-ec2-keypair-name", \
```

```
        "instanceType": "i4i.metal",\
        "esxVersion": "ESXi-8.0U3g-24859861"\
    }'
```

3. Pergi ke Manajer SDDC.
4. Komisi host baru di SDDC Manager. Untuk informasi selengkapnya, lihat Host Komisi di dokumentasi VMware Cloud Foundation.
5. Tambahkan host baru ke cluster, menggunakan SDDC Manager. Untuk informasi selengkapnya, lihat Cara Menambahkan Host ESX ke Cluster vSphere Anda dengan Menggunakan Alur Kerja Mulai Cepat di dokumentasi vSphere.

Hapus host Amazon EVS

Anda dapat menghapus host Amazon EVS dari lingkungan Anda saat host tidak lagi diperlukan. Amazon EVS mengharuskan lingkungan Anda memiliki minimal empat host. Amazon EVS tidak mendukung lingkungan dengan kurang dari empat host.

> **Warning**
>
> Menghapus host tanpa menonaktifkan akan meninggalkan data basi di vCenter dan Manajer SDDC Anda yang mungkin memerlukan upaya tambahan untuk membersihkannya. Pastikan host Anda dinonaktifkan sebelum menghapus host di konsol Amazon EVS atau API.

> **Warning**
>
> Selalu gunakan konsol Amazon EVS atau API untuk menghapus host Amazon EVS Anda. Menghapus host dari EC2 konsol dapat membuat lingkungan Anda dalam keadaan tidak konsisten.

Untuk menghapus host Amazon EVS

Ikuti langkah-langkah ini untuk menghapus host Amazon EVS.

Example

SDDC Managuer UI and Amazon EVS console

1. Pergi ke Manajer SDDC.
2. Hapus cluster dari SDDC Manager.
3. Nonaktifkan host di SDDC Manager. Untuk informasi selengkapnya, lihat Menonaktifkan Host di dokumentasi VMware Cloud Foundation.
4. Buka konsol Amazon EVS.
5. Di panel navigasi, pilih Lingkungan.
6. Pilih lingkungan yang berisi host untuk dihapus.
7. Pilih tab Hosts.
8. Pilih Hapus host.
9. Pilih host dan pilih Hapus dalam tab Hosts. Ulangi langkah ini untuk setiap host yang ingin Anda hapus.

SDDC Manager UI and AWS CLI

1. Pergi ke Manajer SDDC.
2. Hapus cluster dari SDDC Manager.
3. Nonaktifkan host di SDDC Manager. Untuk informasi selengkapnya, lihat Menonaktifkan Host di dokumentasi VMware Cloud Foundation.
4. Buka sesi terminal baru.
5. Hapus host. Lihat contoh perintah di bawah ini untuk referensi.

```
aws evs delete-environment-host \
--environment-id env-abcdefghij \
--host-name my-evs-host.example.com
```

Keamanan di Amazon Elastic VMware 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 ini sebagai keamanan cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS di dalamnya AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi keefektifan keamanan kami sebagai bagian dari program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Elastic VMware Service (Amazon EVS), lihat Layanan AWS di Cakupan berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh Layanan AWS 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 Amazon EVS. Ini menunjukkan kepada Anda cara mengonfigurasi Amazon EVS untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan Layanan AWS yang lain yang membantu Anda memantau dan mengamankan sumber daya Amazon EVS Anda.

Konten

Perlindungan data di Amazon EVS

Model tanggung jawab AWS bersama berlaku untuk perlindungan data di Amazon Elastic VMware Service. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk menjaga

kontrol atas konten Anda yang di-host di infrastruktur ini, termasuk komponen VMware Cloud Foundation (VCF). Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, silakan lihat Pertanyaan Umum Privasi Data. Untuk informasi tentang perlindungan data di Eropa, lihat Model Tanggung Jawab AWS Bersama dan posting blog GDPR di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau. AWS Identity and Access Management Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.

  > **Note**
  >
  > Amazon EVS tidak mencatat aktivitas pengguna untuk AWS non-komponen, seperti aktivitas dalam lingkungan VCF Anda. Aktivitas ini dicatat di berbagai VMware konsol seperti vSphere dan NSX Manager. Jika logging VCF terpusat diinginkan, Anda dapat mengonfigurasi solusi pemantauan VCF seperti Operasi VMware Aria atau Observabilitas VMware Tanzu untuk mencapai hasil ini. Untuk informasi selengkapnya, lihat VMware Cloud Foundation dengan VMware Tanzu dan VMware Aria Suite Lifecyle dalam mode VMware Cloud Foundation dalam dokumentasi VCF.

- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu dalam menemukan dan mengamankan data sensitif yang disimpan di dalamnya. Amazon S3
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif, seperti alamat email pelanggan Anda, ke dalam tag atau bidang teks bentuk bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon EVS atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi saat diam

Amazon EVS menerapkan EC2 instans i4i.metal yang menggunakan enkripsi AES-256 transparan secara default untuk data yang disimpan pada volume penyimpanan instans. Amazon EVS tidak mendukung enkripsi volume boot EBS saat ini.

Volume boot Amazon EBS

Instans Amazon EVS i4i.metal menggunakan volume boot Amazon EBS. Volume boot berisi sistem operasi dan file lain yang diperlukan untuk EC2 instance untuk boot dan jalankan. Volume boot tidak dienkripsi. Amazon EVS tidak mendukung enkripsi volume boot saat ini. Volume boot tidak berisi data pengguna dari mesin virtual Anda.

Volume penyimpanan instans

EC2 Instans Amazon EVS i4i.metal dilengkapi dengan penyimpanan NVMe SSD lokal, yang merupakan bagian dari perangkat keras instans. Amazon EVS menggunakan volume penyimpanan NVMe instance sebagai disk untuk datastores vSAN. Datastore vSan menyimpan mesin virtual manajemen dan beban kerja Anda setelah Anda menerapkan lingkungan Amazon EVS Anda.

Data pada volume penyimpanan NVMe instance dienkripsi menggunakan cipher XTS-AES-256, diimplementasikan pada modul perangkat keras pada instance. Kunci yang digunakan untuk mengenkripsi data yang ditulis ke perangkat NVMe penyimpanan yang terpasang secara lokal adalah per pelanggan, dan per volume. Untuk informasi selengkapnya, lihat Enkripsi saat istirahat di Panduan EC2 Pengguna Amazon.

Setelah menerapkan lingkungan Amazon EVS, Anda dapat mengaktifkan data-at-rest enkripsi vSAN untuk semua data yang disimpan di datastore vSAN, untuk mesin virtual individual ()VMs, atau untuk file individual di dalamnya. VMs Kontrol granular ini dapat berguna ketika beberapa VMs memerlukan enkripsi sementara yang lain tidak, atau ketika disk atau file tertentu dalam VM perlu dienkripsi. Untuk informasi selengkapnya, lihat Cara Kerja Data-At-Rest Enkripsi vSAN di dokumentasi vSAN VMware .

Enkripsi saat bergerak

Amazon EVS tidak mengenkripsi lalu lintas dalam transit Anda secara default. Untuk mengenkripsi data dalam perjalanan yang melintasi Amazon EVS, Anda dapat menggunakan enkripsi lapisan aplikasi dengan protokol seperti Transport Layer Security (TLS). Untuk mempelajari enkripsi lalu lintas EC2 instance, lihat Enkripsi dalam Transit di Panduan EC2 Pengguna Amazon.

> **Note**
>
> Enkripsi jaringan Nitro tidak berlaku untuk EC2 instance yang digunakan Amazon EVS. Amazon EVS tidak mendukung enkripsi lalu lintas antar host dalam transit.

Opsi enkripsi dalam transit untuk konektivitas lokal

Untuk mengenkripsi lalu lintas antara pusat data lokal dan Amazon EVS, Anda dapat menggabungkan penggunaan Direct AWS Connect dan AWS Site-To-Site VPN dengan Transit Gateway AWS . Kombinasi ini menyediakan koneksi pribadi IPsec terenkripsi yang juga mengurangi biaya jaringan, meningkatkan throughput bandwidth, dan memberikan pengalaman jaringan yang lebih konsisten daripada koneksi VPN berbasis internet. Untuk informasi selengkapnya, lihat AWS Site-to-Site VPN IP Pribadi dengan AWS Direct Connect.

> **Note**
>
> Amazon EVS tidak mendukung konektivitas melalui antarmuka virtual pribadi AWS Direct Connect (VIF), atau melalui koneksi AWS Site-to-Site VPN yang berakhir langsung ke VPC underlay. Amazon EVS mendukung penghentian IPSec VPN pada gateway NSX Edge Tier-0 atau Tier-1. Untuk informasi selengkapnya, lihat Menambahkan Layanan IPSec VPN NSX di dokumentasi VMware NSX.

MAC Security (MACsec) adalah standar IEEE yang menyediakan kerahasiaan data, integritas data, dan keaslian asal data. Anda dapat menggunakan koneksi AWS Direct Connect yang mendukung MACsec untuk mengenkripsi data dari pusat data perusahaan ke lokasi AWS Direct Connect. Untuk informasi selengkapnya, lihat Keamanan MAC di AWS Direct Connect di Panduan Pengguna AWS Direct Connect.

Enkripsi dalam perjalanan untuk data VMware jaringan

Setelah lingkungan Amazon EVS diterapkan, Anda memiliki beberapa opsi untuk menerapkan data dalam enkripsi transit di lapisan VCF: VMware

- VMware vDefend Distributed Firewall - Memungkinkan Anda untuk menerapkan segmentasi jaringan halus dan menegakkan TLS/SSL enkripsi antara mesin virtual. Untuk informasi selengkapnya, lihat Mengkonfigurasi Pengaturan Keamanan untuk Firewall Terdistribusi dengan Menggunakan Antarmuka Pengguna dalam dokumentasi VMware VCF.
- data-in-transitenkripsi vSan - Dapat digunakan untuk mengenkripsi semua data dan metadata antara host di cluster vSAN Anda. Untuk informasi selengkapnya, lihat Data-In-TransitEnkripsi vSAN di dokumentasi vSAN VMware .
- VSphere terenkripsi vMotion - mengamankan kerahasiaan, integritas, dan keaslian data yang ditransfer dengan vSphere vMotion. Untuk informasi selengkapnya, lihat Apa yang dienkripsi vSphere vMotion dalam dokumentasi vSphere.

Manajemen kunci dan rahasia

Selama penyebaran lingkungan Amazon EVS, Amazon EVS menggunakan AWS Secrets Manager untuk membuat, mengenkripsi, dan menyimpan rahasia yang berisi kredensyal VCF yang diperlukan untuk menginstal dan mengakses peralatan manajemen VMware VCF, serta kata sandi root ESX. Amazon EVS juga menghapus rahasia terkelola atas nama Anda saat lingkungan EVS dihapus. Untuk informasi selengkapnya, lihat Apa yang ada dalam rahasia Secrets Manager di Panduan Pengguna AWS Secrets Manager.

Secrets Manager menggunakan enkripsi amplop dengan AWS KMS kunci dan kunci data untuk melindungi setiap nilai rahasia. Kunci AWS terkelola default untuk Secrets Manager digunakan kecuali ditentukan lain. Atau, Anda dapat menentukan kunci yang dikelola pelanggan selama pembuatan lingkungan untuk mengenkripsi rahasia Anda. Untuk informasi selengkapnya, lihat Enkripsi dan dekripsi AWS rahasia di Secrets Manager di Panduan Pengguna AWS Secrets Manager.

> **Note**
>
> Ada biaya penggunaan tambahan untuk kunci yang dikelola pelanggan. Kunci AWS terkelola default disediakan tanpa biaya. Untuk informasi selengkapnya, lihat Harga di Panduan Pengguna AWS Secrets Manager.

Amazon EVS tidak menyinkronkan kredensil antara Secrets Manager AWS dan perangkat lunak VCF pasca-penerapan. Anda bertanggung jawab untuk memastikan bahwa rahasia yang terkait dengan lingkungan Amazon EVS Anda tetap sinkron dengan kredensi di SDDC Manager untuk menghindari kedaluwarsa kata sandi VCF dan hilangnya akses ke perangkat lunak VCF.

Amazon EVS tidak memutar rahasia atas nama Anda. Anda bertanggung jawab untuk memutar rahasia yang terkait dengan lingkungan Anda. Kami sangat menyarankan agar putar rahasia Anda segera setelah lingkungan dibuat, dan terapkan jadwal rotasi untuk memperbarui rahasia Anda secara berkala. Untuk informasi selengkapnya tentang memutar AWS rahasia Secrets Manager, lihat fungsi Rotasi oleh Lambda di Panduan Pengguna Secrets AWS Manager. Untuk informasi selengkapnya tentang manajemen kata sandi VCF, lihat Manajemen Kata Sandi di dokumentasi VMware Cloud Foundation.

Important

Amazon EVS tidak menyinkronkan kredensil antara Secrets Manager AWS dan perangkat lunak VCF pasca-penerapan. Jika menggunakan AWS Secrets Manager pasca-penerapan, Anda harus tetap sinkron antara Secrets Manager AWS dan SDDC Manager untuk menghindari masalah kedaluwarsa kata sandi VCF. Anda mungkin kehilangan akses ke perangkat lunak VCF jika kredenal SDDC Manager tidak diperbarui.

Note

Amazon EVS tidak menyediakan rotasi rahasia yang dikelola.

Note

Ada biaya untuk menggunakan fungsi Lambda untuk rotasi AWS rahasia Secrets Manager. Untuk informasi selengkapnya, lihat Harga di Panduan Pengguna AWS Secrets Manager.

Privasi lalu lintas antarjaringan

Amazon EVS menggunakan VPC yang disediakan pelanggan untuk membuat batasan antara sumber daya di lingkungan Amazon EVS dan mengontrol lalu lintas di antara mereka, jaringan lokal

Anda, dan internet. Untuk informasi selengkapnya tentang Amazon VPC keamanan, lihat Memastikan privasi lalu lintas internetwork Amazon VPC di Amazon VPC Panduan Pengguna.

Secara default, Amazon EVS membuat subnet VLAN pribadi selama pembuatan lingkungan yang menolak akses internet langsung. Untuk menambahkan lapisan keamanan lain ke VPC Anda, Anda dapat membuat daftar kontrol akses jaringan khusus untuk VPC Anda dengan aturan yang lebih membatasi konektivitas internet. Untuk informasi selengkapnya, lihat Membuat ACL jaringan untuk VPC Anda di Panduan Pengguna Amazon VPC.

> **Important**
>
> EC2 grup keamanan tidak berfungsi pada antarmuka jaringan elastis yang dilampirkan ke subnet Amazon EVS VLAN. Untuk mengontrol lalu lintas ke dan dari subnet Amazon EVS VLAN, Anda harus menggunakan daftar kontrol akses jaringan.

Jika Anda seorang administrator NSX, Anda dapat mengonfigurasi fitur NSX berikut untuk mengamankan lalu lintas jaringan:

- VMware vDefend Gateway Firewall - Mengamankan perimeter jaringan, melindungi terhadap ancaman eksternal (lalu lintas utara-selatan). Untuk informasi selengkapnya, lihat Menambahkan Kebijakan dan Aturan Firewall Gateway dalam dokumentasi VMware NSX.
- VMware vDefend Distributed Firewall - Melindungi terhadap serangan yang berasal dari dalam jaringan internal (lalu lintas timur-barat). Untuk informasi selengkapnya, lihat Menambahkan Firewall Terdistribusi di dokumentasi VMware NSX.

Manajemen identitas dan akses untuk Amazon Elastic VMware Service

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAM administrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Amazon Elastic Service VMware (Amazon EVS). IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens

- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Amazon EVS bekerja dengan IAM
- Contoh kebijakan berbasis identitas Amazon EVS
- Memecahkan masalah identitas dan akses Amazon EVS
- AWS kebijakan terkelola untuk Amazon EVS
- Menggunakan peran terkait layanan untuk Amazon EVS

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon EVS.

Pengguna layanan — Jika Anda menggunakan layanan Amazon EVS untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Amazon EVS untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda.

Jika Anda tidak dapat mengakses fitur di Amazon EVS, lihatthe section called “Memecahkan masalah identitas dan akses Amazon EVS”.

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Amazon EVS di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon EVS. Tugas Anda adalah menentukan fitur dan sumber daya Amazon EVS mana yang harus diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari selengkapnya tentang cara perusahaan Anda dapat menggunakan IAM Amazon EVS, lihatthe section called “Bagaimana Amazon EVS bekerja dengan IAM”.

IAM administrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Amazon EVS. Untuk melihat contoh kebijakan berbasis identitas Amazon EVS yang dapat Anda gunakan, lihat. IAMthe section called “Contoh kebijakan berbasis identitas Amazon EVS”

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai pengguna root AWS akun Pengguna IAM, atau dengan mengambil peran IAM .

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center (IAM Identity Center) pengguna, autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas gabungan. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke Konsol Manajemen AWS atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara Akun AWS masuk ke Panduan Pengguna AWS Masuk.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Proses penandatanganan Versi Tanda Tangan 4 di Referensi AWS Umum.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor di Panduan Pengguna Pusat AWS Identitas IAM (penerus AWS Single Sign-On) dan Menggunakan otentikasi multi-faktor (MFA) di Panduan Pengguna IAM. AWS

AWS pengguna root akun

Saat pertama kali membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna root AWS akun dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensil pengguna root Anda dan gunakan untuk melakukan tugas yang hanya dapat dilakukan oleh pengguna root. Untuk daftar lengkap tugas

yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di Panduan Referensi Manajemen Akun.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas IAM? di Panduan Pengguna Pusat AWS Identitas IAM (penerus AWS Single Sign-On).

Pengguna IAM dan kelompok

An Pengguna IAMadalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami sarankan untuk mengandalkan kredensi sementara daripada membuat Pengguna IAM yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensil jangka panjang Pengguna IAM, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

IAM Grup adalah identitas yang menentukan kumpulan. Pengguna IAM Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber daya IAM .

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna

memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari lebih lanjut, lihat Kapan membuat Pengguna IAM (bukan peran) di Panduan Pengguna IAM.

IAM peran

IAM Peran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan Pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara Konsol Manajemen AWS dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Menggunakan IAM peran dalam Panduan Pengguna IAM.

IAM peran dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, IAM Identity Center mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin di Panduan Pengguna Pusat Identitas AWS IAM (penerus AWS Single Sign-On).
- Pengguna IAM Izin sementara — Seorang Pengguna IAM dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM peran dari kebijakan berbasis sumber daya di Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, ketika Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek Amazon S3. Layanan mungkin melakukan ini

menggunakan izin kepala panggilan, menggunakan peran layanan, atau menggunakan peran terkait layanan.

- Izin utama — Saat Anda menggunakan peran Pengguna IAM atau untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Kebijakan memberikan izin kepada principal. Saat Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memicu tindakan lain di layanan yang berbeda. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut.
- Peran layanan — Peran layanan adalah IAM peran yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAM Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAM Administrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

- Aplikasi berjalan pada Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredensional sementara untuk aplikasi yang berjalan pada Amazon EC2 instance dan membuat AWS CLI atau permintaan AWS API. Ini lebih baik untuk menyimpan kunci akses dalam Amazon EC2 instance. Untuk menetapkan AWS peran ke Amazon EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada Amazon EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan pada Amazon EC2 instance di Panduan Pengguna IAM.

Untuk mempelajari apakah akan menggunakan IAM peran, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk

informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Setiap IAM entitas (pengguna atau peran) dimulai tanpa izin. Secara default, pengguna tidak dapat melakukan apa pun, bahkan tidak mengubah kata sandi mereka sendiri. Untuk memberikan izin kepada pengguna untuk melakukan sesuatu, administrator harus melampirkan kebijakan izin kepada pengguna. Atau administrator dapat menambahkan pengguna ke grup yang memiliki izin yang dimaksudkan. Ketika administrator memberikan izin untuk grup, semua pengguna dalam grup tersebut akan diberi izin tersebut.

IAM kebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari Konsol Manajemen AWS, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti peran Pengguna IAM, atau grup. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat IAM kebijakan di Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya seperti bucket. Amazon S3 Administrator layanan dapat menggunakan kebijakan ini

untuk menentukan tindakan apa yang dapat dilakukan oleh pelaku utama tertentu (anggota akun, pengguna, atau peran) di sumber daya tersebut dan dengan syarat apa. Kebijakan berbasis sumber daya merupakan kebijakan inline. Tidak ada kebijakan berbasis sumber daya terkelola.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) adalah jenis kebijakan yang mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON. Amazon S3, AWS WAF, dan Amazon VPC merupakan contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat ikhtisar Access Control List (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (atau peran). IAM Pengguna IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah persimpangan kebijakan berbasis identitas entitas dan batas izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk setiap pengguna root AWS akun. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Cara SCPs kerja di Panduan Pengguna AWS Organizations.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah persimpangan kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit

dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Amazon EVS bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon EVS, pelajari IAM fitur apa saja yang tersedia untuk digunakan dengan Amazon EVS.

IAM fitur	Dukungan Amazon EVS
the section called “Kebijakan berbasis identitas untuk Amazon EVS”	Ya
the section called “Kebijakan berbasis sumber daya dalam Amazon EVS”	Tidak
the section called “Tindakan kebijakan untuk Amazon EVS”	Ya
the section called “Sumber daya kebijakan untuk Amazon EVS”	Sebagian
the section called “Kunci kondisi kebijakan untuk Amazon EVS”	Ya
the section called “Daftar kontrol akses (ACLs) di Amazon EVS”	Tidak
the section called “Kontrol akses berbasis atribut (ABAC) dengan Amazon EVS”	Ya
the section called “Menggunakan kredensi sementara dengan Amazon EVS”	Ya

IAM fitur	Dukungan Amazon EVS
the section called “Teruskan sesi akses untuk Amazon EVS”	Ya
the section called “Peran layanan untuk Amazon EVS”	Tidak
the section called “Peran terkait layanan untuk Amazon EVS”	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara Layanan AWS kerja Amazon EVS dan lainnya IAM, lihat Layanan AWS cara kerjanya IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Amazon EVS

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan prinsipal dalam kebijakan berbasis identitas karena berlaku untuk pengguna atau peran yang dilampirkan. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat referensi elemen kebijakan IAM JSON di Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Amazon EVS

Untuk melihat contoh kebijakan berbasis identitas Amazon EVS, lihat. the section called “Contoh kebijakan berbasis identitas Amazon EVS”

Kebijakan berbasis sumber daya dalam Amazon EVS

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Menambahkan principal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Tindakan kebijakan untuk Amazon EVS

Mendukung tindakan Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

`Action`Elemen kebijakan IAM berbasis identitas menggambarkan tindakan atau tindakan spesifik yang akan diizinkan atau ditolak oleh kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Tindakan ini digunakan dalam kebijakan untuk memberikan izin guna melakukan operasi terkait.

Tindakan kebijakan di Amazon EVS menggunakan awalan berikut sebelum tindakan:. `evs:` Misalnya, untuk memberikan izin kepada seseorang untuk membuat lingkungan dengan operasi Amazon EVS `CreateEnvironment` API, Anda menyertakan `evs:CreateEnvironment` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Amazon EVS mendefinisikan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti berikut:

```
"Action": [
      "evs:action1",
      "evs:action2"
```

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `List`, sertakan tindakan berikut:

```
"Action": "evs:List*"
```

Untuk melihat daftar tindakan Amazon EVS, lihat Tindakan yang Ditentukan oleh Amazon EVS di Referensi Otorisasi Layanan.

Sumber daya kebijakan untuk Amazon EVS

Mendukung sumber daya kebijakan: Sebagian

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin tingkat sumber daya, seperti operasi daftar, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Amazon EVS dan jenisnya ARNs, lihat Sumber daya yang ditentukan oleh Amazon Elastic VMware Service di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon Elastic VMware Service.

Beberapa tindakan Amazon EVS API mendukung beberapa sumber daya. Misalnya, beberapa lingkungan dapat direferensikan saat memanggil tindakan `ListEnvironments` API. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARNs dengan koma.

```
"Resource": [
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

Misalnya, sumber daya lingkungan Amazon EVS memiliki ARN berikut:

```
arn:${Partition}:evs:${Region}:${Account}:environment/${EnvironmentId}
```

Untuk menentukan lingkungan `my-environment-1` dan `my-environment-2` pernyataan Anda, gunakan contoh berikut ARNs:

```
"Resource": [
        "arn:aws:evs:us-east-1:123456789012:environment/my-environment-1",
        "arn:aws:evs:us-east-1:123456789012:environment/my-environment-2"
```

Untuk menentukan semua lingkungan yang dimiliki akun tertentu, gunakan wildcard (*):

```
"Resource": "arn:aws:evs:us-east-1:123456789012:environment/*"
```

Kunci kondisi kebijakan untuk Amazon EVS

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

`Condition`Elemen (atau `Condition` blok) memungkinkan Anda menentukan kondisi di mana pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi

AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan Pengguna IAM izin untuk mengakses sumber daya hanya jika ditandai dengan Pengguna IAM namanya. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan Pengguna IAM.

Amazon EVS mendefinisikan kumpulan kunci kondisinya sendiri dan juga mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Semua Amazon EC2 tindakan mendukung kunci `aws:RequestedRegion` dan `ec2:Region` kondisi. Untuk informasi selengkapnya, lihat Contoh: Membatasi akses ke wilayah tertentu.

Untuk melihat daftar kunci kondisi Amazon EVS, lihat Kunci Kondisi untuk Amazon EVS di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon EVS.

Daftar kontrol akses (ACLs) di Amazon EVS

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut (ABAC) dengan Amazon EVS

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang kebijakan ABAC untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Anda dapat melampirkan tag ke sumber daya Amazon EVS atau meneruskan tag dalam permintaan ke Amazon EVS. Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda

di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/<key-name>`, `aws:RequestTag/<key-name>`, atau `aws:TagKeys`. Untuk informasi selengkapnya tentang tindakan yang dapat Anda gunakan dengan tag dalam kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon EVS di Referensi Otorisasi Layanan.

Menggunakan kredensi sementara dengan Amazon EVS

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensi sementara jika Anda masuk Konsol Manajemen AWS menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensitas sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk Amazon EVS

Mendukung sesi akses terusan (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk Amazon EVS

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

Peran terkait layanan untuk Amazon EVS

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan Amazon EVS, lihat. the section called “Menggunakan Peran Terkait Layanan”

Contoh kebijakan berbasis identitas Amazon EVS

Secara default, Pengguna IAM dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon EVS. Mereka juga tidak dapat melakukan tugas menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS API. IAM Administrator harus membuat IAM kebijakan yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke grup Pengguna IAM atau yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan menggunakan editor JSON di Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Amazon EVS
- Mengizinkan pengguna melihat izin mereka sendiri
- Membuat dan mengelola lingkungan Amazon EVS
- Dapatkan dan daftarkan lingkungan Amazon EVS, host, dan VLANs

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Amazon EVS di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di Panduan Pengguna IAM.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM JSON: kondisi di Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda untuk memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan (JSON) dan praktik terbaik. IAM IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi IAM Access Analyzer kebijakan di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang mengharuskan Pengguna IAM atau root pengguna di akun Anda, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk

informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Menggunakan konsol Amazon EVS

Untuk mengakses konsol Amazon EVS, prinsipal IAM harus memiliki set izin minimum. Izin ini harus memungkinkan prinsipal untuk membuat daftar dan melihat detail tentang sumber daya Amazon EVS di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksudkan untuk prinsipal dengan kebijakan yang dilampirkan padanya.

Untuk memastikan bahwa prinsipal IAM Anda masih dapat menggunakan konsol Amazon EVS, buat kebijakan dengan nama unik Anda sendiri, seperti. `AmazonEVSAdminPolicy` Lampirkan kebijakan ke kepala sekolah. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "evs:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EVSServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang Anda coba lakukan.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan Pengguna IAM untuk melihat kebijakan sebaris dan terkelola yang dilampirkan pada identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Membuat dan mengelola lingkungan Amazon EVS

Kebijakan contoh ini mencakup izin yang diperlukan untuk membuat dan menghapus lingkungan Amazon EVS, dan menambah atau menghapus host setelah lingkungan dibuat.

Anda dapat mengganti AWS Region dengan AWS Region yang Anda inginkan untuk menciptakan lingkungan di. Jika akun Anda sudah memiliki `AWSServiceRoleForAmazonEVS` peran, Anda dapat menghapus `iam:CreateServiceLinkedRole` tindakan dari kebijakan. Jika Anda pernah membuat lingkungan Amazon EVS di akun Anda, peran dengan izin ini sudah ada, kecuali Anda menghapusnya.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeHosts",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeRouteServers",
                "ec2:DescribeRouteServerEndpoints",
                "ec2:DescribeRouteServerPeers",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "support:DescribeServices",
                "support:DescribeSupportLevel",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListServiceQuotas"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "ModifyNetworkInterfaceStatement",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "ModifyNetworkInterfaceStatementForSubnetAssociation",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateNetworkInterfaceWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
```

```
            "Sid": "CreateNetworkInterfaceAdditionalResources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "TagOnCreateEC2Resources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateNetworkInterface",
                        "RunInstances",
                        "CreateSubnet",
                        "CreateVolume"
                    ]
                },
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "DetachNetworkInterface",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:DetachNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithTagResource",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
```

```
        },
        {
            "Sid": "RunInstancesWithoutTag",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:image/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:placement-group/*"
            ]
        },
        {
            "Sid": "TerminateInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
```

```
            "Sid": "CreateSubnetWithoutTagForExistingVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "DeleteSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSubnet"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "VolumeDeletion",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*",
             "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "VolumeDetachment",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
```

```
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RouteServerAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:GetRouteServerAssociations"
            ],
            "Resource": "arn:aws:ec2:*:*:route-server/*"

        },
        {
            "Sid": "EVSServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SecretsManagerCreateWithTag",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
```

```
                ]
            }
        }
    },
    {
        "Sid": "SecretsManagerTagging",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:TagResource"
        ],
        "Resource": "arn:aws:secretsmanager:*:*:secret:*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/AmazonEVSManaged": "true",
                "aws:ResourceTag/AmazonEVSManaged": "true"
            },
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "AmazonEVSManaged"
                ]
            }
        }
    },
    {
        "Sid": "SecretsManagerOps",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:DeleteSecret",
            "secretsmanager:GetSecretValue",
            "secretsmanager:UpdateSecret"
        ],
        "Resource": "arn:aws:secretsmanager:*:*:secret:*",
        "Condition": {
            "Null": {
                "aws:ResourceTag/AmazonEVSManaged": "false"
            }
        }
    },
    {
        "Sid": "SecretsManagerRandomPassword",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetRandomPassword"
        ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "EVSPermissions",
            "Effect": "Allow",
            "Action": [
                "evs:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyAccessInConsole",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:*:*:key/*"
        },

        {
            "Sid": "KMSKeyAliasAccess",
            "Effect": "Allow",
            "Action": [
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
}
```

Dapatkan dan daftarkan lingkungan Amazon EVS, host, dan VLANs

Kebijakan contoh ini mencakup izin minimum yang diperlukan administrator untuk mendapatkan dan mencantumkan semua lingkungan Amazon EVS, host, dan VLANs dalam akun tertentu di us-east-2. AWS Region

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "evs:Get*",
```

```
        "evs:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Memecahkan masalah identitas dan akses Amazon EVS

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Amazon EVS dan IAM.

Topik

- AccessDeniedException
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon EVS saya

AccessDeniedException

Jika Anda menerima `AccessDeniedException` saat memanggil operasi AWS API, kredenal utama IAM yang Anda gunakan tidak memiliki izin yang diperlukan untuk melakukan panggilan itu.

```
An error occurred (AccessDeniedException) when calling the CreateEnvironment operation:
User: arn:aws:iam::111122223333:user/user_name is not authorized to perform:
evs:CreateEnvironment on resource: arn:aws:evs:region:111122223333:environment/my-env
```

Dalam pesan contoh sebelumnya, pengguna tidak memiliki izin untuk memanggil operasi Amazon EVS `CreateEnvironment` API. Untuk memberikan izin admin Amazon EVS ke kepala sekolah IAM, lihat. the section called “Contoh kebijakan berbasis identitas Amazon EVS”

Untuk informasi lebih umum tentang IAM, lihat Mengontrol akses ke AWS sumber daya menggunakan kebijakan di Panduan Pengguna IAM.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon EVS saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis

sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Amazon EVS mendukung fitur-fitur ini, lihatthe section called "Bagaimana Amazon EVS bekerja dengan IAM".
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke sumber lain Akun AWS yang Anda miliki di Panduan Pengguna IAM. Pengguna IAM
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Memberikan Akses kepada Pengguna yang Diautentikasi Secara Eksternal (Federasi Identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM peran dari kebijakan berbasis sumber daya di Panduan Pengguna IAM.

AWS kebijakan terkelola untuk Amazon EVS

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 AWS terkelola di Panduan IAM Pengguna.

AWS kebijakan terkelola: Amazon EVSService RolePolicy

Anda tidak dapat melampirkan `AmazonEVSServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan Amazon EVS melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat the section called “Menggunakan Peran Terkait Layanan”. Saat Anda membuat lingkungan menggunakan prinsipal IAM yang memiliki `iam:CreateServiceLinkedRole` izin, peran `AWSServiceRoleforAmazonEVS` terkait layanan akan dibuat secara otomatis untuk Anda dengan kebijakan ini yang dilampirkan padanya.

Kebijakan ini memungkinkan peran `AWSServiceRoleForAmazonEVS` terkait layanan untuk memanggil Layanan AWS atas nama Anda.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan Amazon EVS menyelesaikan tugas-tugas berikut.

- `ec2`- Temukan komponen jaringan VPC, termasuk subnet dan. VPCs Buat, modifikasi, tag, dan hapus antarmuka jaringan elastis yang digunakan untuk membuat koneksi persisten antara Amazon EVS dan alat SDDC Manager VMware Virtual Cloud Foundation (VCF) di subnet VPC Anda. Konektivitas ini diperlukan untuk Amazon EVS untuk menyebarkan, mengelola, dan memantau penyebaran VCF.
- `ec2`- Hapus instans EC2 yang dibuat Amazon EVS saat Anda membuat permintaan penghapusan host EVS. Jelaskan dan modifikasi atribut instans EC2 sehingga penghentian instans EC2 default dan perlindungan penghentian dapat dinonaktifkan jika diperlukan untuk mendukung penghapusan host EVS.
- `ec2`- Kelola volume EBS untuk instalasi dan pembersihan Cloud Builder. Selama pembuatan lingkungan, Cloud Builder diinstal ke salah satu host yang digunakan Amazon EVS untuk melakukan perubahan konfigurasi VCF. Setelah selesai, Amazon EVS menghapus Cloud Builder dengan melepaskan dan menghapus volume EC2 tempat penyimpanannya.
- `ec2`- Hapus subnet EVS VLAN atas nama Anda jika Anda meminta penghapusan lingkungan.
- `secretsmanager`- Hapus kata sandi VCF yang dibuat dan disimpan Amazon EVS di AWS Secrets Manager selama pembuatan lingkungan. Amazon EVS menghapus semua rahasia yang dibuat layanan di akun Anda jika pembuatan lingkungan gagal, atau jika Anda meminta penghapusan lingkungan. Ambil kredensi vCenter dari AWS Secrets Manager ketika Anda mengkonfigurasi konektor vCenter dengan menyediakan ARN rahasia. Izin tersebut dicakup dengan kondisi tag sumber daya `EvsAccess=true` untuk memastikan Amazon EVS hanya mengakses rahasia yang ditandai secara eksplisit untuk akses Amazon EVS vCenter.

- `kms`- Dekripsi rahasia dan jelaskan kunci KMS ketika kredensil vCenter yang disimpan di Secrets Manager dienkripsi dengan kunci KMS. Izin dicakup dengan kondisi tag sumber daya `EvsAccess=true` untuk memastikan Amazon EVS hanya mengakses kunci KMS yang ditandai secara eksplisit untuk akses vCenter.
- `cloudwatch`- Publikasikan metrik AWS penggunaan CloudWatch untuk sumber daya Amazon EVS yang memiliki kuota.

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat Amazon EVSService RolePolicy di Panduan Referensi Kebijakan AWS Terkelola.

Amazon EVS memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon EVS sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman Riwayat dokumen.

Perubahan	Deskripsi	Date
Amazon EVSService RolePolicy - Kebijakan diperbarui	Amazon EVS memperbarui kebijakan untuk memungkinkan layanan mengambil kredenal vCenter dari AWS Secrets Manager dan mendekripsi rahasia yang dienkripsi dengan kunci KMS. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: Amazon EVSService RolePolicy”.	Maret 23, 2026
Amazon EVSService RolePolicy - Kebijakan diperbarui	Amazon EVS memperbarui kebijakan untuk menambahkan kemampuan manajemen sumber daya yang komprehensif termasuk manajemen instans EC2, operasi volume	Agustus 14, 2025

Perubahan	Deskripsi	Date
	EBS, dan integrasi AWS Secrets Manager. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: Amazon EVSService RolePolicy”.	
Amazon EVSService RolePolicy - Kebijakan diperbarui	Amazon EVS memperbarui kebijakan untuk mengizinkan layanan menghapus subnet EVS VLAN, serta mempublikasikan metrik penggunaan Amazon EVS. CloudWatch Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: Amazon EVSService RolePolicy”.	Juli 14, 2025
Amazon EVSService RolePolicy - Kebijakan baru ditambahkan	Amazon EVS menambahkan kebijakan baru yang memungkinkan layanan terhubung ke subnet VPC di akun pelanggan. Koneksi ini diperlukan untuk fungsionalitas layanan. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: Amazon EVSService RolePolicy”.	09 Juni 2025
Amazon EVS mulai melacak perubahan	Amazon EVS mulai melacak perubahan untuk kebijakan yang AWS dikelola.	09 Juni 2025

Menggunakan peran terkait layanan untuk Amazon EVS

Amazon Elastic VMware Service menggunakan peran AWS terkait layanan Identity and Access Management (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Amazon EVS. Peran terkait layanan telah ditentukan sebelumnya oleh Amazon EVS dan menyertakan semua izin yang diperlukan layanan untuk memanggil layanan lain AWS atas nama Anda.

Peran terkait layanan membuat pengaturan Amazon EVS lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon EVS mendefinisikan izin peran terkait layanannya, dan kecuali ditentukan lain, hanya Amazon EVS yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Amazon EVS Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran terkait layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Amazon EVS

Amazon EVS menggunakan peran terkait layanan bernama. `AWSServiceRoleForAmazonEVS` Peran ini memungkinkan Amazon EVS mengelola lingkungan di akun Anda. Kebijakan terlampir memungkinkan peran untuk mengelola sumber daya berikut: antarmuka jaringan elastis EVS, subnet EVS VLAN, host EVS, dan metrik. VPCs CloudWatch

Peran tertaut layanan `AWSServiceRoleForAmazonEVS` memercayai layanan berikut untuk mengambil peran tersebut:

- `evs.amazonaws.com`

Kebijakan izin peran memungkinkan Amazon EVS menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Amazon EVSService RolePolicy

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Amazon EVS

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat lingkungan di Konsol Manajemen AWS, AWS CLI, atau AWS API, Amazon EVS membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat lingkungan, Amazon EVS membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Amazon EVS

Amazon EVS tidak mengizinkan Anda mengedit peran `AWSServiceRoleForAmazonEVS` 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 Amazon EVS

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan dan tidak dipantau atau dipelihara secara aktif. Namun, Anda harus membersihkan peran tertaut layanan terlebih dahulu sebelum dapat menghapusnya secara manual.

Membersihkan peran tertaut-layanan

Sebelum dapat menggunakan IAM untuk menghapus peran tertaut-layanan, Anda harus terlebih dahulu menghapus semua sumber daya yang digunakan oleh peran tersebut. Untuk langkah-langkah menghapus lingkungan Amazon EVS dengan host, lihatthe section called “Hapus host dan lingkungan Amazon EVS”.

> **Note**
>
> Jika layanan Amazon EVS menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran terkait layanan secara manual

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan`AWSServiceRoleForAmazonEVS`. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Wilayah yang didukung untuk peran terkait layanan Amazon EVS

Amazon EVS mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat titik akhir dan kuota Amazon Elastic VMware Service di Panduan Referensi AWS Umum.

Ketahanan di Amazon EVS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung melalui latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Lingkungan Amazon EVS tersedia dalam satu AWS Availability Zone. Untuk memastikan ketersediaan infrastruktur Amazon EVS Single-AZ yang tinggi, Amazon EVS menawarkan fitur-fitur berikut:

> **Note**
>
> Amazon EVS hanya mendukung penerapan Single-AZ saat ini.

- Amazon EVS mendukung penggunaan AWS Elastic Disaster Recovery untuk mengotomatiskan pencadangan dan pemulihan data Anda.
- Amazon EVS menyebarkan cluster NSX Edge dengan dua node Active/Standby NSX Edge per persyaratan VCF. Node NSX Edge berjalan pada host yang berbeda untuk memastikan ketersediaan tinggi dan memungkinkan failover cepat jika node NSX Edge gagal.
- Amazon EVS menerapkan lingkungan minimal empat host ESX, yang dibutuhkan VCF. Host tambahan dapat ditambahkan pasca-penyebaran. Ini adalah persyaratan VMware desain untuk memastikan kuorum vSAN yang tepat dan menjaga ketersediaan selama operasi pemeliharaan dan kegagalan host. Untuk informasi selengkapnya, lihat Desain Cluster vSphere untuk VMware Cloud Foundation di dokumentasi VMware Cloud Foundation.
- Amazon EVS mendukung penggunaan grup penempatan EC2 partisi atau grup penempatan cluster untuk EC2 host. Grup penempatan partisi menyebarkan EC2 instance Anda di seluruh partisi logis sehingga grup instance dalam satu partisi tidak berbagi perangkat keras yang mendasarinya dengan grup instance di partisi yang berbeda. Strategi ini membantu mengurangi kemungkinan kegagalan perangkat keras yang berkorelasi untuk beban kerja terdistribusi yang besar. Grup penempatan cluster digunakan untuk menempatkan EC2 instans Anda dalam rak fisik yang sama untuk memastikan latecy rendah. Untuk informasi selengkapnya, lihat Grup penempatan partisi di Panduan Amazon EC2 Pengguna.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

VMware ketahanan komponen

Pelanggan Amazon EVS bertanggung jawab untuk mengonfigurasi VMware komponen yang berjalan di Amazon EVS untuk memastikan ketersediaan mesin virtual (VMs) dan ketahanan beban kerja Anda yang tinggi.

Amazon EVS mendukung fitur ketahanan VMware Cloud Foundation (VCF) berikut:

- VSphere replikasi - Menyediakan replikasi asinkron berbasis host untuk pemulihan bencana dan tujuan migrasi beban kerja. VMs Untuk informasi selengkapnya, lihat Cara Kerja Replikasi vSphere dalam dokumentasi Replikasi vSphere VMware .
- Perlindungan data vSan - Memungkinkan Anda untuk dengan cepat pulih VMs dari kegagalan operasional untuk serangan ransomware, menggunakan snapshot asli yang disimpan secara lokal di cluster vSAN. Untuk informasi selengkapnya, lihat Menggunakan Perlindungan Data vSAN dalam dokumentasi vSAN.

- vSphere HA - Menyediakan failover otomatis untuk VMs jika terjadi kegagalan host. Untuk informasi selengkapnya, lihat Desain Ketersediaan Tinggi untuk vCenter Server for VMware Cloud Foundation dalam dokumentasi VCF.
- vSphere Fault Tolerance (FT) - Menyediakan ketersediaan berkelanjutan untuk mission-critical VMs dengan membuat dan memelihara VM lain yang identik dan terus tersedia untuk menggantikannya jika terjadi situasi failover. Untuk informasi selengkapnya, lihat Cara Kerja Fault Tolerance dalam dokumentasi vSphere.
- vSan Failure to Tolerance (FTT) - Pengaturan vSAN yang menentukan berapa banyak kegagalan host yang dapat ditahan oleh VM sebelum menjadi tidak dapat diakses. Ini mendefinisikan tingkat redundansi dan toleransi kesalahan untuk mesin virtual Anda dalam cluster vSAN. Untuk informasi selengkapnya, lihat Menoleransi Kegagalan Tambahan dengan Domain Kesalahan di Cluster vSAN dalam dokumentasi vSAN.

Menggunakan Amazon EVS dengan layanan lain AWS

Amazon EVS terintegrasi dengan yang lain Layanan AWS untuk memberikan solusi tambahan. Topik ini mengidentifikasi beberapa layanan yang digunakan Amazon EVS untuk menambahkan fungsionalitas.

Topik

Buat sumber daya Amazon EVS dengan AWS CloudFormation

Amazon EVS terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan menyiapkan AWS sumber daya sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan, lingkungan Amazon EVS misalnya, dan AWS CloudFormation menangani penyediaan dan konfigurasi sumber daya tersebut untuk Anda.

Saat Anda menggunakan AWS CloudFormation, Anda dapat menggunakan kembali template Anda untuk menyiapkan sumber daya Amazon EVS Anda secara konsisten dan berulang kali. Cukup jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

Amazon EVS dan template AWS CloudFormation

Untuk menyediakan dan mengonfigurasi sumber daya untuk Amazon EVS dan layanan terkait, Anda harus memahami AWS CloudFormation templat. Templat adalah file teks dengan format JSON atau YAML. Template ini menjelaskan sumber daya yang ingin Anda sediakan di AWS CloudFormation tumpukan Anda. Jika Anda tidak terbiasa dengan JSON atau YAMAL, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan template. AWS CloudFormation Untuk informasi lebih lanjut, lihat Apa itu AWS CloudFormation Desainer? dalam AWS CloudFormation User Guide.

Amazon EVS mendukung pembuatan lingkungan di AWS CloudFormation. Untuk informasi selengkapnya, termasuk contoh templat JSON dan YAMAL untuk lingkungan Anda, lihat referensi jenis sumber daya Amazon EVS di Panduan Pengguna. AWS CloudFormation

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormation Panduan Pengguna
- AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah

Jalankan beban kerja berkinerja tinggi dengan Amazon FSx untuk ONTAP NetApp

Amazon FSx untuk NetApp ONTAP adalah layanan penyimpanan yang memungkinkan Anda meluncurkan dan menjalankan sistem file ONTAP yang dikelola sepenuhnya di cloud. ONTAP NetApp adalah teknologi sistem file yang menyediakan serangkaian akses data dan kemampuan manajemen data yang diadopsi secara luas. FSx untuk ONTAP menyediakan fitur, kinerja, dan APIs sistem NetApp file lokal dengan kelincahan, skalabilitas, dan kesederhanaan layanan yang dikelola sepenuhnya. AWS Untuk informasi selengkapnya, lihat Panduan Pengguna ONTAP FSx untuk.

Amazon EVS mendukung penggunaan Amazon FSx untuk NetApp ONTAP sebagai NFS/iSCSI datastore dan sebagai penyimpanan yang terhubung dengan tamu untuk mesin virtual VMware yang berjalan di Amazon EVS.

Konfigurasikan FSx untuk NetApp ONTAP sebagai datastore NFS

Prosedur berikut merinci langkah-langkah minimum yang diperlukan FSx untuk mengonfigurasi NetApp ONTAP sebagai datastore NFS untuk Amazon EVS menggunakan FSx konsol dan antarmuka klien VMware vSphere yang berjalan di Amazon EVS.

Prasyarat

Sebelum Anda menggunakan Amazon EVS dengan Amazon FSx untuk NetApp ONTAP, pastikan bahwa tugas prasyarat berikut telah selesai.

- Lingkungan Amazon EVS diterapkan di Virtual Private Cloud (VPC) Anda. Untuk informasi selengkapnya, lihat Mulai menggunakan.
- Anda memiliki akses ke klien vSphere Anda yang berjalan di Amazon EVS.

- Anda atau admin penyimpanan Anda harus memiliki izin yang diperlukan untuk membuat dan mengelola FSx sistem file ONTAP di VPC Anda. Untuk informasi selengkapnya, lihat Identitas dan manajemen akses untuk Amazon FSx untuk NetApp ONTAP.

Prinsipal IAM Anda memiliki izin yang sesuai untuk membuat dan mengelola FSx sistem file ONTAP di VPC Anda. Untuk informasi selengkapnya, lihat the section called “Membuat dan mengelola lingkungan Amazon EVS”.

Buat FSx untuk sistem file NetApp ONTAP

1. Pergi ke FSx konsol Amazon.
2. Pilih Buat sistem file.
3. Pilih Amazon FSx untuk NetApp ONTAP.
4. Pilih Berikutnya.
5. Pilih Standar buat.
6. Untuk jenis Deployment, pilih opsi penerapan Single-AZ.

> **Note**
>
> Amazon EVS hanya mendukung penerapan Single-AZ saat ini.

7. Untuk kapasitas penyimpanan SSD, tentukan 1024 GiB.
8. Untuk kapasitas Throughput, pilih Tentukan kapasitas throughput. Pilih setidaknya 512 MB/s untuk Single-AZ 1 atau setidaknya 768 MB/s untuk Single-AZ 2.
9. Pilih VPC Amazon EVS yang memiliki konektivitas ke subnet Amazon EVS VLAN Anda.
10. Pilih grup keamanan yang mengizinkan semua yang diperlukan FSx untuk lalu lintas NFS ONTAP ke subnet VLAN manajemen host VMkernel Amazon EVS.
11. Pilih subnet akses layanan Amazon EVS tempat sistem file Anda akan digunakan. Untuk informasi selengkapnya, lihat the section called “Subnet akses layanan”.
12. Untuk jalur Junction, tentukan nama yang bermakna seperti `/vol1` untuk mengidentifikasi volume ini di vSphere.
13. Dalam konfigurasi volume Default, atur efisiensi Penyimpanan ke Diaktifkan.
14. Biarkan pengaturan yang tersisa pada nilai defaultnya dan pilih Berikutnya.
15. Tinjau atribut sistem file dan pilih Buat sistem file.

Ambil nama DNS NFS untuk mesin virtual penyimpanan

1. Pergi ke FSx konsol Amazon.
2. Di menu sebelah kiri, pilih Sistem file.
3. Pilih sistem file yang baru dibuat.
4. Pilih tab Storage Virtual Machines.
5. Pilih mesin virtual penyimpanan.
6. Pilih tab Endpoints.
7. Salin nama DNS sistem file jaringan (NFS) untuk digunakan nanti di VMware Vsphere.

Buat datastore NFS di vSphere menggunakan volume untuk ONTAP FSx

Ikuti petunjuk di Buat Datastore NFS di Lingkungan vSphere untuk mengonfigurasi Amazon untuk NetApp ONTAP sebagai penyimpanan eksternal FSx untuk vSphere. VMware Untuk pengaturan Server di antarmuka klien vSphere, gunakan nama DNS NFS mesin virtual penyimpanan (SVM) yang Anda salin pada langkah sebelumnya.

Konfigurasikan FSx untuk NetApp ONTAP FSx sebagai datastore iSCSI

Prosedur berikut merinci langkah-langkah minimum yang diperlukan FSx untuk mengonfigurasi NetApp ONTAP sebagai datastore iSCSI untuk Amazon EVS menggunakan konsol VMware dan antarmuka klien vSphere FSx yang berjalan di Amazon EVS.

Prasyarat

Sebelum Anda menggunakan Amazon EVS dengan Amazon FSx untuk NetApp ONTAP, pastikan bahwa tugas prasyarat berikut telah selesai.

- Lingkungan Amazon EVS diterapkan di Virtual Private Cloud (VPC) Anda. Untuk informasi selengkapnya, lihat Mulai menggunakan.
- Anda memiliki akses ke klien vSphere Anda yang berjalan di Amazon EVS.
- Anda atau admin penyimpanan Anda harus memiliki izin yang diperlukan untuk membuat dan mengelola FSx sistem file ONTAP di VPC Anda. Untuk informasi selengkapnya, lihat Identitas dan manajemen akses untuk Amazon FSx untuk NetApp ONTAP.

Buat FSx untuk sistem file NetApp ONTAP

1. Pergi ke FSx konsol Amazon.
2. Pilih Buat sistem file.
3. Pilih Amazon FSx untuk NetApp ONTAP.
4. Pilih Berikutnya.
5. Pilih Standar buat.
6. Untuk jenis Deployment, pilih opsi penerapan Single-AZ.

> **Note**
>
> Amazon EVS hanya mendukung penerapan Single-AZ saat ini.

7. Untuk kapasitas penyimpanan SSD, tentukan 1024 GiB.
8. Untuk kapasitas Throughput, pilih Tentukan kapasitas throughput. Pilih setidaknya 512 MB/s untuk Single-AZ 1 atau setidaknya 768 MB/s untuk Single-AZ 2.
9. Pilih VPC Amazon EVS yang memiliki konektivitas ke subnet Amazon EVS VLAN Anda.
10. Pilih grup keamanan yang mengizinkan semua yang diperlukan FSx untuk lalu lintas ONTAP iSCSI ke subnet VLAN manajemen host Amazon EVS. VMkernel
11. Pilih subnet akses layanan Amazon EVS tempat sistem file Anda akan digunakan. Untuk informasi selengkapnya, lihat the section called “Subnet akses layanan”.
12. Dalam konfigurasi volume Default, atur efisiensi Penyimpanan ke Diaktifkan.
13. Biarkan pengaturan yang tersisa pada nilai default mereka dan pilih Berikutnya.
14. Tinjau atribut sistem file dan pilih Buat sistem file.

Konfigurasikan adaptor iSCSI perangkat lunak di vSphere untuk penyimpanan host ESX

Untuk setiap host ESX, Anda harus mengkonfigurasi adaptor iSCSI perangkat lunak sehingga host ESX Anda dapat menggunakannya untuk mengakses penyimpanan iSCSI. Untuk instruksi untuk mengkonfigurasi adaptor iSCSI perangkat lunak untuk host ESX di vSphere, lihat Menambahkan atau Menghapus Adaptor iSCSI Perangkat Lunak dalam dokumentasi produk vSphere. VMware

Setelah Anda mengonfigurasi adaptor iSCSI perangkat lunak, salin iSCSI Qualified Name (IQN) yang terkait dengan adaptor iSCSI. Nilai-nilai ini akan digunakan nanti.

Buat iSCSI LUN

FSx untuk ONTAP memungkinkan Anda membuat Logical Unit Numbers (LUNs) yang secara khusus ditujukan untuk akses iSCSI, menyediakan penyimpanan blok bersama ke host ESX Anda. Anda menggunakan CLI NetApp ONTAP untuk membuat LUN.

Di bawah ini adalah contoh perintah.

> **Note**
>
> Disarankan untuk mengkonfigurasi ukuran LUN hingga 90% dari ukuran volume.

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

Untuk informasi selengkapnya, lihat Membuat LUN iSCSI di Panduan Pengguna untuk FSx ONTAP.

Konfigurasikan dan petakan grup inisiator ke iSCSI LUN

Sekarang Anda telah membuat ISCSI LUN, langkah selanjutnya dalam proses ini adalah membuat grup inisiator `igroup` () untuk menghubungkan volume ke cluster dan memetakan LUN ke grup inisiator. Anda menggunakan CLI NetApp ONTAP untuk melakukan tindakan ini.

1. Konfigurasikan grup inisiator.

   Di bawah ini adalah contoh perintah. Untuk`--initiator`, gunakan IQNs adaptor iSCSI yang Anda salin pada langkah sebelumnya.

   ```
   igroup create <svm_name> \
   -igroup <initiator_group_name> \
   -protocol iscsi \
   -ostype vmware \
   -initiator <esxi_iqn_1>,<esxi_iqn_2>,<esxi_iqn_3>,<esxi_iqn_4>
   ```

2. Konfirmasikan bahwa `igroup` ada.

   ```
   lun igroup show
   ```

3. Petakan LUN ke grup inisiator. Di bawah ini adalah contoh perintah.

```
lun mapping create -vserver <svm_name> \
-path /vol/<vol_name>/<lun_name> \
-igroup <initiator_group_name> \
-lun-id <scsi_lun_number_for this_datastore>
```

4. Gunakan `lun show -path` perintah untuk mengonfirmasi bahwa LUN dibuat, online, dan dipetakan.

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

Untuk informasi selengkapnya, lihat Penyediaan iSCSI untuk Linux atau Penyediaan iSCSI untuk Windows di Panduan Pengguna ONTAP. FSx

Konfigurasikan penemuan dinamis iSCSI LUN di vSphere

Untuk memungkinkan host ESX melihat iSCSI LUN, Anda harus mengonfigurasi penemuan dinamis untuk setiap host di antarmuka klien vSphere. Untuk bidang server iSCSI, masukkan nama DNS (NFS) yang Anda salin pada langkah sebelumnya. Untuk informasi selengkapnya, lihat Mengkonfigurasi Penemuan Dinamis atau Statis untuk iSCSI dan iSer di ESX Host dalam VMware dokumentasi produk vSphere.

Buat Datastore VMFS di VMware vSphere menggunakan iSCSI LUN

Datastores Virtual Machine File System (VMFS) berfungsi sebagai repositori untuk mesin virtual. VMware Ikuti instruksi di Create a vSphere VMFS Datastore untuk mengatur datastore VMFS di vSphere menggunakan iSCSI LUN yang sebelumnya Anda konfigurasikan. VMware

Pemecahan Masalah

Bab ini merinci beberapa masalah umum yang dihadapi saat membuat atau mengelola lingkungan Amazon EVS.

Memecahkan masalah pemeriksaan status lingkungan yang gagal

Amazon EVS melakukan pemeriksaan otomatis pada lingkungan Anda untuk mengidentifikasi masalah. Anda dapat melihat status lingkungan Anda untuk mengidentifikasi masalah tertentu yang dapat dideteksi.

Tinjau informasi pemeriksaan status lingkungan

Untuk menyelidiki lingkungan yang terganggu menggunakan konsol Amazon EVS

1. Buka konsol Amazon EVS.
2. Di panel navigasi, pilih Lingkungan, lalu pilih lingkungan Anda.
3. Pilih tab Detail untuk melihat ikhtisar lingkungan.
4. Periksa status Lingkungan. Arahkan kursor ke bidang ini untuk memperluas popover dengan hasil individual untuk setiap pemeriksaan status lingkungan.

Pemeriksaan jangkauan gagal

Pemeriksaan jangkauan memverifikasi bahwa Amazon EVS memiliki koneksi persisten ke Manajer SDDC. Jika Amazon EVS tidak dapat menjangkau lingkungan, pemeriksaan ini akan gagal.

Jika pemeriksaan ini gagal, Amazon EVS tidak dapat lagi menjangkau SDDC Manager untuk memvalidasi status lingkungan, dan host tidak dapat lagi ditambahkan ke lingkungan. Kegagalan jangkauan juga akan menyebabkan gagalnya penggunaan ulang kunci lisensi serta pemeriksaan cakupan kunci, dan pemeriksaan jumlah host akan memunculkan respons Tidak diketahui).

Untuk memastikan jangkauan, periksa hal berikut:

- Pastikan sertifikat Anda valid dan belum kedaluwarsa. Anda dapat menggunakan SDDC Manager UI atau klien vSphere untuk mengelola sertifikat dalam lingkungan VCF. Setelah penerapan, Anda disarankan untuk mengganti semua sertifikat domain manajemen VMware Cloud Foundation.

Untuk informasi selengkapnya, lihat Mengelola Sertifikat di VMware Cloud Foundation di dokumentasi VMware Cloud Foundation.

- Pastikan server DNS Anda dapat dijangkau dari subnet akses layanan, catatan DNS valid, dan tidak ada nama host duplikat atau alamat IP.
- Jika Anda ingin membuat aturan firewall Anda sendiri, ikuti panduan ini:
  - Izinkan TCP/UDP akses ke server DNS.
  - Izinkan HTTPS/SSH akses ke subnet VLAN manajemen host.
  - Izinkan HTTPS/SSH akses ke subnet VM VLAN Manajemen.

Jika Anda masih tidak dapat menyelesaikan masalah setelah mengikuti panduan ini, kami sarankan Anda menghubungi AWS Support untuk bantuan lebih lanjut.

Pemeriksaan jumlah host gagal

Pemeriksaan ini memverifikasi bahwa lingkungan Anda memiliki minimal empat host, yang merupakan persyaratan untuk VCF 5.2.x.

Jika pemeriksaan ini gagal, Anda perlu menambahkan host agar lingkungan Anda memenuhi persyaratan minimum ini. Amazon EVS hanya mendukung lingkungan dengan 4 hingga 16 host.

Pemeriksaan penggunaan kembali kunci gagal

Pemeriksaan ini memverifikasi bahwa kunci lisensi VCF tidak digunakan oleh lingkungan Amazon EVS lainnya. Lisensi VCF dapat digunakan hanya untuk satu lingkungan Amazon EVS. Pemeriksaan ini gagal jika Anda menyediakan kunci lisensi VCF dalam permintaan pembuatan lingkungan yang sudah digunakan oleh lingkungan lain.

Jika pemeriksaan ini gagal, Anda akan menerima respons kesalahan bahwa lingkungan Amazon EVS tidak dapat dibuat. Untuk mengatasi masalah ini, tinjau pengaturan lisensi Anda di SDDC Manager dan ganti lisensi yang sudah digunakan dengan lisensi yang belum digunakan.

> **Important**
>
> Gunakan antarmuka pengguna SDDC Manager untuk mengelola solusi VCF dan kunci lisensi vSAN. Amazon EVS mengharuskan Anda mempertahankan solusi VCF yang valid dan kunci lisensi vSAN di SDDC Manager agar layanan berfungsi dengan baik. Meskipun kunci harus ditetapkan ke host dan kluster vSAN Anda menggunakan Klien vSphere, Anda harus

memastikan bahwa kunci tersebut juga muncul di layar lisensi antarmuka pengguna SDDC Manager.

Pemeriksaan cakupan kunci gagal

Pemeriksaan ini memverifikasi bahwa kunci lisensi VCF yang ditetapkan ke vCenter Server mengalokasikan jumlah core vCPU dan kapasitas penyimpanan vSAN (TiB) yang mencukupi untuk semua host yang di-deploy.

Jika pemeriksaan ini gagal, Anda akan menerima respons kesalahan bahwa lingkungan Amazon EVS tidak dapat dibuat. Kegagalan cakupan kunci dapat mengindikasikan salah satu masalah berikut:

- Lisensi VCF tidak ditetapkan dengan benar ke vCenter Server. Anda harus menetapkan lisensi ke vCenter Server sebelum periode evaluasinya berakhir atau lisensi yang saat ini ditetapkan berakhir. Jika ini masalahnya, tinjau penetapan lisensi di SDDC Manager.
- Lisensi VCF saat ini tidak mencakup inti vCPU dan kebutuhan kapasitas penyimpanan vSAN. Kunci solusi VCF harus memiliki setidaknya 256 core. Kunci lisensi vSAN harus memiliki setidaknya 110 TiB kapasitas vSAN. Jika ini masalahnya, tambahkan lisensi vSAN di SDDC Manager hingga kebutuhan penggunaan Anda terpenuhi.

Jika tindakan di atas tidak menyelesaikan masalah, hubungi AWS Support untuk bantuan lebih lanjut.

⚠ Important

Gunakan antarmuka pengguna SDDC Manager untuk mengelola solusi VCF dan kunci lisensi vSAN. Amazon EVS mengharuskan Anda mempertahankan solusi VCF yang valid dan kunci lisensi vSAN di SDDC Manager agar layanan berfungsi dengan baik. Meskipun kunci harus ditetapkan ke host dan kluster vSAN Anda menggunakan Klien vSphere, Anda harus memastikan bahwa kunci tersebut juga muncul di layar lisensi antarmuka pengguna SDDC Manager.

Agen vSphere HA di host ini tidak dapat mencapai alamat isolasi

Di antarmuka pengguna vCenter, dengan host ESX dipilih, Anda melihat pesan “agen vSphere HA pada host ini tidak dapat mencapai alamat isolasi < alamat>”. IPv6

Pesan kesalahan ini menunjukkan bahwa agen vSphere HA pada host tidak dapat mencapai alamat IPv6 isolasi default yang digunakan vSphere HA untuk pemeriksaan detak jantung. Pesan kesalahan tidak menunjukkan masalah, dan hanya terjadi karena Amazon EVS tidak mendukung IPv6 saat ini. Tidak adanya IPV6 dukungan untuk Amazon EVS tidak mempengaruhi fungsionalitas inti vSphere HA.

Prakecek peningkatan vSan gagal untuk cluster host ESX

Saat mencoba memutakhirkan cluster host ESX menggunakan SDDC Manager, precheck terkait disk vSAN mungkin gagal. Ini karena Amazon EVS menggunakan VSAN Express Storage Architecture (ESA), dan precheck upgrade tidak berlaku untuk vSAN ESA. Untuk informasi lebih lanjut, lihat artikel basis pengetahuan Broadcom tentang topik ini.

Tambahkan kegagalan host karena gambar cluster yang tidak kompatibel

Masalah

Saat Anda menambahkan host ke lingkungan Anda, host memiliki versi terbaru dari add-on vendor khusus EVS yang tersedia. Jika lingkungan Anda menggunakan host dengan versi add-on yang lebih lama, menambahkan host baru gagal dengan kesalahan bahwa host baru tidak kompatibel dengan gambar cluster Anda. Untuk memperbaiki masalah ini, Anda harus menggunakan vSphere Lifecyle Manager untuk mengekstrak versi add-on terbaru yang tersedia dari host yang baru ditambahkan.

Solusi

Ikuti langkah-langkah ini.

1. Pergi ke inventaris Host dan Cluster di VMware vCenter Server.
2. Ekstrak add-on dari host yang baru ditambahkan dengan membuat cluster kosong sementara.
3. Di bawah Dasar-dasar, pilih Impor gambar dari host yang ada di Inventaris vCenter dan buat cluster. Biarkan semua pengaturan lainnya sebagai default.
4. Setelah cluster sementara ini dibuat dengan gambar yang diekstraksi, Anda dapat menghapus cluster sementara. Add-on sekarang akan tersedia di depot vSphere Lifecycle Manager Anda.
5. Buka kluster lingkungan Anda dan pilih tab Pembaruan.
6. Edit gambar cluster Anda dan ubah versi add-on ke versi yang baru diekstraksi.

7. Pilih Simpan.
8. Di SDDC Manager, coba lagi tugas add host yang gagal. Ini akan memulihkan host cluster Anda, memperbarui semua host ke versi add-on terbaru. Remediasi gambar cluster akan membutuhkan reboot host.

Manajer SDDC gagal validasi host VCF selama komisioning host

Masalah

Jika Anda telah memperbarui versi ESX Anda setelah penerapan lingkungan Amazon EVS, manajer SDDC mungkin gagal selama validasi host VCF di langkah host komisi. Untuk memperbaiki masalah ini, Anda harus menggunakan vSphere Lifecyle Manager untuk meningkatkan ESX pada host yang baru ditambahkan.

Solusi

Ikuti langkah-langkah ini.

> **Important**
>
> Langkah-langkah ini memerlukan sementara menambahkan host ke vCenter di luar SDDC Manager. Menggunakan vSphere Lifecyle Manager untuk operasi apa pun selain peningkatan ESX dapat membuat host Anda tidak dapat digunakan, dan mengharuskan Anda untuk menghapus dan membuat host Amazon EVS baru.

1. Pergi ke inventaris Host dan Cluster di VMware vCenter Server.
2. Tambahkan host sementara ke pusat data virtual Anda, pastikan untuk memilih kelola host dengan gambar. Host akan dihapus pada langkah selanjutnya setelah peningkatan ESX selesai. Untuk informasi selengkapnya, lihat Cara Menambahkan Host ke Pusat Data atau Folder vSphere Anda di dokumentasi vSphere.
3. Setelah host ditambahkan ke vSphere, tingkatkan versi ESX pada host. Ini dapat dilakukan di tab Pembaruan host Anda. Edit gambar host agar sesuai dengan versi ESX cluster Anda.
4. Setelah upgrade selesai, hapus host dari inventaris vCenter Anda. Untuk informasi selengkapnya, lihat Cara Menghapus Host ESX dari Instance Server vCenter Anda di dokumentasi vSphere.
5. Komisi host Anda di manajer SDDC. Untuk informasi selengkapnya, lihat Host Komisi di dokumentasi VMware Cloud Foundation.

6. Setelah host ditugaskan, tambahkan host ke cluster Anda menggunakan SDDC Manager.

Mencatat panggilan Amazon EVS API menggunakan AWS CloudTrail

Amazon EVS terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna IAM, peran IAM, atau layanan AWS di Amazon EVS. CloudTrail menangkap semua panggilan AWS API untuk Amazon EVS sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Amazon EVS dan panggilan kode ke operasi Amazon EVS API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Amazon EVS. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Amazon EVS, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

> **Note**
>
> Amazon EVS tidak mencatat aktivitas pengguna untuk AWS non-komponen, seperti aktivitas dalam lingkungan VCF Anda. Aktivitas ini dicatat di berbagai VMware konsol seperti vSphere dan NSX Manager.
> Jika pencatatan VCF terpusat diinginkan, Anda dapat mengonfigurasi solusi pemantauan VCF seperti Operasi VMware Cloud Foundation untuk mencapai hasil ini.

Informasi Amazon EVS di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Amazon EVS, 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 AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Amazon EVS, 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
- Menerima file CloudTrail log dari beberapa akun

Semua tindakan Amazon EVS dicatat oleh CloudTrail dan didokumentasikan dalam Referensi Amazon EVS API. Misalnya, panggilan ke`CreateEnvironment`, `GetEnvironment` dan `DeleteEnvironment` 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 dibuat dengan root atau kredensi pengguna AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log Amazon EVS

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.

Kuota layanan Amazon EVS

Amazon EVS telah terintegrasi dengan Service Quotas, Layanan AWS sebuah yang dapat Anda gunakan untuk melihat dan mengelola kuota Anda dari lokasi pusat. Untuk informasi selengkapnya, lihat Apa itu Service Quotas? di Panduan Pengguna Service Quotas.

Dengan integrasi Service Quotas, Anda dapat menggunakan Konsol Manajemen AWS atau AWS CLI untuk mencari nilai kuota Amazon EVS Anda dan meminta peningkatan kuota untuk kuota yang dapat disesuaikan. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota dalam Panduan Pengguna Service Quotas request-service-quota-increasehttps://docs.aws.amazon.com/cli/latest/reference/service-quotas/request-service-quota-increase.html dan di AWS CLI Referensi Perintah.

Untuk informasi selengkapnya tentang kuota layanan Amazon EVS, lihat kuota Amazon EVS di Panduan Referensi Umum. AWS

Important

Pastikan kuota Instans Standar EC2 Menjalankan Sesuai Permintaan mencerminkan jumlah v CPUs yang Anda perlukan untuk semua EC2 instans yang akan Anda gunakan di Amazon EVS. Setiap instance i4i.metal menggunakan 128 v. CPUs Untuk informasi tentang meningkatkan kuota EC2 layanan, lihat Meminta peningkatan dalam Panduan EC2 Pengguna Amazon.

Note

Jika Anda berencana untuk menggunakan Host EC2 Khusus untuk lingkungan Amazon EVS Anda, pastikan bahwa kuota Host i4i EC2 Khusus Anda mencerminkan jumlah Host Khusus yang ingin Anda gunakan untuk Wilayah yang diinginkan. Untuk informasi tentang meningkatkan kuota EC2 layanan, lihat Meminta peningkatan dalam Panduan EC2 Pengguna Amazon.

> **Note**
>
> Jika mengonfigurasi konektivitas internet HCX, kuota IPAM Anda untuk panjang netmask blok CIDR publik IPv4 bersebelahan yang disediakan Amazon harus/28 atau lebih besar. Untuk informasi selengkapnya, lihat Kuota untuk IPAM Anda.

> **Note**
>
> Amazon CloudWatch mengumpulkan metrik AWS penggunaan untuk sumber daya Amazon EVS yang memiliki kuota (lingkungan dan host). Untuk informasi selengkapnya, lihat Metrik CloudWatch Penggunaan di Panduan CloudWatch Pengguna Amazon.

Lihat kuota layanan Amazon EVS di Konsol Manajemen AWS

1. Buka Konsol Service Quotas.
2. Di panel navigasi kiri, pilih AWS layanan.
3. Dari daftar AWS layanan, cari dan pilih Amazon Elastic VMware Service.
4. Pilih Lihat kuota.

   Dalam daftar Kuota layanan, Anda dapat melihat nama kuota layanan, nilai yang diterapkan (jika tersedia), kuota AWS default, dan apakah nilai kuota dapat disesuaikan.
5. Untuk melihat informasi tambahan tentang service quotas, seperti deskripsi, pilih nama kuota.
6. (Opsional) Untuk meminta kenaikan kuota, pilih kuota yang ingin Anda tingkatkan, pilih Permintaan kenaikan di tingkat akun, masukkan atau pilih informasi yang diperlukan, dan pilih Permintaan.

Untuk bekerja lebih lanjut dengan kuota layanan menggunakan Konsol Manajemen AWS, lihat Panduan Pengguna Service Quotas. Untuk meminta peningkatan kuota, lihat Meminta Peningkatan Kuota dalam Panduan Pengguna Service Quotas.

Lihat kuota layanan Amazon EVS dengan CLI AWS

Jalankan perintah berikut untuk melihat kuota Amazon EVS Anda.

```
aws service-quotas list-aws-default-service-quotas \
```

```
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code evs \
    --output table
```

> **Note**
>
> Kuota yang dikembalikan adalah jumlah lingkungan Amazon EVS atau host yang dapat dibuat di akun ini di Wilayah saat AWS ini.

Untuk bekerja lebih banyak dengan kuota layanan menggunakan CLI, lihat AWS kuota layanan di AWS Referensi Perintah CLI. Untuk meminta peningkatan kuota, lihat request-service-quota-increaseperintah di Referensi Perintah AWS CLI.

Riwayat dokumen untuk Panduan Pengguna Amazon Elastic VMware Service

Tabel berikut menjelaskan rilis dokumentasi untuk Amazon Elastic VMware Service.

Perubahan	Deskripsi	Tanggal
Amazon yang Diperbarui EVSService RolePolicy	Amazon EVS telah memperbarui kebijakan terkelola `AmazonEVSServiceRolePolicy` untuk memungkinkan layanan mengambil kredenal vCenter dari AWS Secrets Manager dan mendekripsi rahasia yang dienkripsi dengan kunci KMS yang dikelola pelanggan.	Maret 23, 2026
Amazon yang Diperbarui EVSService RolePolicy	Amazon EVS telah memperbarui kebijakan terkelola `AmazonEVSServiceRolePolicy` untuk menambahkan kemampuan manajemen sumber daya yang komprehensif termasuk manajemen instans EC2, operasi volume EBS, dan integrasi AWS Secrets Manager. Untuk selengkapnya, lihat Pembaruan Amazon EVS ke kebijakan AWS terkelola.	Agustus 14, 2025
Amazon yang Diperbarui EVSService RolePolicy	Memperbarui kebijakan AWS terkelola Amazon EVSServiceRolePolicy.	Agustus 4, 2025

Merilis jumlah lingkungan per AWS kuota akun	Amazon EVS merilis jumlah lingkungan per kuota AWS akun. Jumlah lingkungan per kuota AWS akun mewakili jumlah maksimum lingkungan Amazon EVS yang dapat dibuat di akun dan Wilayah tertentu.	Juli 8, 2025
Amazon EVS dirilis di Wilayah Eropa (Irlandia)	Amazon EVS dirilis di Wilayah Eropa (Irlandia).	Juni 18, 2025
Merilis Amazon EVSService RolePolicy	Kebijakan AWS terkelola Amazon EVSService RolePolicy dirilis.	Juni 9, 2025
Rilis Panduan Pengguna Awal	Panduan Pengguna VMware Layanan Elastis Amazon dirilis. Panduan Pengguna Amazon EVS menjelaskan semua konsep Amazon EVS dan memberikan instruksi tentang penggunaan berbagai fitur dengan konsol dan antarmuka baris perintah.	Juni 9, 2025

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.