Panduan Pengguna

# VMware Layanan Elastis Amazon

# VMware Layanan Elastis Amazon: Panduan Pengguna

# Table of Contents

# Apa itu Amazon Elastic VMware Service?

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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 dengan Amazon EVS

Untuk membuat lingkungan Amazon EVS pertama Anda, lihatMemulai. 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 migrasikan. 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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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 SDDC Manager. Lingkungan berisi domain VCF terkonsolidasi dengan cluster vSphere yang menampung komponen untuk mengelola, memantau, dan membuat instance 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  VMware ESXi host yang berjalan pada instance Amazon EC2 bare metal.

## 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 dan host VCF. ESXi 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. 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**

EC2 Aturan grup keamanan 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.

**Note**

Amazon EVS tidak mendukung IPv6 saat ini.

## VMkernel Manajemen host VLAN subnet

Subnet VLAN VMkernel 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. ESXi

## 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. ESXi

## Manajemen VM subnet VLAN

Subnet VLAN manajemen VM 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 AWS 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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

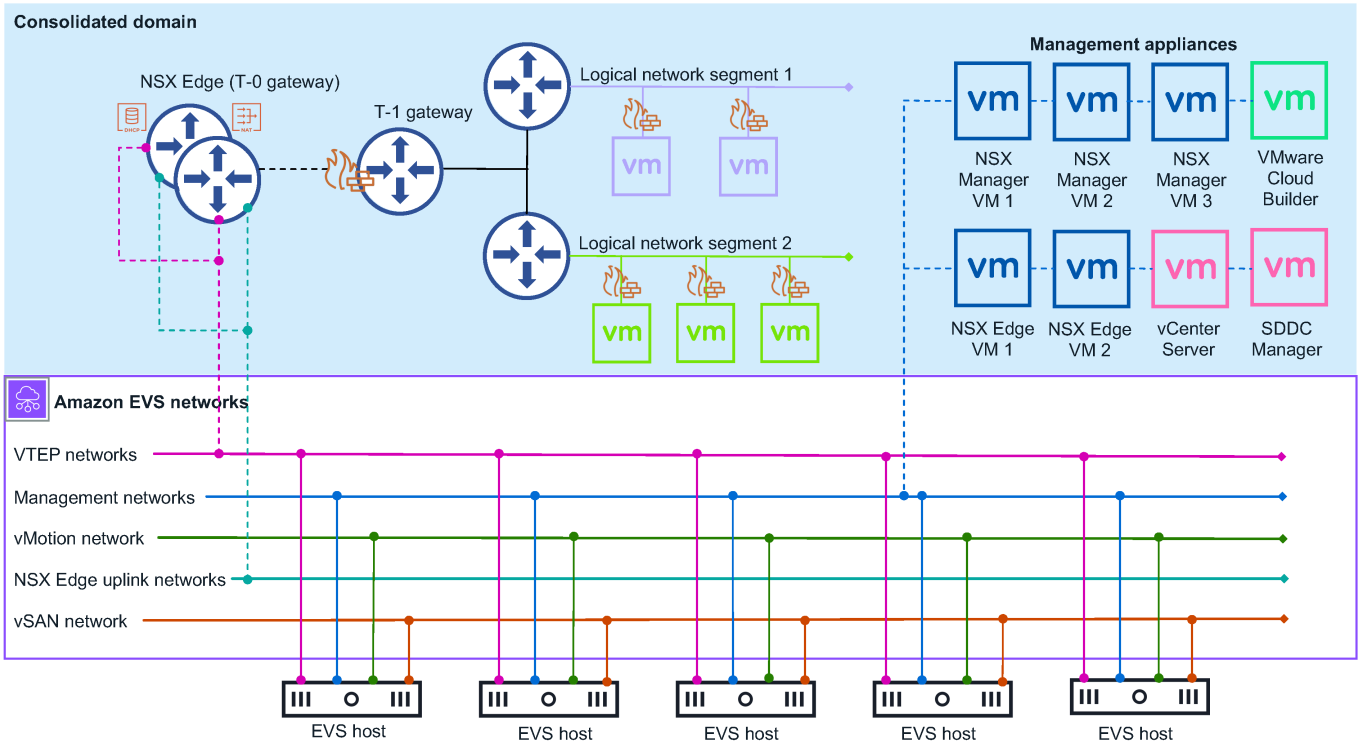
Amazon EVS mengimplementasikan model arsitektur terkonsolidasi VMware Cloud Foundation (VCF). Dalam model ini, komponen manajemen VCF dan beban kerja pelanggan berjalan bersama pada domain terkonsolidasi. Lingkungan Amazon EVS dikelola dari Server vCenter tunggal dengan kumpulan sumber daya vSphere yang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

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

- ESXi tuan rumah
- 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 AWS 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 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 “Konfigurasi 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 AWS Management Console 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.

- ESXi Host Amazon EVS 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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

Untuk menggunakan Amazon EVS, Anda perlu mengonfigurasi AWS layanan lain, serta menyiapkan lingkungan Anda untuk memenuhi persyaratan VMware Cloud Foundation (VCF).

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 akar dan memasukkan alamat email akun AWS 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 Buat kelompok kotak dialog, untuk Nama kelompok masukkan `Administrators`.
10. Pilih Kebijakan filter, lalu pilih Fungsi pekerjaan - terkelola AWS untuk memfilter isi tabel.
11. Dalam daftar kebijakan, pilih kotak centang untuk AdministratorAccess. Lalu, pilih Create group (Buat grup).

    > **Note**
    >
    > Anda harus mengaktifkan pengguna IAM dan akses peran ke Penagihan sebelum Anda dapat menggunakan `AdministratorAccess` izin untuk mengakses konsol Penagihan AWS dan Manajemen Biaya. 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 untuk memberi pengguna Anda akses ke sumber daya akun AWS Anda. Untuk mempelajari cara menggunakan kebijakan yang membatasi izin pengguna ke sumber daya AWS tertentu, lihat Kebijakan Manajemen Akses dan 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 kredensi 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 Amazon EVS dan panduan arsitektur. 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 the section called “Kuota layanan”.

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

# Rencanakan ukuran VPC CIDR dan konfigurasikan komponen VPC

Untuk mengaktifkan pembuatan lingkungan Amazon EVS, Anda harus menyediakan Amazon EVS dengan VPC yang berisi subnet dan ruang alamat IP yang cukup untuk Amazon EVS untuk membuat subnet VLAN yang terhubung ke peralatan VCF Anda. Untuk informasi selengkapnya tentang persyaratan pembuatan VPC, lihat. the section called “Buat VPC dengan subnet dan tabel rute”

## Tabel rute utama

Subnet Amazon EVS secara implisit terkait dengan tabel rute utama VPC Anda saat dibuat. Untuk mengaktifkan konektivitas ke layanan dependen seperti DNS atau sistem lokal agar penerapan

lingkungan berhasil, Anda harus mengonfigurasi tabel rute utama VPC untuk memungkinkan lalu lintas ke sistem ini. Untuk informasi selengkapnya tentang konfigurasi tabel rute utama untuk Amazon EVS, lihatthe section called “Konfigurasikan tabel rute utama VPC”.

### Pengaturan opsi DHCP

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

- Domain Name System (DNS) server yang digunakan untuk menyelesaikan alamat IP host.
- Network Time Protocol (NTP) server yang digunakan untuk menghindari masalah sinkronisasi waktu di SDDC.

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 seperti yang dijelaskan dalam. the section called “Buat lingkungan Amazon EVS”
- Zona pencarian terbalik dengan catatan PTR untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda seperti yang dijelaskan dalam. the section called “Buat lingkungan Amazon EVS”

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 opsi yang didukung Amazon EVS untuk konfigurasi server DNS dan NTP, lihat. the section called “Konfigurasikan server DNS dan NTP menggunakan set opsi VPC DHCP”

## Buat infrastruktur Server Rute VPC

Amazon EVS menggunakan Amazon VPC Route Server untuk mengaktifkan perutean dinamis berbasis BGP ke jaringan underlay VPC Anda. Untuk informasi tentang pengaturan Server Route untuk penggunaan Amazon EVS, lihatthe section called “Siapkan instance VPC Route Server dengan titik akhir dan rekan”.

# Buat gerbang transit untuk konektivitas on-premesis

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

# Buat Reservasi EC2 Kapasitas Amazon

Amazon EVS meluncurkan instans Amazon EC2 i4i.metal yang mewakili host ESXi 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 kredensil ini di. AWS CLI Untuk informasi selengkapnya, lihat AWS CLI Mengatur 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 5.2.1. Untuk informasi lebih lanjut, lihat catatan rilis VCF 5.2.1

> **Note**
>
> Amazon EVS hanya mendukung VCF versi 5.2.1.x saat ini.

## Dapatkan 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.

> **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**
>
> 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. Jika Anda mengelola kunci ini menggunakan Klien vSphere, Anda harus memastikan bahwa kunci tersebut juga muncul di layar lisensi antarmuka pengguna SDDC Manager.

# 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

# Memulai dengan Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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 5.2.1. Untuk informasi lebih lanjut, lihat catatan rilis VCF 5.2.1.

> **Important**
>
> Amazon EVS hanya mendukung VCF versi 5.2.1.x saat ini.

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.

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, lihatTitik akhir dan kuota.

9. (Opsional) Jika Anda membutuhkan konektivitas internet, untuk Jumlah subnet publik, pilih 1.
10. Untuk Jumlah subnet pribadi, pilih 1.
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.

## Konfigurasikan tabel rute utama VPC

Subnet Amazon EVS secara implisit terkait dengan tabel rute utama VPC Anda saat dibuat. 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 tentang mengelola tabel rute subnet, lihat Mengelola tabel rute subnet di Amazon VPC Panduan Pengguna.

Setelah lingkungan Amazon EVS diterapkan, Anda dapat mengonfigurasi asosiasi tabel rute eksplisit untuk mengaktifkan konektivitas melalui tabel rute khusus. Untuk informasi selengkapnya, lihat Mengganti tabel rute utama di Panduan Amazon VPC Pengguna.

> **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.

# Konfigurasikan server DNS dan NTP menggunakan set opsi VPC DHCP

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

- Domain Name System (DNS) server yang digunakan untuk menyelesaikan alamat IP host.
- Server Network Time Protocol (NTP) yang digunakan untuk menghindari masalah sinkronisasi waktu di SDDC.

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.

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

## Konfigurasi server DNS

Anda dapat memasukkan IPv4 alamat hingga empat server Domain Name System (DNS). Anda dapat menggunakan Route 53 sebagai penyedia server DNS Anda, atau Anda dapat menyediakan server DNS kustom Anda sendiri. Untuk informasi selengkapnya tentang mengonfigurasi Route 53 sebagai layanan DNS untuk domain yang ada, lihat Menjadikan Route 53 sebagai layanan DNS untuk domain yang sedang digunakan.

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

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

Agar berhasil menerapkan lingkungan, 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 seperti yang dijelaskan dalam. the section called “Buat lingkungan Amazon EVS”
- Zona pencarian terbalik dengan catatan PTR untuk setiap alat manajemen VCF dan host Amazon EVS dalam penerapan Anda seperti yang dijelaskan dalam. the section called “Buat lingkungan Amazon EVS”

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

> **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.

## Konfigurasi server NTP

Server NTP menyediakan waktu untuk jaringan Anda. Anda dapat memasukkan IPv4 alamat hingga empat server Network Time Protocol (NTP). Untuk informasi selengkapnya tentang mengonfigurasi server NTP dalam kumpulan opsi DHCP, lihat Membuat set opsi DHCP.

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

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 Mengatur waktu instans Anda di Panduan EC2 Pengguna Amazon.

## (Opsional) Konfigurasikan konektivitas jaringan lokal

Anda dapat mengonfigurasi konektivitas untuk pusat data lokal ke AWS infrastruktur Anda menggunakan AWS Direct Connect gateway transit terkait, atau menggunakan lampiran AWS Site-to-Site VPN ke gateway transit. AWS Site-to-Site VPN membuat koneksi IPsec VPN ke gateway transit melalui internet. AWS Direct Connect membuat koneksi IPsec VPN ke gateway transit melalui koneksi khusus pribadi. Setelah lingkungan Amazon EVS dibuat, Anda dapat menggunakan salah satu opsi untuk menghubungkan firewall pusat data lokal ke lingkungan NSX. VMware

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 “(Opsional) Konfigurasikan tabel rute gateway transit dan awalan Direct Connect untuk konektivitas lokal”.

Untuk informasi selengkapnya tentang pengaturan AWS Direct Connect koneksi, lihat AWS 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.

**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.

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

**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.

# 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.

> **Note**
>
> Operasi Amazon EVS yang dipicu dari konsol Amazon EVS tidak akan menghasilkan CloudTrail peristiwa.

2. Pada panel navigasi, pilih Lingkungan.
3. Pilih Buat lingkungan.
4. Pada halaman Validasi persyaratan Amazon EVS, lakukan hal berikut.
   a. Periksa apakah persyaratan AWS Support dan persyaratan kuota layanan terpenuhi. Untuk informasi selengkapnya tentang persyaratan dukungan Amazon EVS, lihatthe section called “Mendaftar untuk paket AWS Business, AWS Enterprise On-Ramp, atau Enterprise AWS Support”. Untuk informasi selengkapnya tentang persyaratan kuota Amazon EVS, lihat. the section called “Kuota layanan”
   b. (Opsional) Untuk Nama, masukkan nama lingkungan.
   c. Untuk versi Lingkungan, pilih versi VCF Anda. Amazon EVS saat ini hanya mendukung versi 5.2.1.x.
   d. Untuk ID Situs, masukkan ID Situs Broadcom Anda.
   e. Untuk kunci Solusi VCF, masukkan kunci solusi 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.

f. 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 SDDC Manager agar layanan 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.

g. 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.

h. Pilih Berikutnya.

5. Pada halaman Tentukan detail host, selesaikan langkah-langkah berikut 4 kali untuk menambahkan 4 host ke lingkungan. Lingkungan Amazon EVS memerlukan 4 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.

> **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.

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

e. Pilih Tambahkan host.

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

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

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

c. Untuk grup Keamanan - opsional, Anda dapat memilih hingga 2 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.

d. Di bawah konektivitas Manajemen, masukkan blok CIDR yang akan digunakan untuk subnet Amazon EVS VLAN.

> **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”.

e. 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.

> **Note**
>
> Pastikan blok VLAN CIDR yang Anda berikan berukuran benar di dalam VPC. Untuk informasi selengkapnya, lihat the section called “Pertimbangan jaringan Amazon EVS”.

f. Di bawah konektivitas beban kerja/VCF, masukkan blok CIDR untuk VLAN uplink NSX, dan pilih 2 rekan Server Rute VPC yang mengintip titik akhir Server IDs Route melalui uplink NSX.

> **Note**
>
> Amazon EVS memerlukan instance Server Rute VPC yang terkait dengan 2 titik akhir Server Rute dan 2 rekan Server Rute. 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”.

g. 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 tentang persyaratan dukungan Amazon EVS, lihatthe section called “Mendaftar untuk paket AWS Business, AWS Enterprise On-Ramp, atau Enterprise AWS Support”. Untuk informasi selengkapnya tentang persyaratan kuota Amazon EVS, lihat. the section called “Kuota layanan”

> **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`, Amazon EVS saat ini hanya mendukung VCF 5.2.1.x.
- 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 dan kunci lisensi vSAN Anda.

> **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.

> **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.

  **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 Server Rute VPC yang terkait dengan 2 titik akhir Server Rute dan 2 rekan Server Rute. 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 pada penutupan kontrak perangkat lunak atau perpanjangan kontrak Anda.
- (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-5.2.1 \
--terms-accepted \
```

```
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"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\"
    },
    {
      \"hostName\": \"esx02\",
```

```
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    }
  ]" \
--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-5.2.1",
        "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-5.2.1",
        "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.

Example

Amazon VPC console

1. Buka 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
```

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

Jika Anda mengonfigurasi konektivitas jaringan lokal menggunakan AWS 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.

# 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.

**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.

# 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. Untuk informasi selengkapnya tentang mengambil rahasia, lihat Mendapatkan AWS rahasia dari Secrets Manager.

**Note**

Amazon EVS tidak menyediakan rotasi rahasia Anda yang terkelola. Kami menyarankan Anda memutar rahasia Anda secara teratur pada jendela rotasi yang ditetapkan untuk memastikan bahwa rahasia tidak berumur panjang.

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

Secara default, Amazon EVS mengaktifkan ESXi 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 secara lokal. ESXi

> **Note**
>
> Amazon EVS menonaktifkan SSH jarak jauh secara default. Untuk informasi selengkapnya tentang mengaktifkan SSH mengakses Shell jarak jauh, lihat Akses ESXi ESXi Shell 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

SDDC UI and Amazon EVS console

1. Pergi ke antarmuka pengguna SDDC Manager.
2. Hapus host dari cluster vSphere. Ini akan membatalkan penetapan host dari domain SDDC. Ulangi langkah ini untuk setiap host di cluster. Untuk informasi selengkapnya, lihat Menghapus Host dari Cluster vSphere di Domain Beban Kerja dalam dokumentasi produk VCF.

3. Nonaktifkan host yang tidak ditugaskan. Untuk informasi selengkapnya, lihat Menonaktifkan Host dalam dokumentasi produk VCF.
4. Buka konsol Amazon EVS.

> **Note**
>
> Operasi Amazon EVS yang dipicu dari konsol Amazon EVS tidak akan menghasilkan CloudTrail peristiwa.

5. Di panel navigasi, pilih Lingkungan.
6. Pilih lingkungan yang berisi host untuk dihapus.
7. Pilih tab Hosts.
8. Pilih host dan pilih Hapus dalam tab Hosts. Ulangi langkah ini untuk setiap host di lingkungan.
9. 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.

10. 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.

SDDC UI and 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-5.2.1",
            "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-5.2.1",
            "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. Pergi ke antarmuka pengguna SDDC Manager.
4. Hapus host dari cluster vSphere. Ini akan membatalkan penetapan host dari domain SDDC. Ulangi langkah ini untuk setiap host di cluster. Untuk informasi selengkapnya, lihat Menghapus Host dari Cluster vSphere di Domain Beban Kerja dalam dokumentasi produk VCF.
5. Nonaktifkan host yang tidak ditugaskan. Untuk informasi selengkapnya, lihat Menonaktifkan Host dalam dokumentasi produk VCF.
6. 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
```

7. Ulangi langkah sebelumnya untuk menghapus host yang tersisa di lingkungan Anda.
8. 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.

9. 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 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.

## Hapus antarmuka jaringan elastis

Untuk langkah-langkah menghapus antarmuka jaringan elastis, lihat Menghapus antarmuka jaringan di Panduan EC2 Pengguna Amazon.

## 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 VMware Hybrid Cloud Extension (HCX) VMware

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

Setelah membuat lingkungan Amazon EVS, Anda dapat memigrasikan beban kerja VMware berbasis yang ada ke Amazon Elastic Service VMware (Amazon EVS) menggunakan VMware Hybrid Cloud Extension (HCX). VMware Untuk informasi selengkapnya tentang migrasi VMware HCX, lihat Jenis Migrasi VMware HCX di Panduan Pengguna HCX. VMware

Tutorial berikut menjelaskan cara menggunakan VMware HCX untuk memigrasikan VMware beban kerja ke Amazon EVS.

Anda dapat menggunakan VMware HCX untuk memigrasikan beban kerja melalui koneksi pribadi menggunakan AWS Direct Connect gateway transit terkait, atau menggunakan lampiran AWS Site-to-Site VPN ke gateway 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.

Untuk informasi selengkapnya tentang pengaturan AWS Direct Connect koneksi, lihat AWS Direct Connect gateway dan asosiasi gateway transit di  AWS Direct Connect Panduan Pengguna. 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.

## Prasyarat

Sebelum menggunakan VMware HCX dengan Amazon EVS, pastikan bahwa prasyarat HCX telah terpenuhi dan lingkungan Amazon EVS telah dibuat dan terhubung ke jaringan lokal Anda

menggunakan gateway transit AWS Direct Connect atau VPN dengan gateway transit. AWS Site-to-Site Untuk langkah-langkah membuat lingkungan Amazon EVS, lihatMemulai. Untuk informasi lebih lanjut tentang prasyarat VMware HCX, lihat. the section called “VMware Prasyarat HCX”

# Periksa status subnet HCX VLAN

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.
6. Salin `vlan` ID HCX untuk digunakan nanti.

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
```

Berikut ini adalah contoh respon.

```
{
 "environmentVlans": [
        {
            "vlan": 80,
            "cidr": "10.10.7.0/24",
            "availabilityZone": "us-east-2c",
            "functionName": "hcx",
            "createdAt": "2025-04-13T13:39:58.845000+00:00",
            "modifiedAt": "2025-04-13T13:47:57.067000+00:00",
```

```
            "vlanState": "CREATED",
            "stateDetails": ""
        },
        {
            "vlan": 20,
            "cidr": "10.10.1.0/24",
            "availabilityZone": "us-east-2c",
            "functionName": "vmManagement",
            "createdAt": "2025-04-13T13:39:58.456000+00:00",
            "modifiedAt": "2025-04-13T13:47:57.524000+00:00",
            "vlanState": "CREATED",
            "stateDetails": ""
        }
 ]
}
```


2. Identifikasi VLAN dengan `functionName` a `hcx` dan periksa apakah `vlanState` ada`CREATED`.
3. Salin `vlan` ID HCX untuk digunakan nanti.

## 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”.

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.

## 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

Layanan HCX WAN Optimization (HCX-WAN-OPT) 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-WAN-IX). HCX-WAN-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, 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 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

# Keamanan di Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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, 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 kepekaan data Anda, persyaratan perusahaan, serta peraturan perundangan yang berlaku

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon Elastic VMware Service. Ini menunjukkan kepada Anda cara mengonfigurasi Amazon Elastic VMware Service 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 Elastic VMware Service Anda.

Konten

# Manajemen identitas dan akses untuk Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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 VMware Service. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik



## Audiens

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

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

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Amazon Elastic VMware Service di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon Elastic VMware Service. Tugas Anda adalah menentukan fitur dan sumber daya Amazon Elastic VMware Service 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 Elastic VMware Service, lihatthe section called "Bagaimana Amazon Elastic VMware Service bekerja dengan IAM".

IAM administrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Amazon Elastic VMware Service. Untuk melihat contoh kebijakan berbasis identitas Amazon Elastic VMware Service yang dapat Anda gunakan, IAM lihat contoh kebijakan berbasis identitas Amazon Elastic VMware Service.

## Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai pengguna root akun AWS 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 AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Akun AWS Panduan Pengguna Masuk AWS.

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 penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat proses penandatanganan Versi Tanda Tangan 4 di AWS General Reference.

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 AWS IAM Identity Center (penerus AWS Single Sign-On) dan Menggunakan autentikasi multi-faktor (MFA) di Panduan Pengguna IAM. AWS

## Pengguna akar akun AWS

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 akar akun AWS dan diakses dengan cara masuk menggunakan 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 gabungan

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 AWS IAM Identity Center (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 AWS Management Console 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 AWS IAM Identity Center (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 peran layanan. 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 instance 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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 AWS Management Console, 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 organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap pengguna akar akun AWS. 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 Elastic VMware Service bekerja dengan IAM

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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

| IAM fitur | Dukungan Amazon EVS |
| --- | --- |
| the section called “Kebijakan berbasis identitas untuk Amazon EVS” | Ya |

| IAM fitur | Dukungan Amazon EVS |
| --- | --- |
| 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 |
| 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 Elastic VMware Service dan lainnya IAM, lihat Layanan AWS cara kerjanya IAM di Panduan Pengguna IAM.

Topik

- Kebijakan berbasis identitas untuk Amazon EVS
- Daftar kontrol akses (ACLs) di Amazon EVS

- Kontrol akses berbasis atribut (ABAC) dengan Amazon EVS
- Menggunakan kredensi sementara dengan Amazon EVS
- Teruskan sesi akses untuk Amazon EVS
- Peran layanan untuk Amazon EVS
- Peran terkait layanan untuk Amazon EVS

## 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 Elastic VMware Service, lihat contoh kebijakan berbasis identitas Amazon Elastic VMware Service.

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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus

menentukan prinsipal 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 prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal 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 hal apa. Yaitu, prinsipal mana yang dapat melakukan tindakan di sumber daya apa, dan dalam kondisi apa.

`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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service, lihat Tindakan yang Ditentukan oleh Amazon Elastic VMware Service 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 hal apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan 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 hal apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan 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 Elastic VMware Service mendefinisikan rangkaian 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 Elastic VMware Service, lihat Kunci Kondisi untuk Amazon Elastic VMware Service di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon Elastic VMware Service.

## 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 Elastic VMware Service atau meneruskan tag dalam permintaan ke Amazon Elastic VMware Service. 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 AWS Management Console 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 kredensil 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 kredensil 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 maju (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 maju.

## 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 VMware layanan Amazon Elastic Service, lihat. the section called “Menggunakan peran terkait layanan”

## Contoh kebijakan berbasis identitas Amazon EVS

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

Secara default, Pengguna IAM dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon Elastic VMware Service. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, 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 Elastic VMware Service
- 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 Elastic VMware Service 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 AWS 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 Elastic VMware Service

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

Untuk memastikan bahwa prinsipal IAM Anda masih dapat menggunakan konsol Amazon Elastic VMware Service, 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 Wilayah AWS dengan Wilayah AWS 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"
            ],
            "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. Wilayah AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "evs:Get*",
        "evs:List*"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

# Memecahkan masalah identitas dan akses Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Amazon Elastic VMware Service dan IAM.

Topik

- AccessDeniedException
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service mendukung fitur-fitur ini, lihatthe section called “Bagaimana Amazon Elastic VMware Service 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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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 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`- Membuat, memodifikasi, menandai, dan menghapus elastic network interface yang digunakan untuk membuat koneksi persisten antara Amazon EVS dan alat SDDC Manager VMware Virtual Cloud Foundation (VCF) di subnet VPC pelanggan. Konektivitas ini diperlukan agar Amazon EVS dapat menyebarkan, mengelola, dan memantau penyebaran VCF.

Untuk melihat versi terbaru 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 | Tanggal |
| --- | --- | --- |
| 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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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. Kebijakan izin 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, dan. VPCs

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 AWS Management Console, 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. Lihat informasi yang lebih lengkap di Titik akhir dan kuota.

# Menggunakan Amazon EVS dengan layanan lain AWS

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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
- Jalankan beban kerja berkinerja tinggi dengan Amazon FSx untuk ONTAP NetApp

## Buat sumber daya Amazon EVS dengan AWS CloudFormation

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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 Memulai.
- 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 default mereka 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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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 Memulai.
- 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 ESXi

Untuk setiap ESXi host, Anda harus mengkonfigurasi adaptor iSCSI perangkat lunak sehingga host ESXi Anda dapat menggunakannya untuk mengakses penyimpanan iSCSI. Untuk instruksi untuk mengkonfigurasi adaptor iSCSI perangkat lunak untuk ESXi host di vSphere, lihat Tambah atau Hapus 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 Anda. ESXi 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 ESXi host 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 ESXi Host dalam dokumentasi produk vSphere. VMware

## 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

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

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 spesifik dan terdeteksi.

### 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 gagal.

Jika pemeriksaan ini gagal, Amazon EVS tidak dapat lagi menjangkau Manajer SDDC untuk memvalidasi status lingkungan, dan host tidak dapat lagi ditambahkan ke lingkungan. Kegagalan jangkauan juga akan menyebabkan penggunaan kembali kunci lisensi dan pemeriksaan cakupan kunci gagal, dan pemeriksaan jumlah host mengembalikan respons Tidak Dikenal.

Kegagalan Reachabilty menunjukkan bahwa mungkin ada masalah dengan SDDC Manager, konfigurasi firewall, atau sertifikat yang hilang. Anda dapat mencoba menyelesaikan masalah ini, atau 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 5.2.1.

Jika pemeriksaan ini gagal, Anda perlu menambahkan host sehingga 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 hanya dapat digunakan untuk satu lingkungan Amazon EVS. Pemeriksaan ini gagal jika lisensi yang digunakan ditambahkan ke lingkungan.

Jika pemeriksaan ini gagal, Anda 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 sebelumnya digunakan dengan lisensi yang tidak digunakan.

> **Important**
>
> Gunakan antarmuka pengguna SDDC Manager untuk mengelola kunci lisensi komponen VCF. Amazon EVS mengharuskan Anda mempertahankan kunci lisensi komponen yang valid di SDDC Manager agar layanan berfungsi dengan baik. Jika Anda mengelola kunci lisensi komponen menggunakan Klien vSphere, Anda harus memastikan bahwa kunci tersebut juga muncul di layar lisensi antarmuka pengguna SDDC Manager untuk mencegah kegagalan pemeriksaan kunci lisensi.

## Pemeriksaan cakupan kunci gagal

Pemeriksaan ini memverifikasi bahwa kunci lisensi VCF Anda yang ditetapkan ke vCenter Server mengalokasikan inti vCPU dan kapasitas penyimpanan vSAN (TiB) yang memadai untuk semua host yang digunakan.

Jika pemeriksaan ini gagal, Anda menerima respons kesalahan bahwa lingkungan Amazon EVS tidak dapat dibuat, atau host Amazon EVS tidak dapat ditambahkan ke lingkungan. Kegagalan cakupan utama dapat mengindikasikan salah satu masalah berikut:

- Anda telah melampaui jumlah host yang didukung untuk Amazon EVS. Amazon EVS mendukung 4 hingga 16 host per lingkungan. Jika ini masalahnya, hapus atau tambahkan host hingga lingkungan Anda berada dalam rentang host yang didukung.
- 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 penugasan 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 kunci lisensi komponen VCF. Amazon EVS mengharuskan Anda mempertahankan kunci lisensi komponen yang valid di SDDC Manager agar layanan berfungsi dengan baik. Jika Anda mengelola kunci lisensi komponen menggunakan Klien vSphere, Anda harus memastikan bahwa kunci tersebut juga muncul di layar lisensi antarmuka pengguna SDDC Manager untuk mencegah kegagalan pemeriksaan kunci lisensi.

## Agen vSphere HA di host ini tidak dapat mencapai alamat isolasi

Di antarmuka pengguna vCenter, dengan ESXi host yang 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.

Untuk menghapus pesan kesalahan vSphere HA, Anda harus menonaktifkan vSphere HA. Untuk langkah-langkah untuk menonaktifkan vSphere HA di klien vSphere, lihat artikel Broadcom Menonaktifkan dan mengaktifkan Ketersediaan Tinggi (HA). VMware

## Prakecek pemutakhiran VSAN gagal untuk cluster host ESXi

Saat mencoba memutakhirkan cluster ESXi host 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.

# Titik akhir dan kuota Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

Berikut ini adalah titik akhir layanan dan kuota layanan untuk layanan ini. Untuk terhubung secara terprogram ke sebuah Layanan AWS, Anda menggunakan endpoint. Selain titik akhir standar, beberapa Layanan AWS menawarkan AWS titik akhir FIPS di Wilayah tertentu. Untuk informasi selengkapnya, lihat AWS titik akhir layanan. Kuota layanan, juga disebut sebagai batas, adalah jumlah maksimum sumber daya layanan atau operasi untuk Anda Akun AWS. Untuk informasi lebih lanjut, lihat AWS kuota layanan.

## Titik akhir layanan

Amazon EVS API menyediakan titik akhir regional dan dual-stack, serta titik akhir FIPS untuk Wilayah AS. Untuk menggunakan titik akhir dual-stack dengan AWS CLI, lihat konfigurasi titik akhir Dual-stack dan FIPS di Panduan Referensi Alat dan. AWS SDKs

| Nama Wilayah | Wilayah | Titik Akhir | Protokol |
|---|---|---|---|
| AS Timur (Virginia Utara) | us-east-1 | evs.us-east-1.amazonaws.com<br>evs-fips.us-east-1.amazonaws.com<br>evs.us-east-1.api.aws<br>evs-fips.us-east-1.api.aws | HTTPS |
| US East (Ohio) | us-east-2 | evs.us-east-2.amazonaws.com<br>evs-fips.us-east-2.amazonaws.com<br>evs.us-east-2.api.aws<br>evs-fips.us-east-2.api.aws | HTTPS |

| Nama Wilayah | Wilayah | Titik Akhir | Protokol |
|---|---|---|---|
| US West (Oregon) | us-west-2 | evs.us-west-2.amazonaws.com<br>evs-fips.us-west-2.amazonaws.com<br>evs.us-west-2.api.aws<br>evs-fips.us-west-2.api.aws | HTTPS |
| Asia Pacific (Tokyo) | ap-northeast-1 | evs.ap-northeast-1.amazonaws.com<br>evs.ap-northeast-1.api.aws | HTTPS |
| Europe (Frankfurt) | eu-central-1 | evs.eu-central-1.amazonaws.com<br>evs.eu-central-1.api.aws | HTTPS |
| Europe (Ireland) | eu-west-1 | evs.eu-west-1.amazonaws.com<br>evs.eu-west-1.api.aws | HTTPS |

## Kuota layanan

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 AWS Management Console 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.

> **Important**
>
> Untuk mengaktifkan pembuatan lingkungan Amazon EVS, jumlah host per kuota lingkungan EVS harus minimal 4. Kuota default adalah 0. Untuk menambah kuota ini, buka konsol Service Quotas dan minta kenaikan kuota.

**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.

| Nama | Default | Dapat disesuaikan | Deskripsi |
|---|---|---|---|
| Jumlah host per lingkungan EVS | 0 | Ya | Jumlah maksimum host yang dapat disediakan dalam satu lingkungan Amazon EVS. |
| Jumlah lingkungan per AWS akun | 1 | Ya | Jumlah maksimum lingkungan EVS yang dapat dibuat di akun ini di Wilayah saat ini. |

# Riwayat dokumen untuk Panduan Pengguna Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS dalam rilis pratinjau publik dan dapat berubah sewaktu-waktu.

Tabel berikut menjelaskan rilis dokumentasi untuk Amazon Elastic VMware Service.

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Merilis jumlah lingkungan per AWS kuota akun | Amazon EVS merilis jumlah lingkungan per kuota AWS akun.<br><br>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.<br><br>Panduan Pengguna Amazon EVS menjelaskan semua konsep Amazon EVS dan | Juni 9, 2025 |

memberikan instruksi tentang penggunaan berbagai fitur dengan konsol dan antarmuka baris perintah.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.