Manual do usuário

Amazon Elastic VMware Service

Amazon Elastic VMware Service: Manual do usuário

Table of Contents

O que é o Amazon Elastic VMware Service?

Você pode usar o Amazon Elastic VMware Service (Amazon EVS) para implantar e executar um ambiente VMware Cloud Foundation (VCF) diretamente em instâncias EC2 bare metal internas (Amazon Virtual Private Cloud VPC).

Tópicos

Características do Amazon EVS

A seguir estão os principais recursos do Amazon EVS:

Simplifique e acelere sua migração para AWS

Elimine o atrito de migração e garanta a consistência operacional com a portabilidade de assinaturas e a implantação automatizada do VMware Cloud Foundation (VCF) na nuvem. Estenda as redes locais e migre cargas de trabalho sem precisar alterar endereços IP, treinar novamente a equipe ou reescrever runbooks operacionais.

Mantenha o controle de sua VMware arquitetura na nuvem

Mantenha controle total sobre sua VMware arquitetura e otimize uma pilha de virtualização que atenda às demandas exclusivas de seus aplicativos, incluindo complementos e soluções de terceiros.

Autogerencie ou utilize AWS parceiros para uma experiência gerenciada

Descubra opções e flexibilidade para se autogerenciar ou aproveite a experiência dos AWS parceiros para gerenciar e operar seu ambiente de VCF AWS a fim de atingir suas metas de negócios em termos de talento, tempo e custos.

Dimensione e proteja sua empresa contra interrupções

Melhore a escalabilidade na nuvem mais segura, escalável e resiliente para migrar e operar suas cargas de trabalho baseadas. VMware

Adote a AWS inovação para transformar seus aplicativos e sua infraestrutura

Como um serviço AWS nativo, o Amazon EVS simplifica a extensão e a expansão do seu VMware ambiente com mais de 200 serviços (incluindo bancos de dados gerenciados, análises, sem servidor e contêineres e IA generativa) para transformar seus negócios.

Comece a usar o Amazon EVS

Para criar seu primeiro ambiente Amazon EVS, consulteIntrodução. Em geral, começar a usar o Amazon EVS envolve a conclusão das etapas a seguir.

1. Concluir os pré-requisitos. Para obter mais informações, consulte Configurando o Amazon Elastic VMware Service.
2. Crie um ambiente Amazon EVS. Durante a criação do ambiente, o Amazon EVS cria as sub-redes de VLAN necessárias usando os intervalos CIDR que você especifica e adiciona hosts ao ambiente.
3. Personalize o VCF. Configure seu ambiente na interface de usuário do vSphere de acordo com suas necessidades. Isso pode incluir a configuração de logins, políticas, monitoramento e muito mais.
4. Conecte-se e migre. Conecte seu ambiente ao seu datacenter local e migre suas cargas de trabalho do VCF para o Amazon EVS.

Acessando o Amazon EVS

Você pode definir e configurar suas implantações do Amazon EVS usando as seguintes interfaces:

- Console Amazon EVS - Fornece uma interface web para criar ambientes Amazon EVS.
- AWS CLI - Fornece comandos para um amplo conjunto de Serviços da AWS e é compatível com Windows, macOS e Linux. Para obter mais informações, consulte AWS Command Line Interface.
- AWS CloudFormation - Fornece uma especificação para cada tipo de recurso, como`AWS::EVS::Environment`. Você cria um modelo usando a especificação do recurso e CloudFormation cuida do provisionamento e da configuração dos recursos para você.

Conceitos e componentes do Amazon EVS

Esta seção explica alguns dos principais conceitos e componentes do Amazon EVS.

Ambiente do Amazon EVS

Um ambiente Amazon EVS é um contêiner lógico para recursos do VMware Cloud Foundation (VCF), como hosts vSphere, vSAN, NSX e SDDC Manager. Ele contém um domínio do VCF consolidado com um cluster do vSphere que hospeda os componentes para gerenciar, monitorar e instanciar a pilha de software do VCF. Cada ambiente é mapeado diretamente para um dispositivo SDDC Manager. Para obter mais informações, consulte the section called “Arquitetura”.

Hospedeiro Amazon EVS

Um host Amazon EVS é um host VMware ESX executado em instâncias Amazon EC2 bare metal. Os hosts do Amazon EVS usam volumes de armazenamento de NVMe instâncias locais para datastores vSAN, que armazenam suas máquinas virtuais de gerenciamento e carga de trabalho.

> **Warning**
>
> Os volumes de armazenamento de instâncias são efêmeros. Os dados armazenados nesses volumes não persistem se a instância EC2 subjacente for interrompida ou encerrada. Interromper ou encerrar Amazon EC2 instâncias usadas pelo Amazon EVS sem descomissionamento no VCF pode resultar em perda de dados.
> Para obter mais informações sobre a manutenção do host, consultethe section called “Manutenção de host”.

Sub-rede de acesso ao serviço

A sub-rede de acesso ao serviço é uma sub-rede VPC padrão que permite que o Amazon EVS acesse a implantação do VCF. Durante a criação do ambiente Amazon EVS, você especifica a VPC e a sub-rede que o Amazon EVS usará para acesso ao serviço.

Quando você cria um ambiente Amazon EVS, o Amazon EVS provisiona interfaces de rede elásticas na sub-rede de acesso ao serviço para facilitar a conectividade de gerenciamento com dispositivos VCF e hosts ESX. Essa conectividade é necessária para que o Amazon EVS possa implantar, gerenciar e monitorar a implantação do VCF.

Sub-rede VLAN Amazon EVS

Uma sub-rede VLAN do Amazon EVS é uma sub-rede do Amazon VPC gerenciada pelo Amazon EVS. As sub-redes de VLAN fornecem conectividade VPC para hosts Amazon EVS e dispositivos VCF, como VMware NSX, HCX e vCenter Server. VMware VMware Cada sub-rede VLAN tem uma tag de VLAN para permitir que o tráfego da rede VLAN seja segmentado logicamente.

O Amazon EVS cria todas as sub-redes de VLAN que o serviço usa quando o ambiente do Amazon EVS é criado. Você fornece as entradas do bloco CIDR que as sub-redes da VLAN usam. Você deve garantir que os blocos CIDR da sub-rede da VLAN sejam dimensionados adequadamente de acordo com o número de hosts que serão configurados, levando em consideração as necessidades futuras de escalabilidade. Os blocos CIDR devem ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24 máscara de rede. Os blocos CIDR não devem se sobrepor a nenhum bloco CIDR existente associado à VPC.

Na criação, as sub-redes da VLAN são associadas implicitamente à tabela de rotas principal da VPC. Após a implantação, você pode associar explicitamente as sub-redes da VLAN a uma tabela de rotas personalizada. Para obter mais informações, consulte the section called “Considerações sobre a rede Amazon EVS”.

Important

As sub-redes de VLAN do Amazon EVS só podem ser criadas durante a criação do ambiente Amazon EVS e não podem ser modificadas após a criação do ambiente. Você deve garantir que os blocos CIDR da sub-rede da VLAN estejam dimensionados adequadamente antes de criar o ambiente. Você não poderá adicionar sub-redes de VLAN após a implantação do ambiente.

Important

As regras do grupo de segurança do EC2 não são aplicadas nas interfaces de rede elástica do Amazon EVS conectadas a sub-redes de VLAN. Para controlar o tráfego de e para sub-redes de VLAN, você deve usar uma lista de controle de acesso à rede.

Sub-rede VLAN de gerenciamento de host

A sub-rede VLAN de gerenciamento do host separa o tráfego de gerenciamento do tráfego do usuário e permite o gerenciamento remoto dos hosts. A interface de rede vmkernel de gerenciamento de host EVS se conecta a essa sub-rede.

Sub-rede VLAN vMotion

A sub-rede VLAN do vMotion segmenta logicamente o tráfego do VMware vMotion e é usada durante um processo do vMotion para mover máquinas virtuais entre hosts.

Sub-rede vSAN VLAN

A sub-rede vSAN VLAN é usada pelo vSAN para separar o tráfego relacionado às operações de armazenamento do VMware vSAN de outros tráfegos de rede.

Sub-rede VLAN VTEP

A sub-rede VLAN VTEP usa endpoints de túnel virtual (VTEP) VMware NSX para encapsular e desencapsular o tráfego de rede de sobreposição para os hosts Amazon EVS ESX.

Sub-rede Edge VTEP VLAN

A sub-rede VLAN Edge VTEP é uma sub-rede VLAN VTEP especializada dedicada ao tráfego de sobreposição do dispositivo NSX Edge. Essa VLAN é usada para comunicação de sobreposição entre as bordas do NSX e os hosts ESX.

Sub-rede VM VLAN de gerenciamento

A sub-rede VLAN da VM de gerenciamento é usada para gerenciar dispositivos virtuais, incluindo NSX Manager, vCenter Server e SDDC Manager.

Sub-rede VLAN de uplink HCX

A sub-rede VLAN de uplink HCX é usada para comunicação entre os dispositivos HCX Interconnect (HCX-IX) e HCX Network Extension (HCX-NE) e permite a criação do uplink de malha de serviço HCX.

Sub-rede VLAN de uplink NSX

A sub-rede VLAN de uplink do NSX é usada para conectar suas redes de sobreposição do NSX ao resto da sua VPC e a qualquer outra rede externa que você configurar. A sub-rede VLAN de uplink do NSX é configurada nos uplinks dos nós do NSX Edge.

Sub-rede VLAN de expansão

A sub-rede VLAN de expansão pode ser usada para ativar funções adicionais suportadas pelo VCF, como NSX Federation. O Amazon EVS cria duas sub-redes VLAN de expansão durante a criação do ambiente.

VMware NSX

VMware O NSX é uma plataforma de rede definida por software (SDN) que permite a virtualização da rede. O Amazon EVS usa o VMware NSX para criar e gerenciar a rede de sobreposição na qual os dispositivos e cargas de trabalho do VMware Cloud Foundation (VCF) são executados. O Amazon EVS implanta um par de nós Active/Standby NSX Edge, junto com uma rede de sobreposição NSX. O Amazon EVS configura automaticamente todo o roteamento e os uplinks do NSX em seu nome como parte da implantação. Para obter mais informações sobre conceitos comuns do NSX, consulte Conceitos principais no Guia de instalação do VMware NSX.

VMware Extensão de nuvem híbrida (HCX)

VMware A Hybrid Cloud Extension (VMware HCX) é uma plataforma de mobilidade de aplicativos projetada para simplificar a migração de aplicativos, reequilibrar cargas de trabalho e otimizar a recuperação de desastres em data centers e nuvens. Você pode usar o HCX para migrar suas cargas de trabalho VMware baseadas para o Amazon EVS.

Você pode configurar a conectividade para VMware HCX usando Direct Connect um gateway de trânsito associado ou usando um anexo AWS Site-to-Site VPN a um gateway de trânsito. Para obter mais informações, consulte Migração.

Arquitetura do Amazon EVS

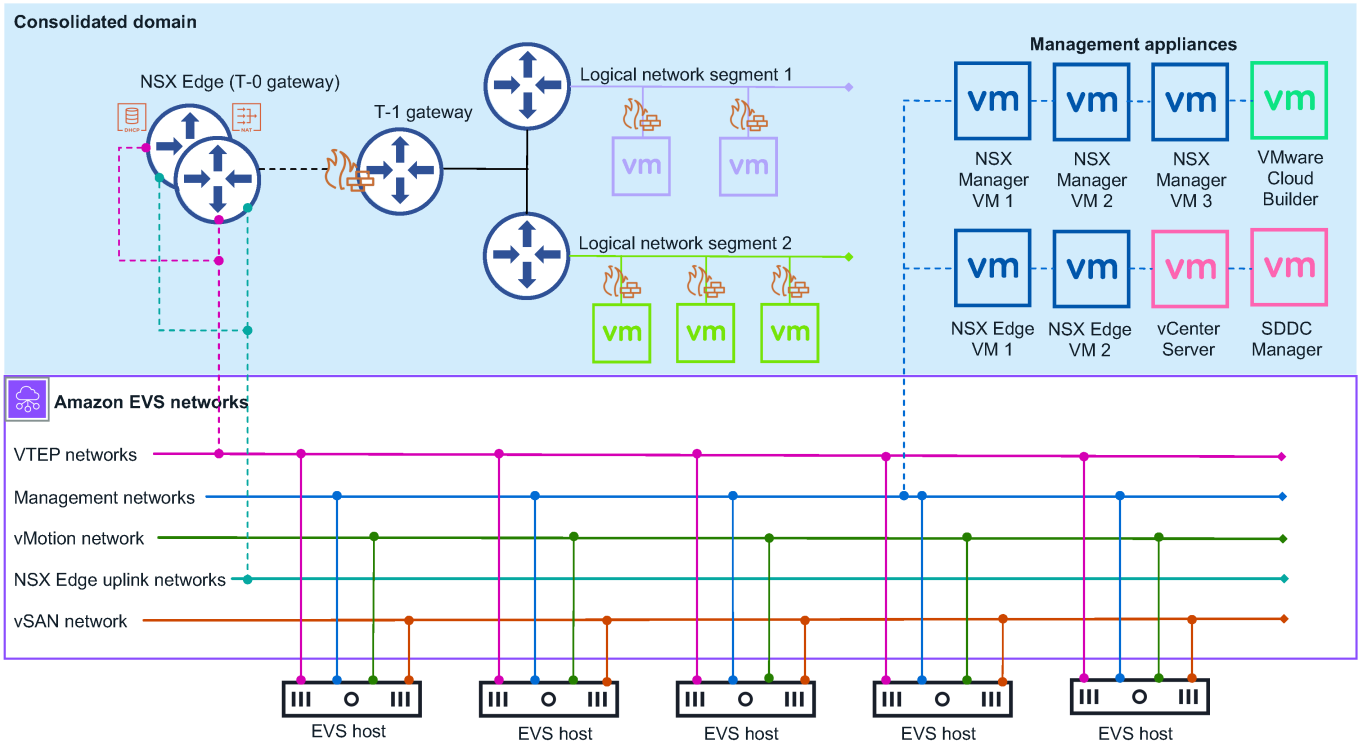
O Amazon EVS implementa um modelo de arquitetura consolidada do VMware Cloud Foundation (VCF). Nesse modelo, os componentes de gerenciamento do VCF e as cargas de trabalho do cliente são executados juntos em um domínio consolidado. O ambiente Amazon EVS é gerenciado a partir

de um único vCenter Server com pools de recursos do vSphere que fornecem isolamento entre as cargas de trabalho do gerenciamento e do cliente.

O domínio consolidado que o Amazon EVS implanta contém os seguintes componentes de gerenciamento do VCF:

- Hospedeiros ESX
- Instância do vCenter Server
- Gerenciador de SDDC
- Armazenamento de dados vSAN
- Cluster NSX Manager de três nós
- Cluster vSphere
- Cluster NSX Edge

O diagrama a seguir mostra um exemplo da arquitetura Amazon EVS que foi implantada em um ambiente Amazon EVS e mostra como os componentes do ambiente estão conectados. No diagrama, o ambiente Amazon EVS com uma arquitetura de domínio consolidada está sombreado em azul. A topologia de rede subjacente do Amazon EVS é ilustrada na linha roxa sólida.



Topologia de rede

Um ambiente Amazon EVS tem duas camadas de rede de gerenciamento separadas:

Amazon VPC

As sub-redes Amazon VPC e Amazon EVS VLAN que são criadas na VPC durante a criação do ambiente formam a rede subjacente para sua implantação de VCF. Essa infraestrutura fornece conectividade para redes de sobreposição NSX, gerenciamento de host, VMotion e VSAN. O Amazon VPC Route Server permite o roteamento dinâmico entre a rede subjacente e as redes sobrepostas. Para obter mais informações, consulte the section called “Componentes e conceitos”.

> **Note**
>
> As sub-redes VLAN do Amazon EVS são usadas somente para facilitar a comunicação subjacente do VCF. As máquinas virtuais convidadas que executam cargas de trabalho do cliente devem ser implantadas nas redes de sobreposição do NSX. A implantação de máquinas virtuais convidadas na rede subjacente de sub-rede VLAN do Amazon EVS não é suportada.

VMware Rede de sobreposição NSX

O Amazon EVS configura uma rede de sobreposição NSX em seu nome como parte da implantação. Você pode configurar redes adicionais de sobreposição do NSX para obter isolamento de rede entre diferentes cargas de trabalho ou aplicativos em seu ambiente Amazon EVS. Para obter mais informações, consulte Design de sobreposição para VMware Cloud Foundation na documentação do produto VMware Cloud Foundation.

> **Note**
>
> O Amazon EVS oferece suporte a apenas um gateway de nível 0 para um cluster Active/Standby NSX Edge com dois nós NSX Edge. Esse gateway de nível 0 se conecta e anuncia todas as redes de sobreposição que você configura para uso com o Amazon EVS.

As duas camadas de rede são conectadas por um cluster Active/Standby NSX Edge com dois nós NSX Edge. Os nós do NSX Edge permitem a comunicação pela VPC entre máquinas virtuais no, bem como VLANs a conectividade com a Internet e a conectividade privada Direct Connect usando uma VPN com um AWS Site-to-Site gateway de trânsito.

Considerações sobre a rede Amazon EVS

A rede de gerenciamento requer as seguintes configurações de recursos de rede. Você fornece essas entradas durante a criação do ambiente Amazon EVS. Para obter mais informações, consulte the section called “Componentes e conceitos”.

- Uma Amazon VPC. Certifique-se de que seu bloco IPv4 CIDR da VPC seja dimensionado adequadamente para acomodar a sub-rede VPC necessária e as sub-redes VLAN do Amazon EVS que o Amazon EVS provisiona durante a criação do ambiente. Para obter mais informações, consulte the section called “Sub-rede VLAN Amazon EVS”.

  > **Note**
  >
  > O Amazon EVS não oferece suporte IPv6 no momento.

- Uma sub-rede de acesso ao serviço em sua VPC. O Amazon EVS usa essa sub-rede para manter uma conexão persistente com seu dispositivo SDDC Manager. Para obter mais informações, consulte the section called “Sub-rede de acesso ao serviço”.

  > **Note**
  >
  > No momento, o Amazon EVS só oferece suporte a implantações Single-AZ. Todas as sub-redes VPC que o Amazon EVS usa devem existir em uma única zona de disponibilidade em uma região onde o serviço está disponível.

  > **Note**
  >
  > Todas as sub-redes VPC exigem tabelas de rotas associadas que são configuradas de acordo com os requisitos de rede da sua organização.

- Um endereço IP do servidor DNS primário e um endereço IP do servidor DNS secundário no conjunto de opções DHCP da VPC para resolver endereços IP do host. O Amazon EVS também exige que você crie uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa

reversa com registros PTR para cada dispositivo de gerenciamento de VCF e host Amazon EVS em sua implantação. Para obter mais informações, consulte the section called “Configurar servidores DNS”.

- Bloqueios CIDR de sub-rede de VLAN do Amazon EVS para cada sub-rede de VLAN que o Amazon EVS provisiona para você durante a criação do ambiente. Os blocos CIDR devem ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24 máscara de rede. Os blocos CIDR não devem ser sobrepostos.
- Uma instância do Amazon VPC Route Server com a propagação do Route Server ativada.
- Dois endpoints do Route Server na sub-rede de acesso ao serviço.
- Dois pares do Route Server que emparelham os nós do NSX Edge que o Amazon EVS provisiona com endpoints do Route Server.

Gateway de nível 0

O gateway de nível 0 manipula todo o tráfego norte-sul entre as redes lógica e física e é criado na rede de sobreposição NSX. Esse gateway de nível 0 é criado como parte da implantação do Amazon EVS.

> **Note**
>
> O Amazon EVS oferece suporte a apenas um gateway de nível 0 para um cluster Active/Standby NSX Edge com dois nós NSX Edge.

Gateway de nível 1

O gateway de nível 1 manipula o tráfego leste-oeste entre segmentos de rede roteados em um ambiente e é criado na rede de sobreposição NSX. O gateway de nível 1 tem conexões de downlink para segmentos e conexões de uplink para o gateway de nível 0. Você pode criar e configurar gateways de nível 1 adicionais se precisar deles.

Cluster NSX Edge

O Amazon EVS usa a interface do NSX Manager para implantar um cluster NSX Edge com dois nós do NSX Edge que são executados no modo. Active/Standby Esse cluster NSX Edge fornece a plataforma na qual os gateways de nível 0 e nível 1 são executados, junto com as conexões IPsec VPN e seu mecanismo de roteamento BGP.

Recursos do Amazon EVS

O Amazon EVS provisiona os seguintes AWS recursos durante a criação do ambiente. Esses recursos aparecem na VPC que você permite que o Amazon EVS acesse e são visíveis na Console de gerenciamento da AWS e AWS CLI depois de serem criados.

> **Important**
>
> A modificação desses recursos fora do console e da API do Amazon EVS pode afetar a disponibilidade e a estabilidade do seu ambiente Amazon EVS.

- Interfaces de rede elásticas do Amazon EVS que permitem a conectividade com seus dispositivos e hosts VCF.
- Hospedeiros Amazon EVS ESX que são executados em instâncias Amazon EC2 bare metal. Para obter mais informações, consulte the section called “Hospedeiro Amazon EVS”.

  > **Important**
  >
  > Seu ambiente Amazon EVS deve ter no mínimo 4 hosts e no máximo 16 hosts. O Amazon EVS só oferece suporte a ambientes com 4 a 16 hosts.

- Sub-redes de VLAN do Amazon EVS que conectam sua VPC aos dispositivos VCF. Para obter mais informações, consulte the section called “Sub-rede VLAN Amazon EVS”.

Configurando o Amazon Elastic VMware Service

Para usar o Amazon EVS, você precisará configurar outros AWS serviços, bem como configurar seu ambiente para atender aos requisitos do VMware Cloud Foundation (VCF). Para obter uma lista de verificação resumida dos pré-requisitos de implantação, consulte. the section called “Lista de verificação de implantação”

Tópicos

Inscreva-se para AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

1. Abra a https://portal.aws.amazon.com/billing/ inscrição.

2. Siga as instruções online.

Criar um usuário do IAM

1. Faça login no console do IAM como proprietário da conta, escolhendo Usuário raiz e inserindo o endereço de e-mail AWS da sua conta. Na próxima página, insira a senha.

> **Note**
>
> Recomendamos seguir as melhores práticas para utilizar o usuário do IAM `Administrator` a seguir e armazenar as credenciais do usuário raiz com segurança. Cadastre-se como o usuário raiz apenas para executar algumas tarefas de gerenciamento de serviços e contas.

2. No painel de navegação, escolha Usuários e, em seguida, escolha Criar usuário.
3. Em Nome do usuário, digite `Administrator`.
4. Marque a caixa de seleção ao lado do acesso ao AWS Management Console. Então, selecione Custom password (Senha personalizada), e insira sua nova senha na caixa de texto.
5. (Opcional) Por padrão, AWS exige que o novo usuário crie uma nova senha ao fazer login pela primeira vez. Você pode desmarcar a caixa de seleção próxima de User must create a new password at next sign-in (O usuário deve criar uma senha no próximo login) para permitir que o novo usuário redefina a senha depois de fazer login.
6. Escolha Próximo: Permissões.
7. Em Set permissions (Conceder permissões), escolha Add user to group (Adicionar usuário ao grupo).
8. Escolha Create group (Criar grupo).
9. Na caixa de diálogo Create group (Criar grupo), em Group name (Nome do grupo), digite `Administrators`.
10. Escolha Políticas de filtro e, em seguida, selecione a função -job AWS gerenciada para filtrar o conteúdo da tabela.
11. Na lista de políticas, marque a caixa de seleção para AdministratorAccess. A seguir escolha Criar grupo.

> **Note**
>
> Você deve ativar o acesso de usuário e função do IAM ao Billing antes de poder usar as `AdministratorAccess` permissões para acessar o console AWS Billing and Cost Management. Para fazer isso, siga as instruções na etapa 1 do tutorial sobre como delegar acesso ao console de faturamento.

12. Suporte a lista de grupos, selecione a caixa de seleção para seu novo grupo. Escolha Refresh (Atualizar) caso necessário, para ver o grupo na lista.
13. Escolha Next: Tags (Próximo: etiquetas).
14. (Opcional) Adicione metadados ao usuário anexando tags como pares de chave-valor. Para obter mais informações sobre como usar etiquetas no IAM, consulte Marcar entidades do IAM no Guia do usuário do IAM.
15. Escolha Next: Review (Próximo: Análise) para ver uma lista de associações de grupos a serem adicionadas ao novo usuário. Quando você estiver pronto para continuar, escolha Create user (Criar usuário).

Você pode usar esse mesmo processo para criar mais grupos e usuários e dar aos usuários acesso aos recursos AWS da sua conta. Para saber mais sobre o uso de políticas que restringem as permissões do usuário a AWS recursos específicos, consulte Gerenciamento de acesso e exemplos de políticas.

Crie uma função do IAM para delegar a permissão do Amazon EVS a um usuário do IAM

Você pode usar funções para delegar acesso aos seus AWS recursos. Com as funções do IAM, você pode estabelecer relações de confiança entre sua conta confiável e outras contas AWS confiáveis. A conta confiável é proprietária do recurso a ser acessado, e a conta confiável contém os usuários que precisam acessar o recurso.

Depois de criar a relação de confiança, um usuário do IAM ou um aplicativo da conta confiável pode usar a operação da `AssumeRole` API AWS Security Token Service (AWS STS). Essa operação fornece credenciais de segurança temporárias que permitem o acesso aos AWS recursos em sua conta. Para obter mais informações, consulte Criar uma função para delegar permissões a um usuário do IAM no Guia do AWS Identity and Access Management usuário.

Siga estas etapas para criar uma função do IAM com uma política de permissões que permita acesso às operações do Amazon EVS.

> **Note**
>
> O Amazon EVS não suporta o uso de um perfil de instância para passar uma função do IAM para uma EC2 instância.

Example

IAM console

1. Acesse o console do IAM.
2. No menu à esquerda, escolha Políticas.
3. Selecione Criar política.
4. No editor de políticas, crie uma política de permissões que habilite as operações do Amazon EVS. Para visualizar um exemplo de política, consulte the section called “Crie e gerencie um ambiente Amazon EVS”. Para ver todas as ações, recursos e chaves de condição disponíveis do Amazon EVS, consulte Ações na Referência de autorização de serviço.
5. Escolha Próximo.
6. Em Nome da política, insira um nome de política significativo para identificar essa política.
7. Revise as permissões definidas nesta política.
8. (Opcional) Adicione tags para ajudar a identificar, organizar ou pesquisar esse recurso.
9. Selecione Criar política.
10. No menu à esquerda, escolha Funções.
11. Selecione Criar perfil.
12. Para Tipo de entidade confiável, escolha Conta da AWS.
13. Em An Conta da AWS , especifique a conta na qual você deseja realizar ações do Amazon EVS e escolha Avançar.
14. Na página Adicionar permissões, selecione a política de permissões que você criou anteriormente e escolha Avançar.
15. Em Nome da função, insira um nome significativo para identificar essa função.
16. Revise a política de confiança e certifique-se de que a correta Conta da AWS esteja listada como a principal.

17. (Opcional) Adicione tags para ajudar a identificar, organizar ou pesquisar esse recurso.
18. Selecione Criar perfil.

AWS CLI

1. Copie o conteúdo a seguir em um arquivo JSON de política de confiança. Para o ARN principal, substitua o Conta da AWS ID e o `service-user` nome do exemplo por seu próprio Conta da AWS ID e nome de usuário do IAM.

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

2. Crie a função. `evs-environment-role-trust-policy.json`Substitua pelo nome do arquivo da política de confiança.

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

3. Crie uma política de permissões que habilite as operações do Amazon EVS e anexe a política à função. Substitua `myAmazonEVSEnvironmentRole` pelo nome da função. Para visualizar um exemplo de política, consulte the section called “Crie e gerencie um ambiente Amazon EVS”. Para ver todas as ações, recursos e chaves de condição disponíveis do Amazon EVS, consulte Ações na Referência de autorização de serviço.

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

Inscreva-se em um plano AWS Business, AWS Enterprise On-Ramp ou Enterprise AWS Support

O Amazon EVS exige que os clientes estejam inscritos em um plano AWS Business, AWS Enterprise On-Ramp ou Enterprise AWS Support para receber acesso contínuo ao suporte técnico e orientação arquitetônica. AWS O Business Support é o nível mínimo de AWS suporte que atende aos requisitos do Amazon EVS. Se você tiver cargas de trabalho essenciais para os negócios, recomendamos que você se inscreva nos planos Enterprise On-Ramp ou AWS Enterprise Support. AWS Para obter mais informações, consulte Compare AWS Support Plans.

> **Important**
>
> A criação do ambiente Amazon EVS falhará se você não se inscrever em um plano AWS Business, AWS Enterprise On-Ramp ou Enterprise AWS Support.

Verifique as cotas

Para permitir a criação do ambiente Amazon EVS, certifique-se de que sua conta tenha as cotas mínimas exigidas em nível de conta. Para obter mais informações, consulte Cotas de serviço.

> **Important**
>
> A criação do ambiente Amazon EVS falhará se a contagem de hosts por valor da cota do ambiente EVS não for pelo menos 4.

Planejar tamanhos de CIDR de VPC

Ao criar um ambiente Amazon EVS, você precisa especificar um bloco CIDR de VPC. O bloco CIDR da VPC não pode ser alterado após a criação do ambiente e precisará ter espaço suficiente reservado para acomodar as sub-redes e os hosts EVS necessários que o Amazon EVS cria durante a implantação do ambiente. Como resultado, é fundamental planejar cuidadosamente o tamanho do bloco CIDR, levando em consideração os requisitos do Amazon EVS e suas necessidades futuras de escalabilidade antes da implantação. O Amazon EVS exige um bloco CIDR VPC com um tamanho mínimo de /22 máscara de rede para permitir espaço suficiente para as sub-redes e hosts EVS

necessários. Para obter mais informações, consulte the section called “Considerações sobre a rede Amazon EVS”.

> **Important**
>
> Certifique-se de ter espaço de endereço IP suficiente para sua sub-rede VPC e para as sub-redes de VLAN que o Amazon EVS cria para dispositivos VCF. O bloco CIDR da VPC deve ter um tamanho mínimo de máscara de rede /22 para permitir espaço suficiente para as sub-redes e hosts EVS necessários.

> **Note**
>
> O Amazon EVS não oferece suporte IPv6 no momento.

Crie uma VPC com sub-redes

O Amazon EVS implanta seu ambiente em uma VPC que você fornece. Essa VPC deve conter uma sub-rede para acesso ao serviço Amazon EVS (). the section called “Sub-rede de acesso ao serviço” Para ver as etapas para criar uma VPC com sub-redes para o Amazon EVS, consulte. the section called “Crie uma VPC com sub-redes e tabelas de rotas”

Configurar a tabela de rotas principal da VPC

As sub-redes de VLAN do Amazon EVS estão implicitamente associadas à tabela de rotas principal da VPC. Para habilitar a conectividade com serviços dependentes, como DNS ou sistemas locais, para uma implantação bem-sucedida do ambiente, você deve configurar a tabela de rotas principal para permitir o tráfego para esses sistemas. Para obter mais informações, consulte the section called “Associe explicitamente as sub-redes de VLAN do Amazon EVS a uma tabela de rotas da VPC”.

> **Important**
>
> O Amazon EVS suporta o uso de uma tabela de rotas personalizada somente após a criação do ambiente Amazon EVS. Tabelas de rotas personalizadas não devem ser usadas durante a criação do ambiente Amazon EVS, pois isso pode resultar em problemas de conectividade.

Requisitos de rota de gateway

Configure rotas para esses tipos de gateway com base em seus requisitos de conectividade:

- Gateway NAT (NGW)
  - Opcional para acesso somente de saída à Internet.
  - Deve estar em uma sub-rede pública com acesso ao gateway da Internet.
  - Adicione rotas de sub-redes privadas e sub-redes EVS VLAN ao gateway NAT.
  - Para obter mais informações, consulte Trabalhar com gateways NAT no Guia do usuário da Amazon VPC.
- Gateway de trânsito (TGW)
  - Necessário para conectividade local via AWS Direct Connect e AWS Site-to-Site VPN.
  - Adicione rotas para intervalos de rede locais.
  - Configure a propagação da rota se estiver usando o BGP.
  - Para obter mais informações, consulte Transit Gateways no Amazon VPC Transit Gateways no Guia do usuário do Amazon VPC.

Práticas recomendadas

- Documente todas as configurações da tabela de rotas.
- Use convenções de nomenclatura consistentes.
- Audite regularmente suas tabelas de rotas.
- Teste a conectividade depois de fazer alterações.
- Faça backup das configurações da tabela de rotas.
- Monitore a integridade e a propagação da rota.

Para obter mais informações sobre como trabalhar com tabelas de rotas, consulte Configurar tabelas de rotas no Guia do usuário da Amazon VPC.

Configure o conjunto de opções DHCP da sua VPC

Important

A implantação do seu ambiente falhará se você não atender aos seguintes requisitos do Amazon EVS:

- Inclua um endereço IP do servidor DNS primário e um endereço IP do servidor DNS secundário no conjunto de opções DHCP.
- Inclua uma zona de consulta direta de DNS com registros A para cada dispositivo de gerenciamento VCF e host Amazon EVS em sua implantação.
- Inclua uma zona de pesquisa reversa de DNS com registros PTR para cada dispositivo de gerenciamento VCF e host Amazon EVS em sua implantação.
- Configure a tabela de rotas principal da VPC para garantir que exista uma rota para seus servidores DNS.
- Verifique se seu registro de nome de domínio é válido e não expirou e se não há nomes de host ou endereços IP duplicados.
- Configure seus grupos de segurança e listas de controle de acesso à rede (ACLs) para permitir que o Amazon EVS se comunique com:
  - Servidores DNS na TCP/UDP porta 53.
  - Sub-rede VLAN de gerenciamento de host via HTTPS e SSH.
  - Sub-rede VLAN de gerenciamento por HTTPS e SSH.

Para obter mais informações, consulte the section called “Configurar servidores de DNS e NTP usando o conjunto de opções de DHCP da VPC”.

Crie e configure a infraestrutura do VPC Route Server

O Amazon EVS usa o Amazon VPC Route Server para habilitar o roteamento dinâmico baseado em BGP para sua rede subjacente VPC. Você deve especificar um servidor de rotas que compartilhe rotas para pelo menos dois endpoints do servidor de rotas na sub-rede de acesso ao serviço. O ASN do par configurado nos pares de servidor de rotas deve corresponder e os endereços IP do par devem ser exclusivos.

Important

A implantação do seu ambiente falhará se você não atender a esses requisitos do Amazon EVS para a configuração do VPC Route Server:

- Você deve configurar pelo menos dois endpoints do servidor de rotas na sub-rede de acesso ao serviço.
- Ao configurar o Border Gateway Protocol (BGP) para o gateway de nível 0, o valor do ASN de mesmo nível do VPC Route Server deve corresponder ao valor do ASN de mesmo nível do NSX Edge.
- Ao criar os dois pares de servidores de rotas, você deve usar um endereço IP exclusivo da VLAN de uplink do NSX para cada endpoint. Esses dois endereços IP serão atribuídos às bordas do NSX durante a implantação do ambiente Amazon EVS.
- Ao habilitar a propagação do Route Server, você deve garantir que todas as tabelas de rotas que estão sendo propagadas tenham pelo menos uma associação explícita de sub-rede. O anúncio da rota BGP falhará se as tabelas de rotas propagadas não tiverem uma associação explícita de sub-rede.

Note

Para a detecção de atividade entre pares do Route Server, o Amazon EVS suporta apenas o mecanismo padrão de manutenção de atividade do BGP. O Amazon EVS não oferece suporte à detecção de encaminhamento bidirecional (BFD) de vários saltos.

Pré-requisitos

Antes de começar, você precisa de:

- Uma sub-rede VPC para seu servidor de rotas.
- Permissões do IAM para gerenciar recursos do VPC Route Server.
- Um valor BGP ASN para o servidor de rotas (ASN do lado da Amazon). O valor deve estar entre 1 e 4294967295.

- Um ASN ponto a ponto para emparelhar seu servidor de rotas com o gateway NSX Tier-0. Os valores de ASN de mesmo nível inseridos no servidor de rotas e no gateway NSX Tier-0 devem corresponder. O ASN padrão para um dispositivo NSX Edge é 65000.

Etapas

Para ver as etapas de configuração do VPC Route Server, consulte o tutorial de introdução do Route Server.

> **Note**
>
> Se você estiver usando um gateway NAT ou um gateway de trânsito, certifique-se de que seu servidor de rotas esteja configurado corretamente para propagar as rotas do NSX para a (s) tabela (s) de rotas da VPC.

> **Note**
>
> Recomendamos que você habilite rotas persistentes para a instância do servidor de rotas com uma duração persistente entre 1 e 5 minutos. Se ativada, as rotas serão preservadas no banco de dados de roteamento do servidor de rotas, mesmo que todas as sessões do BGP terminem.

> **Note**
>
> O status de conectividade do BGP ficará inativo até que o ambiente Amazon EVS esteja implantado e operacional.

Crie um gateway de trânsito para conectividade local

Você pode configurar a conectividade do seu data center local Direct Connect com sua AWS infraestrutura usando um gateway de trânsito associado ou usando um anexo de AWS Site-to-Site VPN a um gateway de trânsito. Para obter mais informações, consulte the section called “Configurar a conectividade de rede local (opcional)”.

Crie uma reserva de EC2 capacidade da Amazon

O Amazon EVS lança instâncias Amazon EC2 i4i.metal que representam hosts ESX em seu ambiente Amazon EVS. Para garantir que você tenha capacidade suficiente de instância i4i.metal disponível quando precisar, recomendamos que você solicite uma reserva de capacidade da Amazon EC2 . É possível criar uma reserva de capacidade a qualquer momento e escolher quando ela começa. Você pode solicitar uma reserva de capacidade para uso imediato ou solicitar uma reserva de capacidade para uma data futura. Para obter mais informações, consulte Reservar capacidade computacional com reservas de capacidade EC2 sob demanda no Guia do usuário do Amazon Elastic Compute Cloud.

Configure o AWS CLI

AWS CLI É uma ferramenta de linha de comando para trabalhar Serviços da AWS, incluindo o Amazon EVS. Ele também é usado para autenticar usuários ou funções do IAM para acessar o ambiente de virtualização do Amazon EVS e outros AWS recursos da sua máquina local. Para provisionar AWS recursos a partir da linha de comando, você precisa obter um ID de chave de AWS acesso e uma chave secreta para usar na linha de comando. Em seguida, você precisará configurar essas credenciais na AWS CLI. Para obter mais informações, consulte Configurar o AWS CLI no Guia do AWS Command Line Interface usuário para a versão 2.

Crie um Amazon EC2 key pair

O Amazon EVS usa um par de Amazon EC2 chaves que você fornece durante a criação do ambiente para se conectar aos seus hosts. Para criar um par de chaves, siga as etapas em Criar um par de chaves para sua Amazon EC2 instância no Guia do Amazon Elastic Compute Cloud usuário.

Prepare seu ambiente para o VMware Cloud Foundation (VCF)

Antes de implantar seu ambiente Amazon EVS, seu ambiente deve atender aos requisitos de infraestrutura do VMware Cloud Foundation (VCF). Para ver os pré-requisitos detalhados do VCF, consulte a pasta de trabalho de planejamento e preparação na documentação do VMware produto Cloud Foundation.

Você também deve se familiarizar com os requisitos do VCF 5.2.x. Consulte as notas de lançamento do VCF 5.2.x para obter informações relevantes sobre a versão.

> **Note**
>
> Para obter informações sobre as versões do VCF fornecidas pelo Amazon EVS, consulte. the section called “Versões e EC2 instâncias do VCF”

Adquirir chaves de licença do VCF

Para usar o Amazon EVS, você precisa fornecer uma chave de solução VCF e uma chave de licença vSAN. A chave da solução VCF deve ter pelo menos 256 núcleos. A chave de licença do vSAN deve ter pelo menos 110 TiB de capacidade do vSAN. Para obter mais informações sobre licenças VCF, consulte Gerenciamento de chaves de licença no VMware Cloud Foundation no Guia de administração do VMware Cloud Foundation.

> **Important**
>
> Use a interface de usuário do SDDC Manager para gerenciar a solução VCF e as chaves de licença do vSAN. O Amazon EVS exige que você mantenha uma solução VCF válida e as chaves de licença do vSAN no SDDC Manager para que o serviço funcione adequadamente.

> **Note**
>
> Sua licença VCF estará disponível para o Amazon EVS em todas as AWS regiões para fins de conformidade com a licença. O Amazon EVS não valida as chaves de licença. Para validar as chaves de licença, visite o suporte da Broadcom.

VMware Pré-requisitos do HCX

Você pode usar o VMware HCX para migrar suas cargas de trabalho VMware baseadas existentes para o Amazon EVS. Antes de usar o VMware HCX com o Amazon EVS, certifique-se de que as seguintes tarefas pré-solicitadas tenham sido concluídas.

> **Note**
>
> VMware O HCX não está instalado no ambiente EVS por padrão.

- Antes de usar o VMware HCX com o Amazon EVS, os requisitos mínimos de base de rede devem ser atendidos. Para obter mais informações, consulte Requisitos mínimos do Network Underlay no Guia do usuário do VMware HCX.
- Confirme se o VMware NSX está instalado e configurado no ambiente. Para obter mais informações, consulte o Guia de instalação do VMware NSX.
- Certifique-se de que o VMware HCX esteja ativado e instalado no ambiente. Para obter mais informações sobre como ativar e instalar o VMware HCX, consulte Sobre como começar a usar o VMware HCX no Guia de introdução ao HCX. VMware
- Se você precisar de conectividade HCX com a Internet, deverá concluir as seguintes tarefas de pré-requisito:
  - Certifique-se de que sua cota de IPAM para o comprimento da máscara de rede de blocos IPv4 CIDR públicos contíguos fornecidos pela Amazon seja /28 ou maior.

    > **Important**
    >
    > Para conectividade HCX com a Internet, o Amazon EVS exige o uso do bloco IPv4 CIDR de um pool IPAM público com um comprimento de máscara de rede de /28 ou maior. O uso de qualquer bloco CIDR com um comprimento de máscara de rede menor que /28 resultará em problemas de conectividade HCX. Para obter mais informações sobre o aumento das cotas do IPAM, consulte Cotas para seu IPAM.

  - Crie um IPAM e um pool IPv4 IPAM público com CIDR que tenha um comprimento mínimo de máscara de rede de /28.
  - Aloque pelo menos dois endereços IP elásticos (EIPs) do pool IPAM para os dispositivos HCX Manager e HCX Interconnect (HCX-IX). Aloque um endereço IP elástico adicional para cada dispositivo de rede HCX que você precisa implantar.
  - Adicione o bloco IPv4 CIDR público como um CIDR adicional à sua VPC.

Para obter mais informações sobre a configuração do HCX, consulte the section called “Escolha sua opção de conectividade HCX” e. the section called “Opções de conectividade HCX”

Lista de verificação de pré-requisitos de implantação do Amazon EVS

Esta seção contém uma lista de pré-requisitos que devem ser preenchidos para permitir a implantação bem-sucedida do ambiente Amazon EVS.

Informações sobre a chave de licença do VCF

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID do site	ID do site fornecido pela Broadcom para acesso ao portal de suporte da Broadcom.	É necessário fornecer uma ID do site da Broadcom na solicitação de criação do ambiente EVS.	01234567
Chave de solução do VCF	Uma única chave de licença do VCF que desbloqueia recursos de toda a pilha do VCF, incluindo vSphere, NSX, SDDC Manager e vCenter Server.	Deve fornecer uma chave de solução VCF ativa válida na solicitação de criação do ambiente EVS. A chave ainda não pode estar em uso por um ambiente EVS existente.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ
Chave de licença do vSAN	Uma chave de licença do vSAN permite que você ative e use o software vSAN em um ambiente VCF.	Deve fornecer uma chave de licença ativa válida do vSAN na solicitação de criação do ambiente EVS. A chave ainda não pode estar em uso por um ambiente EVS existente.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

AWS informações da conta e da região

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
AWS número de identificação da conta	A AWS conta permite criar e gerenciar AWS recursos e acessar AWS serviços.	Deve ter acesso a uma AWS conta.	999999999999
AWS Região	Uma área geográfica física onde AWS mantém vários data centers isolados chamados de zonas de disponibilidade.	É necessário especificar uma AWS região na qual o Amazon EVS possa ser implantado. Para obter uma lista das regiões em que o Amazon EVS está disponível atualmente, consulte os endpoints e cotas do Amazon Elastic VMware Service no Guia de referência AWS geral.	Oeste dos EUA (Oregon)

AWS Transit Gateway para conectividade de data center local

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID de gateway de trânsito	Um gateway de trânsito atua como um roteador virtual regional para o tráfego que flui entre sua VPC e as redes locais.	É necessário usar um gateway de trânsito para conectar um ambiente Amazon EVS às suas redes locais.	Exemplo do TGW-0262A0E521

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
Método de conexão	Para conectar suas redes locais a um ambiente Amazon EVS, você deve usar um gateway de trânsito com AWS Direct Connect ou AWS Site-to-Site VPN.	Determine se você usará AWS Direct Connect, AWS Site-to-Site VPN ou uma combinação de ambos. Para obter mais informações sobre como usar Site-to-Site VPN com Direct Connect, consulte AWS Site-to-Site VPN IP privada com AWS Direct Connect.	AWS Site-to-Site VPN com AWS Direct Connect

VPC para o ambiente Amazon EVS

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID da VPC	Uma VPC é uma rede virtual que se assemelha muito a uma rede tradicional que você operaria em seu próprio data center.	Qualquer Amazon VPC pode ser usada para implantação do ambiente.	vpc-0abcdef1234567890
Bloco CIDR VPC	Na Amazon VPC, um bloco CIDR define o intervalo de endereços IP disponíveis na sua VPC.	Um bloco CIDR RFC 1918 com um tamanho mínimo de máscara de rede /22. O bloco CIDR da VPC deve ser dimensionado adequadamente para acomodar	10.1.0.0/20

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
		todas as sub-redes e hosts do EVS a serem implantados em sua VPC. Esse bloco CIDR deve ser exclusivo em seus ambientes.	

Sub-redes VPC para ambiente EVS

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID da sub-rede de acesso ao serviço	Uma sub-rede de acesso ao serviço é uma sub-rede VPC padrão que permite o acesso aos serviços do Amazon EVS. Para obter mais informações, consulte the section called “Sub-rede de acesso ao serviço”.	Qualquer sub-rede VPC pode ser usada, desde que a sub-rede tenha o tamanho apropriado dentro da VPC. Sugerimos especificar um bloco CIDR de sub-rede VPC com uma máscara de rede de /24.	sub-rede - abcdef1234567890e
CIDR da sub-rede de acesso ao serviço	um bloco CIDR de sub-rede VPC é um intervalo de endereços IP, definido usando a notação CIDR, que é alocado a uma sub-rede específica dentro de uma VPC.	A sub-rede de acesso ao serviço deve ser dimensionada adequadamente para acomodar também as outras sub-redes e hosts EVS a serem implantados em sua VPC. Sugerimos especificar um bloco CIDR de sub-	10.1.0.0/24

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
		rede VPC com uma máscara de rede de /24.	
AWS ID da zona de disponibilidade na região	Um local distinto dentro de uma AWS região, projetado para ser isolado de falhas em outras AZs, e consiste em um ou mais data centers.	Você pode especificar a zona de disponibilidade na qual as sub-redes VPC são implantadas durante a criação da sub-rede. Para obter mais informações, consulte Criar uma sub-rede no Guia do usuário da Amazon VPC.	us-west-2a

Sub-redes EVS VLAN para ambiente EVS

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
VLAN CIDR de gerenciamento de host	O bloco CIDR para a sub-rede VLAN de gerenciamento de host. Para obter mais informações, consulte the section called “Sub-rede VLAN de gerenciamento de host”.	Deve ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24. Não deve se sobrepor a nenhum bloco CIDR existente associado à VPC.	10.1.1.0/24
CIDR de VLAN do VMotion	O bloco CIDR para a sub-rede VLAN do vMotion. Para obter mais informações, consulte the section	Deve ter o mesmo tamanho da VLAN de gerenciamento do host.	10.1.2.0/24

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
	called “Sub-rede VLAN vMotion”.		
CIDR de VLAN do vSAN	O bloco CIDR para a sub-rede vSAN VLAN. Para obter mais informações, consulte the section called “Sub-rede vSAN VLAN”.	Deve ter o mesmo tamanho da VLAN de gerenciamento do host.	10.1.3.0/24
CIDRA DE CLÃ VTEP	O bloco CIDR para a sub-rede VLAN VTEP. Para obter mais informações, consulte the section called “Sub-rede VLAN VTEP”.	Deve ter o mesmo tamanho da VLAN de gerenciamento do host.	10.1.4.0/24
Edge VTEP VLAN CIDR	O bloco CIDR para a sub-rede VLAN VTEP de borda. Para obter mais informações, consulte the section called “Sub-rede Edge VTEP VLAN”.	Deve ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24. Não deve se sobrepor a nenhum bloco CIDR existente associado à VPC.	10.1.5.0/24
VM de gerenciamento VLAN CIDR	O bloco CIDR para a sub-rede VLAN da VM de gerenciam ento. Para obter mais informações, consulte the section called “Sub-rede VM VLAN de gerenciamento”.	Deve ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24. Não deve se sobrepor a nenhum bloco CIDR existente associado à VPC.	10.1.6.0/24

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
CIDR de VLAN de uplink HCX	O bloco CIDR para a sub-rede VLAN de uplink HCX. Para obter mais informaçõ es, consulte the section called “Sub-rede VLAN de uplink HCX”.	Deve ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24. Não deve se sobrepor a nenhum bloco CIDR existente associado à VPC.	10.1.7.0/24
VLAN CIDR de uplink NSX	O bloco CIDR para a sub-rede VLAN de uplink do NSX. Para obter mais informaçõ es, consulte the section called “Sub-rede VLAN de uplink NSX”.	Deve ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24. Não deve se sobrepor a nenhum bloco CIDR existente associado à VPC.	10.1.8.0/24
VLAN de expansão 1 CIDR	Bloco CIDR para a sub-rede VLAN de expansão. Para obter mais informações, consulte the section called “Sub-rede VLAN de expansão”.	Deve ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24. Não deve se sobrepor a nenhum bloco CIDR existente associado à VPC.	10.1.9.0/24
VLAN de expansão 2 CIDR	Bloco CIDR para a sub-rede VLAN de expansão. Para obter mais informações, consulte the section called “Sub-rede VLAN de expansão”.	Deve ter um tamanho mínimo de /28 máscara de rede e um tamanho máximo de /24. Não deve se sobrepor a nenhum bloco CIDR existente associado à VPC.	10.1.10.0/24

Infraestrutura de DNS e NTP

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
Endereço IP do servidor DNS primário	O servidor principal do sistema de nomes de domínio (DNS) usado como fonte confiável para todos os registros DNS do domínio.	Você pode usar qualquer IPv4 endereço válido e não utilizado dentro do intervalo de hosts utilizáveis.	10.1.1.10
Endereço IP do servidor DNS secundário	Um servidor DNS de backup para os registros DNS do domínio.	Você pode usar qualquer IPv4 endereço válido e não utilizado dentro do intervalo de hosts utilizáveis.	10.1.5.25
Endereço IP do servidor NTP	Um servidor de protocolo de horário de rede (NTP) é um dispositivo ou aplicativo que sincroniza relógios em uma rede usando o padrão NTP.	Você pode usar o Amazon Time Sync Service padrão com o endereço `169.254.169.123` IP local ou outro endereço IP do servidor NTP.	169.254.169.123 (Serviço de sincronização de horário da Amazon)
FQDN para implantação de VCF	Um nome de domínio totalmente qualificado (FQDN) é o nome absoluto de um dispositivo em uma rede. Um FQDN consiste em um nome de host e nome de domínio.	Um FQDN só pode conter caracteres alfanuméricos, o sinal de menos (-) e pontos que são usados como delimitador entre rótulos. Deve ser um FQDN exclusivo válido e não expirado.	versus local

Conjunto de opções VPC DHCP

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID do conjunto de opções DHCP	Um conjunto de opções DHCP é um grupo de configurações de rede usado por recursos em sua VPC, EC2 como instâncias, para se comunicar pela sua rede virtual.	Deve conter no mínimo 2 servidores DNS. Você pode usar o Route 53 ou servidores DNS personalizados. Também deve conter seu nome de domínio DNS e um servidor NTP.	dopt-0a1b2c3d

EC2 key pair

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
EC2 nome do par de chaves	Um EC2 key pair é um conjunto de credenciais de segurança usado para se conectar com segurança a uma instância da Amazon. EC2	O nome do par de chaves deve ser exclusivo.	`my-ec2-key-pair`

Tabelas de rotas da VPC

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID da tabela de rotas principal	Na Amazon VPC, a tabela de rotas principal é a tabela de rotas padrão criada automaticamente com	Deve ser configurado para permitir a conectividade com serviços dependentes, como DNS ou	rtb-0123456789abcdef0

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
	a VPC e controla o tráfego de qualquer sub-rede da VPC que não esteja explicita mente associada a uma tabela de rotas diferente. As sub-redes EVS VLAN são associadas implicita mente à tabela de rotas principal da sua VPC quando o Amazon EVS as cria.	sistemas locais, para que a implantação do ambiente seja bem-sucedida.	

Lista de controle de acesso à rede (ACL)

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID da ACL de rede	Uma lista de controle de acesso à rede (ACL) permite ou nega tráfego de entrada ou saída no nível da sub-rede.	É necessário permitir que o Amazon EVS se comunique com: • Servidores DNS na TCP/UDP porta 53. • Sub-rede VLAN de gerenciamento de host via HTTPS e SSH. • Gerenciamento da sub-rede VM VLAN por HTTPS e SSH.	acl-0f62c640e793a38a3

Registros DNS para componentes VCF

Componente	Description	Requisitos mínimos	Exemplo de endereço IP	Exemplo de nome de host
Host ESX 1	Endereço IP e nome do host definidos no registro A e no registro PTR do host ESX 1.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada host ESX em cada implantação do EVS.	10.1.0.10	sexi 01
Host ESX 2	Endereço IP e nome do host definidos no registro A e no registro PTR do host ESX 2.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada host ESX em cada implantação do EVS.	10.1.0.11	sex02
Host ESX 3	Endereço IP e nome do host definidos no registro A e no	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A	10.1.0.12	sexi 03

Componente	Description	Requisitos mínimos	Exemplo de endereço IP	Exemplo de nome de host
	registro PTR do host ESX 3.	e uma zona de pesquisa reversa com registros PTR criados para cada host ESX em cada implantação do EVS.		
Host ESX 4	Endereço IP e nome do host definidos no registro A e no registro PTR do host ESX 4.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada host ESX em cada implantação do EVS.	10.1.0.13	sexi 04

Componente	Description	Requisitos mínimos	Exemplo de endereço IP	Exemplo de nome de host
Dispositivo vCenter Server	Endereço IP e nome do host definidos no registro A e no registro PTR do dispositivo vCenter Server.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.10	vc01
Cluster do NSX Manager	Endereço IP e nome de host definidos no registro A e no registro PTR do cluster do NSX Manager.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.11	nsx

Componente	Description	Requisitos mínimos	Exemplo de endereço IP	Exemplo de nome de host
Dispositivo SDDC Manager	Endereço IP e nome de host definidos no registro A e no registro PTR do dispositivo SDDC Manager.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.12	sddcm01
Dispositivo Cloud Builder	Endereço IP e nome de host definidos no registro A e no registro PTR do dispositivo Cloud Builder.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.13	cb01

Componente	Description	Requisitos mínimos	Exemplo de endereço IP	Exemplo de nome de host
Dispositivo NSX Edge 1	Endereço IP e nome de host definidos no registro A e no registro PTR do dispositivo NSX Edge 1.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.14	borda 01
Dispositivo NSX Edge 2	Endereço IP e nome de host definidos no registro A e no registro PTR do dispositivo NSX Edge 2.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.15	borda 02

Componente	Description	Requisitos mínimos	Exemplo de endereço IP	Exemplo de nome de host
Dispositivo NSX Manager 1	Endereço IP e nome de host definidos no registro A e no registro PTR do dispositivo NSX Manager 1.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.16	nsx01
Dispositivo NSX Manager 2	Endereço IP e nome de host definidos no registro A e no registro PTR do dispositivo NSX Manager 2.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.17	nsx02

Componente	Description	Requisitos mínimos	Exemplo de endereço IP	Exemplo de nome de host
Dispositivo NSX Manager 3	Endereço IP e nome de host definidos no registro A e no registro PTR do dispositivo NSX Manager 3.	O Amazon EVS exige uma zona de pesquisa direta de DNS com registros A e uma zona de pesquisa reversa com registros PTR criados para cada dispositivo de gerenciamento de VCF em cada implantação do EVS.	10.1.5.18	nsx03

Infraestrutura do VPC Route Server

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID do servidor de rota	O Amazon EVS usa o Amazon VPC Route Server para habilitar o roteamento dinâmico baseado em BGP para sua rede subjacente VPC.	Você deve especificar um servidor de rotas que compartilhe rotas para pelo menos dois endpoints do servidor de rotas na sub-rede de acesso ao serviço. O ASN de mesmo nível configurado no servidor de rotas e o correspondente do NSX Edge devem corresponder, e os	rs-0a1b2c3d4e5f67890

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
		endereços IP de mesmo nível devem ser exclusivos.	

associação de servidores de rotas	A conexão entre um servidor de rotas e uma VPC.	Seu servidor de rotas deve estar associado à sua VPC.	<pre>{
			"RouteServerAssociation": {
			"RouteServerId": "rs-0a1b2c3d4e5f67890",
			"VpcId": "vpc-1",
			"State": "associating"
			}
			}</pre>

BGP ASN do lado do servidor de rotas VPC (ASN do lado da Amazon)	O ASN do lado da Amazon represent a o AWS lado da sessão do BGP entre o servidor de rotas VPC e o par do NSX Edge. Você especific a esse BGP ASN ao criar o servidor de rotas. Para obter mais informações, consulte Criar um servidor de rotas no Guia do usuário da Amazon VPC.	Esse valor deve ser exclusivo e estar no intervalo de 1 a 4294967295. AWS recomenda usar um ASN privado no intervalo 64512—655 34 (ASN de 16 bits) ou 4200000000— 4294967294 (ASN de 32 bits).	65001

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
ID do endpoint 1 do servidor de rotas	Um endpoint de servidor de rotas é um componente AWS gerenciado dentro de uma sub-rede que facilita as conexões BGP (Border Gateway Protocol) entre seu servidor de rotas e seus pares de BGP.	É necessário implantar o endpoint do servidor de rotas na sub-rede de acesso ao serviço.	rse-0123456789abcdef0
ID do servidor de rotas por 1	O peer do servidor de rotas é uma sessão de emparelhamento BGP entre um endpoint do servidor de rotas e o dispositivo implantado no (NSX Edge). AWS	O valor do ASN do mesmo nível especificado no par do servidor de rotas deve corresponder ao valor do ASN do mesmo nível usado para o gateway NSX Edge de nível 0.	rsp-0123456789abcdef0
endereço IP de par 1 do servidor de rotas (EVS NSX Edge 1 lado)	O endereço IP do servidor de rotas peer (`PeerAddress`).	É necessário usar um endereço IP exclusivo não utilizado da VLAN de uplink do NSX. O Amazon EVS aplicará esse endereço IP ao NSX Edge 1 como parte da implantação e emparelhará com o ponto final do servidor de rotas.	10.1.7.10

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
endereço ENI do endpoint ponto final do servidor de rotas	O endereço IP ENI do endpoint do servidor de rotas peer (). `EndpointEniAddress`	Gerado automatic amente pelo servidor de rotas na criação de pares.	10.1.7.11
ID do endpoint 2 do servidor de rotas	Um endpoint de servidor de rotas é um componente AWS gerenciado dentro de uma sub-rede que facilita as conexões BGP (Border Gateway Protocol) entre seu servidor de rotas e seus pares de BGP.	É necessário implantar o endpoint do servidor de rotas na sub-rede de acesso ao serviço.	rse-fedcba9876543210f
ID do servidor de rota peer 2 (EVS NSX Edge 2 side)	O peer do servidor de rotas é uma sessão de emparelhamento BGP entre um endpoint do servidor de rotas e o dispositivo implantado no (NSX Edge). AWS	O valor do ASN do mesmo nível especificado no par do servidor de rotas deve corresponder ao valor do ASN do mesmo nível usado para o gateway NSX Edge de nível 0.	rsp-fedcba9876543210f

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
endereço IP par 2 do servidor de rotas	O endereço IP do servidor de rotas peer (`PeerAddress`).	É necessário usar um endereço IP exclusivo da VLAN de uplink do NSX. O Amazon EVS aplicará esse endereço IP ao NSX Edge 2 como parte da implantação e emparelhará com o ponto final do servidor de rotas.	10.1.7.200
endereço ENI do endpoint peer 2 do servidor de rotas	O endereço IP ENI do endpoint do servidor de rotas peer (). `EndpointEniAddress`	Gerado automatic amente pelo servidor de rotas na criação de pares.	10.1.7.201
propagação do servidor de rotas	A propagação do servidor de rotas instala as rotas no FIB na tabela de rotas que você especificou.	É necessário especific ar a tabela de rotas associada à sua sub-rede de acesso ao serviço. No momento, o Amazon EVS só oferece suporte a IPv4 redes.	`{ "RouteServerEndpoint": { "RouteServerId": "rs-1", "RouteServerEndpointId": "rse-1", "VpcId": "vpc-1", "SubnetId": "subnet-1", "State": "pending" } }`
BGP ASN do lado de pares do NSX	BGP ASN para o lado NSX da conexão.	Sugira usar o ASN 65000 padrão do NSX	65000

Recursos de acesso à Internet HCX (opcional)

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
IDENTIFICAÇÃO IPAM	Amazon VPC IP Address Manager (IPAM) usado para gerenciar endereços IP para acesso HCX à Internet.	Deve ser configurado para fornecer IPv4 endereços públicos. Necessário somente para a configuração do acesso à Internet HCX.	ipam-0123456789abcdef0
ID do pool IPAM	Um pool IPv4 IPAM público de propriedade da Amazon que fornece endereços para componentes HCX.	Deve ser configurado como um IPv4 pool público. Necessário somente para a configuração do acesso à Internet HCX.	ipam-pool-0123456789abcdef0
Bloco CIDR de VLAN pública HCX	Um bloco IPv4 CIDR público secundário alocado do pool IPAM para a sub-rede VLAN pública HCX.	Deve ter uma máscara de rede /28 e ser alocada do pool público IPAM de propriedade da Amazon. Necessário somente para a configuração do acesso à Internet HCX.	18.97.137.0/28
Endereços IP elásticos	Endereços IP elásticos sequenciais alocados do pool IPAM para componentes HCX.	Mínimo de 3 EIPs do mesmo pool IPAM para HCX Manager, HCX Interconnect Appliance (HCX-IX) e HCX Network Extension (HCX-NE).	eipalloc-0123456789abcdef0, eipalloc-0123456789abcdef1, eipalloc-0123456789abcdef2

Componente	Description	Requisitos mínimos	Exemplo de valor (es)
		Necessário somente para a configuração do acesso à Internet HCX.	

Comece a usar o Amazon Elastic VMware Service

Use este guia para começar a usar o Amazon Elastic VMware Service (Amazon EVS). Você aprenderá a criar um ambiente Amazon EVS com hosts dentro da sua própria Amazon Virtual Private Cloud (VPC).

Depois de terminar, você terá um ambiente Amazon EVS que poderá usar para migrar suas cargas de trabalho baseadas no VMware vSphere para o. Nuvem AWS

> **Important**
>
> Para começar da forma mais simples e rápida possível, este tópico inclui etapas para criar uma VPC e especifica os requisitos mínimos para a configuração do servidor DNS e a criação do ambiente Amazon EVS. Antes de criar esses recursos, recomendamos que você planeje o espaço de endereço IP e a configuração do registro DNS que atendam aos seus requisitos. Você também deve se familiarizar com os requisitos do VCF 5.2.x. Consulte as notas de lançamento do VCF 5.2.x para obter informações relevantes sobre a versão.

> **Important**
>
> Para obter informações sobre as versões do VCF fornecidas pelo Amazon EVS, consulte. the section called “Versões e EC2 instâncias do VCF”

Tópicos

Pré-requisitos

Antes de começar, você deve concluir as tarefas de pré-requisito do Amazon EVS. Para obter mais informações, consulte Configurando o Amazon Elastic VMware Service.

Crie uma VPC com sub-redes e tabelas de rotas

> **Note**
>
> A VPC, as sub-redes e o ambiente Amazon EVS devem ser criados na mesma conta. O Amazon EVS não oferece suporte ao compartilhamento entre contas de sub-redes VPC ou ambientes Amazon EVS.

Example

Amazon VPC console

1. Abra o console do Amazon VPC.
2. No painel da VPC, escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).
4. Mantenha a opção Geração automática de tags de nome selecionada para criar tags de nome para os recursos da VPC, ou desmarque-a para fornecer suas próprias tags de nome para os recursos da VPC.
5. Para bloco IPv4 CIDR, insira um bloco IPv4 CIDR. Uma VPC deve ter um bloco IPv4 CIDR. Certifique-se de criar uma VPC com o tamanho adequado para acomodar as sub-redes do Amazon EVS. Para obter mais informações, consulte the section called “Considerações sobre a rede Amazon EVS”.

> **Note**
>
> IPv6 No momento, o Amazon EVS não oferece suporte.

6. Mantenha a locação como`Default`. Com essa opção selecionada, as EC2 instâncias que são executadas nessa VPC usarão o atributo de locação especificado quando as instâncias forem executadas. O Amazon EVS lança EC2 instâncias bare metal em seu nome.
7. Em Número de zonas de disponibilidade (AZs), escolha 1.

> **Note**
>
> No momento, o Amazon EVS só oferece suporte a implantações Single-AZ.

8. Expanda Personalizar AZs e escolha a AZ para suas sub-redes.

> **Note**
>
> Você deve implantar em uma AWS região em que o Amazon EVS seja suportado. Para obter mais informações sobre a disponibilidade da região do Amazon EVS, consulte endpoints e cotas do Amazon Elastic VMware Service no Guia de referência AWS geral.

9. (Opcional) Se você precisar de conectividade com a Internet, em Número de sub-redes públicas, escolha 1.
10. Em Número de sub-redes privadas, escolha 1. Essa sub-rede privada será usada como a sub-rede de acesso ao serviço que você forneceu ao Amazon EVS durante a etapa de criação do ambiente. Para obter mais informações, consulte the section called “Sub-rede de acesso ao serviço”.
11. Para escolher os intervalos de endereços IP para suas sub-redes, expanda Personalizar blocos CIDR de sub-redes.

> **Note**
>
> As sub-redes de VLAN do Amazon EVS também precisarão ser criadas a partir desse espaço CIDR da VPC. Certifique-se de deixar espaço suficiente no bloco CIDR da

VPC para as sub-redes da VLAN que o serviço exige. Para obter mais informações, consulte the section called “Considerações sobre a rede Amazon EVS”.

12. (Opcional) Para conceder acesso à Internet IPv4 aos recursos, para gateways NAT, escolha Em 1 AZ. Observe que existe um custo associado aos gateways NAT. Para obter mais informações, consulte Preços para gateways NAT.

> **Note**
>
> O Amazon EVS exige o uso de um gateway NAT para permitir a conectividade de saída com a Internet.

13. Em VPC endpoints (Endpoints de VPC), escolha None (Nenhum).

> **Note**
>
> No momento, o Amazon EVS não oferece suporte a endpoints VPC Amazon S3 de gateway. Para habilitar a Amazon S3 conectividade, você deve configurar uma interface VPC endpoint usando for. AWS PrivateLink Amazon S3Para obter mais informações, consulte AWS PrivateLink o Guia do usuário do Amazon Simple Storage Service. Amazon S3

14. Para opções de DNS, mantenha os padrões selecionados. O Amazon EVS exige que sua VPC tenha capacidade de resolução de DNS para todos os componentes do VCF.
15. (Opcional) Para adicionar uma tag à sua VPC, expanda Tags adicionais, escolha Adicionar nova tag e digite uma chave de tag e um valor de tag.
16. Escolha Criar VPC.

> **Note**
>
> Durante a criação da VPC, cria Amazon VPC automaticamente uma tabela de rotas principal e associa implicitamente sub-redes a ela por padrão.

AWS CLI

1. Abra uma sessão do terminal.

2. Crie uma VPC com uma sub-rede privada e uma sub-rede pública opcional em uma única zona de disponibilidade.

```
aws ec2 create-vpc \
  --cidr-block 10.0.0.0/16 \
  --instance-tenancy default \
  --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=evs-vpc}]'
---
. Store the VPC ID for use in subsequent commands.
+
[source,bash]
```

VPC_ID=$ (aws ec2 descrebe-vpcs\ --filters name=tag:name, values=EVS-VPC\ --query 'Vpcs [0]. VpcId'\ --texto de saída) ---

3. Ative nomes de host DNS e suporte a DNS.

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

4. Crie uma sub-rede privada na VPC.

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

5. Armazene o ID da sub-rede privada para uso em comandos subsequentes.

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

6. (Opcional) Crie uma sub-rede pública se for necessária conectividade com a Internet.

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

7. (Opcional) Armazene o ID da sub-rede pública para uso em comandos subsequentes.

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

8. (Opcional) Crie e conecte um gateway da Internet se a sub-rede pública for criada.

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

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

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

9. (Opcional) Crie um gateway NAT se for necessária conectividade com a Internet.

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

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

aws ec2 create-nat-gateway \
```

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

10. Crie e configure as tabelas de rotas necessárias.

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

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

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

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

11. Adicione as rotas necessárias às tabelas de rotas.

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

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

12. Associe as tabelas de rotas às suas sub-redes.

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

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

> **Note**
>
> Durante a criação da VPC, cria Amazon VPC automaticamente uma tabela de rotas principal e associa implicitamente sub-redes a ela por padrão.

Escolha sua opção de conectividade HCX

Selecione uma opção de conectividade para seu ambiente Amazon EVS:

- Conectividade privada: fornece caminhos de rede de alto desempenho para HCX, otimizando a confiabilidade e a consistência. Requer o uso do AWS Direct Connect ou Site-to-Site VPN para conectividade de rede externa.
- Conectividade com a Internet: usa a Internet pública para estabelecer um caminho de migração flexível e rápido de configurar. Requer o uso do VPC IP Address Manager (IPAM) e endereços IP elásticos.

Para uma análise detalhada, consultethe section called “Opções de conectividade HCX”.

Escolha sua opção:

- Opção A: Somente conectividade privada → Continuar parathe section called “Configurar a tabela de rotas principal da VPC”.
- Opção B: Conectividade com a Internet → Continuar parathe section called “Configuração de conectividade com a Internet HCX”.

Configuração de conectividade com a Internet HCX

> **Note**
>
> Ignore esta seção se você escolheu a conectividade privada HCX e continue. the section called “Configurar a tabela de rotas principal da VPC”

Para habilitar a conectividade HCX com a Internet para o Amazon EVS, você deve:

- Certifique-se de que sua cota do VPC IP Address Manager (IPAM) para o comprimento da máscara de rede de blocos CIDR públicos IPv4 contíguos fornecidos pela Amazon seja /28 ou maior.

  Important

  O uso de qualquer bloco IPv4 CIDR público contíguo fornecido pela Amazon com um comprimento de máscara de rede menor que /28 resultará em problemas de conectividade HCX. Para obter mais informações sobre o aumento das cotas do IPAM, consulte Cotas para seu IPAM.

- Crie um IPAM e um pool IPv4 IPAM público com um CIDR que tenha um comprimento mínimo de máscara de rede de /28.
- Aloque pelo menos dois endereços IP elásticos (EIPs) do pool IPAM para os dispositivos HCX Manager e HCX Interconnect (HCX-IX). Aloque um endereço IP elástico adicional para cada dispositivo de rede HCX que você precisa implantar.
- Adicione o bloco IPv4 CIDR público como um CIDR adicional à sua VPC.

Para obter mais informações sobre como gerenciar a conectividade HCX com a Internet após a criação do ambiente, consultethe section called “Conectividade pública HCX”.

Crie um IPAM

Siga estas etapas para criar um IPAM.

Note

Você pode usar o nível gratuito do IPAM para criar recursos do IPAM para uso com o Amazon EVS. Embora o IPAM em si seja gratuito com o nível gratuito, você é responsável pelos custos de outros AWS serviços usados em conjunto com o IPAM, como gateways NAT e quaisquer IPv4 endereços públicos usados que estejam além do limite do nível gratuito. Para obter mais informações sobre os preços do IPAM, consulte a página Amazon VPC de preços.

> **Note**
>
> CIDRs No momento, o Amazon EVS não oferece suporte ao IPv6 Global Unicast Address (GUA) privado.

Crie um pool IPv4 IPAM público

Siga estas etapas para criar um IPv4 pool público.

IPAM console

1. Abra o console do IPAM.
2. No painel de navegação, selecione Pools (Grupos).
3. Escolha o escopo público. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. Selecione Criar.
5. (Opcional) Adicione uma Name tag (Etiqueta de nome) e uma Description (Descrição) para o grupo.
6. Em Família de endereços, escolha IPv4.
7. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada.
8. Em Locale (Local), escolha o local do grupo. A localidade é a AWS região em que você deseja que esse pool IPAM esteja disponível para alocações. A localidade escolhida deve corresponder à AWS região em que sua VPC está implantada.
9. Em Serviço, escolha EC2 (EIP/VPC). Isso anunciará CIDRs alocado desse pool para o EC2 serviço da Amazon (para endereços IP elásticos).
10. Em Origem de IP público, escolha Propriedade da Amazon.
11. Em CIDRs Para provisionar, escolha Adicionar CIDR público de propriedade da Amazon.
12. Em Máscara de rede, escolha um comprimento de máscara de rede CIDR. /28 é o comprimento mínimo necessário da máscara de rede.
13. Selecione Criar.

AWS CLI

1. Abra uma sessão do terminal.
2. Obtenha o ID do escopo público do seu IPAM.

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

3. Crie um pool IPAM no escopo público.

```
aws ec2 create-ipam-pool \
  --ipam-scope-id $SCOPE_ID \
  --address-family ipv4 \
  --no-auto-import \
  --locale us-east-2 \
  --description "Public IPv4 pool for HCX" \
  --tag-specifications 'ResourceType=ipam-pool,Tags=[{Key=Name,Value=evs-hcx-
public-pool}]' \
  --public-ip-source amazon \
  --aws-service ec2
```

4. Armazene o ID do pool para uso em comandos subsequentes.

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

5. Provisione um bloco CIDR do pool com um comprimento mínimo de máscara de rede de /28.

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

Aloque endereços IP elásticos do pool IPAM

Siga estas etapas para alocar endereços IP elásticos (EIPs) do pool IPAM para dispositivos HCX Service Mesh.

Amazon VPC console

1. Abra o console da Amazon VPC.
2. No painel de navegação, escolha Elastic IPs.
3. Escolha Alocar endereço IP elástico.
4. Selecione Alocar usando um pool IPv4 IPAM.
5. Selecione o IPv4 pool público de propriedade da Amazon que você configurou anteriormente.
6. Em Alocar método IPAM, escolha Inserir endereço manualmente no pool IPAM.

> **Important**
>
> Você não pode associar os dois primeiros EIPs ou o último EIP do bloco IPAM CIDR público à sub-rede da VLAN. Eles EIPs são reservados como rede, gateway padrão e endereços de transmissão. O Amazon EVS gera um erro de validação se você tentar EIPs associá-los à sub-rede da VLAN.

> **Important**
>
> Insira manualmente os endereços no pool IPAM para garantir EIPs que as reservas do Amazon EVS não sejam alocadas. Se você permitir que o IPAM escolha o EIP, o IPAM poderá alocar um EIP que o Amazon EVS reserva, causando falhas durante a associação do EIP à sub-rede da VLAN.

7. Especifique o EIP a ser alocado do pool IPAM.
8. Escolha Allocate.
9. Repita esse processo para alocar o restante EIPs que você precisa. É necessário alocar pelo menos dois EIPs do pool IPAM para os dispositivos HCX Manager e HCX Interconnect (HCX-IX). Aloque um EIP adicional para cada dispositivo de rede HCX que você precisa implantar.

AWS CLI

1. Abra uma sessão do terminal.
2. Obtenha o ID do pool IPAM que você criou anteriormente.

```
POOL_ID=$(aws ec2 describe-ipam-pools \
```

```
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)
```

3. Aloque endereços IP elásticos do pool IPAM. É necessário alocar pelo menos dois EIPs do pool IPAM para os dispositivos HCX Manager e HCX Interconnect (HCX-IX). Aloque um EIP adicional para cada dispositivo de rede HCX que você precisa implantar.

> **Important**
>
> Você não pode associar os dois primeiros EIPs ou o último EIP do bloco CIDR IPAM público a uma sub-rede VLAN. Eles EIPs são reservados como rede, gateway padrão e endereços de transmissão. O Amazon EVS gera um erro de validação se você tentar EIPs associá-los à sub-rede da VLAN.

> **Important**
>
> Insira manualmente os endereços no pool IPAM para garantir EIPs que as reservas do Amazon EVS não sejam alocadas. Se você permitir que o IPAM escolha o EIP, o IPAM poderá alocar um EIP que o Amazon EVS reserva, causando falhas durante a associação do EIP à sub-rede da VLAN.

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

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

aws ec2 allocate-address \
  --domain vpc \
```

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

Adicione o bloco IPv4 CIDR público do pool IPAM à VPC para conectividade com a Internet HCX

Para habilitar a conectividade HCX com a Internet, você deve adicionar o bloco IPv4 CIDR público do pool IPAM à sua VPC como um CIDR adicional. O Amazon EVS usa esse bloco CIDR para conectar o VMware HCX à sua rede. Siga estas etapas para adicionar o bloco CIDR à sua VPC.

> **Important**
>
> Você deve inserir manualmente o bloco IPv4 CIDR que você adiciona à sua VPC. No momento, o Amazon EVS não oferece suporte ao uso de um bloco CIDR alocado pelo IPAM. O uso de um bloco CIDR alocado pelo IPAM pode resultar em falha na associação do EIP.

Amazon VPC console

1. Abra o console da Amazon VPC.
2. No painel de navegação, escolha Seu VPCs.
3. Selecione a VPC que você criou anteriormente e escolha Ações, Editar. CIDRs
4. Escolha Adicionar novo IPV4 CIDR.
5. Selecione a entrada manual IPV4 CIDR.
6. Especifique o bloco CIDR do pool IPAM público que você criou anteriormente.

AWS CLI

1. Abra uma sessão do terminal.
2. Obtenha o ID do pool IPAM e o bloco CIDR provisionado.

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

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

3. Adicione o bloco CIDR à sua VPC.

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

Configurar a tabela de rotas principal da VPC

As sub-redes de VLAN do Amazon EVS estão implicitamente associadas à tabela de rotas principal da VPC. Para habilitar a conectividade com serviços dependentes, como DNS ou sistemas locais, para uma implantação bem-sucedida do ambiente, você deve configurar a tabela de rotas principal para permitir o tráfego para esses sistemas. A tabela de rotas principal deve incluir uma rota para o CIDR da VPC. O uso da tabela de rotas principal só é necessário para a implantação inicial do ambiente Amazon EVS. Após a implantação do ambiente, você pode configurar seu ambiente para usar uma tabela de rotas personalizada. Para obter mais informações, consulte the section called “Configurar tabela de rotas personalizada”.

Após a implantação do ambiente, você deve associar explicitamente cada uma das sub-redes de VLAN do Amazon EVS a uma tabela de rotas em sua VPC. A conectividade do NSX falhará se suas sub-redes de VLAN não estiverem explicitamente associadas a uma tabela de rotas da VPC. É altamente recomendável que você associe explicitamente suas sub-redes a uma tabela de rotas personalizada após a implantação do ambiente. Para obter mais informações, consulte the section called “Configurar a tabela de rotas principal da VPC”.

> **Important**
>
> O Amazon EVS suporta o uso de uma tabela de rotas personalizada somente após a criação do ambiente Amazon EVS. Tabelas de rotas personalizadas não devem ser usadas durante a criação do ambiente Amazon EVS, pois isso pode resultar em problemas de conectividade.

Configurar servidores de DNS e NTP usando o conjunto de opções de DHCP da VPC

Important

A implantação do seu ambiente falhará se você não atender aos seguintes requisitos do Amazon EVS:

- Inclua um endereço IP do servidor DNS primário e um endereço IP do servidor DNS secundário no conjunto de opções DHCP.
- Inclua uma zona de consulta direta de DNS com registros A para cada dispositivo de gerenciamento VCF e host Amazon EVS em sua implantação.
- Inclua uma zona de pesquisa reversa de DNS com registros PTR para cada dispositivo de gerenciamento VCF e host Amazon EVS em sua implantação.
- Configure a tabela de rotas principal da VPC para garantir que exista uma rota para seus servidores DNS.
- Verifique se seu registro de nome de domínio é válido e não expirou e se não há nomes de host ou endereços IP duplicados.
- Configure seus grupos de segurança e listas de controle de acesso à rede (ACLs) para permitir que o Amazon EVS se comunique com:
  - Servidores DNS na TCP/UDP porta 53.
  - Sub-rede VLAN de gerenciamento de host via HTTPS e SSH.
  - Sub-rede VLAN de gerenciamento por HTTPS e SSH.

O Amazon EVS usa o conjunto de opções DHCP da sua VPC para recuperar o seguinte:

- Servidores DNS (Sistema de Nomes de Domínio) para resolução de endereços IP do host.
- Nomes de domínio para resolução de DNS.
- Servidores Network Time Protocol (NTP) para sincronização de horário.

Você pode criar um conjunto de opções DHCP usando o Amazon VPC console ou AWS CLI. Para obter mais informações, consulte Criar um conjunto de opções DHCP no Guia do Amazon VPC usuário.

Configurar servidores DNS

A configuração do DNS permite a resolução de nomes de host em seu ambiente Amazon EVS. Para implantar com sucesso um ambiente Amazon EVS, o conjunto de opções DHCP da sua VPC deve ter as seguintes configurações de DNS:

- Um endereço IP do servidor DNS primário e um endereço IP do servidor DNS secundário no conjunto de opções DHCP.
- Uma zona de consulta direta de DNS com registros A para cada dispositivo de gerenciamento VCF e host Amazon EVS em sua implantação.
- Uma zona de pesquisa reversa com registros PTR para cada dispositivo de gerenciamento VCF e host Amazon EVS em sua implantação. Para configuração de NTP, você pode usar o endereço `169.254.169.123` NTP padrão da Amazon ou outro IPv4 endereço de sua preferência.

Para obter mais informações sobre como configurar servidores DNS em um conjunto de opções DHCP, consulte Criar um conjunto de opções DHCP.

Configurar o DNS para conectividade local

Para conectividade local, recomendamos o uso de zonas hospedadas privadas do Route 53 com resolvedores de entrada. Essa configuração permite a resolução de DNS híbrida, na qual você pode usar o Route 53 para DNS interno em sua VPC e integrá-lo à sua infraestrutura de DNS local existente. Isso permite que os recursos em sua VPC resolvam nomes de domínio hospedados em sua rede local e vice-versa, sem exigir configurações complexas. Se necessário, você também pode usar seu próprio servidor DNS com os resolvedores de saída do Route 53. Para ver as etapas de configuração, consulte Criação de uma zona hospedada privada e Encaminhamento de consultas DNS de entrada para sua VPC no Amazon Route 53 Developer Guide.

> **Note**
>
> Usar o Route 53 e um servidor DNS (Sistema de Nomes de Domínio) personalizado no conjunto de opções DHCP pode causar um comportamento inesperado.

> **Note**
>
> Se você usa nomes de domínio DNS personalizados definidos em uma zona hospedada privada em Route 53, ou usa DNS privado com interface VPC endpoints (AWS PrivateLink),

você deve definir os atributos e como. `enableDnsHostnames` `enableDnsSupport` `true` Para obter mais informações, consulte Atributos de DNS para sua VPC.

Solucionar problemas de acessibilidade do DNS

O Amazon EVS exige uma conexão persistente com o SDDC Manager e os servidores DNS no conjunto de opções DHCP da sua VPC para alcançar registros de DNS. Se a conexão persistente com o SDDC Manager ficar indisponível, o Amazon EVS não poderá mais validar o status do ambiente e você poderá perder o acesso ao ambiente. Para obter as etapas para solucionar esse problema, consultethe section called “Falha na verificação de acessibilidade”.

Configurar servidores NTP

Os servidores NTP fornecem as horas para a rede. Uma referência de tempo consistente e precisa em sua EC2 instância da Amazon é crucial para muitas tarefas e processos do ambiente VCF. A sincronização de horário é essencial para:

- Registro e auditoria do sistema
- Operações de segurança
- Gerenciamento distribuído do sistema
- Solução de problemas

Você pode inserir os IPv4 endereços de até quatro servidores NTP no conjunto de opções DHCP da sua VPC. Você pode especificar o Amazon Time Sync Service no IPv4 endereço`169.254.169.123`. Por padrão, as EC2 instâncias da Amazon que o Amazon EVS implanta usam o Amazon Time Sync Service no IPv4 endereço. `169.254.169.123`

Para obter mais informações sobre servidores NTP, consulte RFC 2123. Para obter mais informações sobre o Amazon Time Sync Service, consulte Precision clock e sincronização de horário em sua EC2 instância e Configurar o NTP nos hosts do VMware Cloud Foundation na documentação do VMware Cloud Foundation.

Para definir as configurações de NTP

1. Escolha sua fonte de NTP:
   - Serviço Amazon Time Sync (recomendado)

- Servidores NTP personalizados

2. Adicione servidores NTP ao seu conjunto de opções de DHCP. Para obter mais informações, consulte Criar um conjunto de opções DHCP no Guia do usuário da Amazon VPC.
3. Verifique a sincronização de horário. Para obter mais informações sobre a configuração do conjunto de opções DHCP, consultethe section called “Configure o conjunto de opções DHCP da sua VPC”.

Configurar a conectividade de rede local (opcional)

Você pode configurar a conectividade do seu data center local Direct Connect com sua AWS infraestrutura usando um gateway de trânsito associado ou usando um anexo de AWS Site-to-Site VPN a um gateway de trânsito.

Para permitir a conectividade com sistemas locais para uma implantação bem-sucedida do ambiente, você deve configurar a tabela de rotas principal da VPC para permitir o tráfego para esses sistemas. Para obter mais informações, consulte the section called “Configurar a tabela de rotas principal da VPC”.

Depois que o ambiente Amazon EVS for criado, você deverá atualizar as tabelas de rotas do gateway de trânsito com a CIDRs VPC criada dentro do ambiente Amazon EVS. Para obter mais informações, consulte the section called “Configure tabelas de rotas do Transit Gateway e prefixos do Direct Connect para conectividade local (opcional)”.

Para obter mais informações sobre como configurar uma Direct Connect conexão, consulte Direct Connect gateways e associações de gateways de trânsito. Para obter mais informações sobre o uso de AWS Site-to-Site VPN com o AWS Transit Gateway, consulte Anexos de AWS Site-to-Site VPN em Amazon VPC Transit Gateways no Guia do usuário do Amazon VPC Transit Gateway.

> **Note**
>
> O Amazon EVS não oferece suporte à conectividade por meio de uma interface virtual privada (VIF) do AWS Direct Connect ou por meio de uma conexão AWS Site-to-Site VPN que termina diretamente na VPC subjacente.

Configurar uma instância do VPC Route Server com endpoints e pares

O Amazon EVS usa o Amazon VPC Route Server para habilitar o roteamento dinâmico baseado em BGP para sua rede subjacente VPC. Você deve especificar um servidor de rotas que compartilhe rotas para pelo menos dois endpoints do servidor de rotas na sub-rede de acesso ao serviço. O ASN do par configurado nos pares de servidor de rotas deve corresponder e os endereços IP do par devem ser exclusivos.

Se você estiver configurando o Route Server para conectividade HCX com a Internet, deverá configurar as propagações do Route Server para a sub-rede de acesso ao serviço e a sub-rede pública que você criou na primeira etapa deste procedimento.

Important

A implantação do seu ambiente falhará se você não atender a esses requisitos do Amazon EVS para a configuração do VPC Route Server:

- Você deve configurar pelo menos dois endpoints do servidor de rotas na sub-rede de acesso ao serviço.
- Ao configurar o Border Gateway Protocol (BGP) para o gateway de nível 0, o valor do ASN de mesmo nível do VPC Route Server deve corresponder ao valor do ASN de mesmo nível do NSX Edge.
- Ao criar os dois pares de servidores de rotas, você deve usar um endereço IP exclusivo da VLAN de uplink do NSX para cada endpoint. Esses dois endereços IP serão atribuídos às bordas do NSX durante a implantação do ambiente Amazon EVS.
- Ao habilitar a propagação do Route Server, você deve garantir que todas as tabelas de rotas que estão sendo propagadas tenham pelo menos uma associação explícita de sub-rede. O anúncio da rota BGP falhará se as tabelas de rotas propagadas não tiverem uma associação explícita de sub-rede.

Para obter mais informações sobre como configurar o VPC Route Server, consulte o tutorial de introdução do Route Server.

Important

Ao habilitar a propagação do Route Server, certifique-se de que todas as tabelas de rotas que estão sendo propagadas tenham pelo menos uma associação explícita de sub-rede. O anúncio da rota BGP falhará se a tabela de rotas tiver uma associação explícita de sub-rede.

Note

Para a detecção de atividade entre pares do Route Server, o Amazon EVS suporta apenas o mecanismo padrão de manutenção de atividade do BGP. O Amazon EVS não oferece suporte à detecção de encaminhamento bidirecional (BFD) de vários saltos.

Note

Recomendamos que você habilite rotas persistentes para a instância do servidor de rotas com uma duração persistente entre 1 e 5 minutos. Se ativada, as rotas serão preservadas no banco de dados de roteamento do servidor de rotas, mesmo que todas as sessões do BGP terminem. Para obter mais informações, consulte Criar um servidor de rotas no Guia Amazon VPC do usuário.

Note

Se você estiver usando um gateway NAT ou um gateway de trânsito, verifique se o servidor de rotas está configurado corretamente para propagar as rotas do NSX para a (s) tabela (s) de rotas da VPC.

Solução de problemas

Se você encontrar problemas:

- Verifique se cada tabela de rotas tem uma associação explícita de sub-rede.
- Verifique se os valores de ASN de mesmo nível inseridos para o servidor de rotas e o gateway NSX Tier-0 coincidem.

- Confirme se os endereços IP do endpoint do Route Server são exclusivos.
- Revise o status de propagação da rota em suas tabelas de rotas.
- Use o registro em pares do VPC Route Server para monitorar a integridade da sessão do BGP e solucionar problemas de conexão. Para obter mais informações, consulte Registro em pares do servidor Route no Guia do usuário da Amazon VPC.

Crie uma rede ACL para controlar o tráfego de sub-rede VLAN do Amazon EVS

O Amazon EVS usa uma lista de controle de acesso à rede (ACL) para controlar o tráfego de e para as sub-redes de VLAN do Amazon EVS. Você pode usar a ACL de rede padrão para sua VPC ou criar uma ACL de rede personalizada para sua VPC com regras semelhantes às regras de seus grupos de segurança para adicionar uma camada de segurança à sua VPC. Para obter mais informações, consulte Criar uma rede ACL para sua VPC no Guia do usuário da Amazon VPC.

Se você planeja configurar a conectividade HCX com a Internet, certifique-se de que as regras de ACL de rede que você configura permitam as conexões de entrada e saída necessárias para os componentes HCX. Para obter mais informações sobre os requisitos da porta HCX, consulte o Guia do usuário do VMware HCX.

> **Important**
>
> Se você estiver se conectando pela Internet, associar um endereço IP elástico a uma VLAN fornece acesso direto à Internet a todos os recursos dessa sub-rede da VLAN. Certifique-se de ter listas de controle de acesso à rede apropriadas configuradas para restringir o acesso conforme necessário para seus requisitos de segurança.

> **Important**
>
> EC2 os grupos de segurança não funcionam em interfaces de rede elásticas conectadas às sub-redes VLAN do Amazon EVS. Para controlar o tráfego de e para as sub-redes VLAN do Amazon EVS, você deve usar uma lista de controle de acesso à rede.

Crie um ambiente Amazon EVS

Important

Para começar da forma mais simples e rápida possível, este tópico inclui etapas para criar um ambiente Amazon EVS com configurações padrão. Antes de criar um ambiente, recomendamos que você se familiarize com todas as configurações e implante um ambiente com as configurações que atendam aos seus requisitos. Os ambientes só podem ser configurados durante a criação inicial do ambiente. Os ambientes não podem ser modificados depois de serem criados. Para uma visão geral de todas as configurações possíveis do ambiente Amazon EVS, consulte o Guia de referência da API Amazon EVS.

Note

Seu ID de ambiente estará disponível para o Amazon EVS em todas as AWS regiões para atender às necessidades de conformidade da licença VCF.

Note

Os ambientes Amazon EVS devem ser implantados na mesma região e zona de disponibilidade das sub-redes VPC e VPC.

Conclua esta etapa para criar um ambiente Amazon EVS com hosts e sub-redes de VLAN.

Example

Amazon EVS console

1. Acesse o console do Amazon EVS.

   Note

   Certifique-se de que a AWS região mostrada no canto superior direito do console seja a AWS região na qual você deseja criar seu ambiente. Se não estiver, escolha a lista

suspensa ao lado do nome da AWS região e escolha a AWS região que você deseja usar.

2. No painel de navegação, escolha Ambientes.
3. Selecione Criar ambiente.
4. Na página Validar requisitos do Amazon EVS, verifique se os requisitos de serviço foram atendidos. Para obter mais informações, consulte Configurando o Amazon Elastic VMware Service.
   a. (Opcional) Em Nome, insira um nome de ambiente.
   b. Para a versão Ambiente, escolha sua versão do VCF. Para obter informações sobre as versões do VCF fornecidas pelo Amazon EVS, consulte. the section called “Versões e EC2 instâncias do VCF”
   c. Em ID do site, insira sua ID do site Broadcom.
   d. Para a chave da solução VCF, insira uma chave da solução VCF (VMware vSphere 8 Enterprise Plus for VCF). Essa chave de licença não pode ser usada por um ambiente existente.

> **Note**
>
> A chave da solução VCF deve ter pelo menos 256 núcleos.

> **Note**
>
> Sua licença VCF estará disponível para o Amazon EVS em todas as AWS regiões para fins de conformidade com a licença. O Amazon EVS não valida as chaves de licença. Para validar as chaves de licença, visite o suporte da Broadcom.

> **Note**
>
> O Amazon EVS exige que você mantenha uma chave de solução VCF válida no SDDC Manager para que o serviço funcione adequadamente. Se você gerenciar a chave da solução VCF usando o vSphere Client após a implantação, deverá garantir

que as chaves também apareçam na tela de licenciamento da interface de usuário do SDDC Manager.

e. Para a chave de licença do vSAN, insira uma chave de licença do vSAN. Essa chave de licença não pode ser usada por um ambiente existente.

> **Note**
>
> A chave de licença do vSAN deve ter pelo menos 110 TiB de capacidade do vSAN.

> **Note**
>
> Sua licença VCF estará disponível para o Amazon EVS em todas as AWS regiões para fins de conformidade com a licença. O Amazon EVS não valida as chaves de licença. Para validar as chaves de licença, visite o suporte da Broadcom.

> **Note**
>
> O Amazon EVS exige que você mantenha uma chave de licença vSAN válida no SDDC Manager para escolher o serviço para funcionar corretamente. Se você gerenciar a chave de licença do vSAN usando o vSphere Client após a implantação, deverá garantir que as chaves também apareçam na tela de licenciamento da interface de usuário do SDDC Manager.

f. Para os termos da licença VCF, marque a caixa para confirmar que você comprou e continuará mantendo o número necessário de licenças de software VCF para cobrir todos os núcleos de processadores físicos no ambiente Amazon EVS. As informações sobre seu software VCF no Amazon EVS serão compartilhadas com a Broadcom para verificar a conformidade da licença.

g. Escolha Próximo.

5. Na página Especificar detalhes do host, conclua as etapas a seguir quatro vezes para adicionar quatro hosts ao ambiente. Os ambientes Amazon EVS exigem quatro hosts para a implantação inicial.

   a. Escolha Adicionar detalhes do host.

b. Em Nome do host DNS, insira o nome do host.

c. Por tipo de instância, escolha o tipo de EC2 instância.

d. Para a versão do host ESX, durante a criação do ambiente, uma versão padrão do ESX para a versão escolhida do VCF será usada. Consulte the section called “Versões e EC2 instâncias do VCF” para obter mais informações.

> **Important**
>
> Não interrompa nem encerre as EC2 instâncias que o Amazon EVS implanta. Essa ação resulta em perda de dados.

> **Note**
>
> No momento, o Amazon EVS só oferece suporte a EC2 instâncias i4i.metal.

e. Para o par de chaves SSH, escolha um par de chaves SSH para acesso SSH ao host.

f. Escolha Adicionar host.

6. Na página Configurar redes e conectividade, faça o seguinte.

a. Para os requisitos de conectividade HCX, selecione se você deseja usar o HCX com conectividade privada ou pela Internet.

b. Para VPC, escolha a VPC que você criou anteriormente.

c. (Somente para conexão com a Internet HCX) Para ACL de rede HCX, escolha a qual ACL de rede sua VLAN HCX será associada.

> **Important**
>
> É altamente recomendável que você crie uma ACL de rede personalizada dedicada à VLAN HCX. Para obter mais informações, consulte the section called “Configurar ACL de rede”.

d. Em Sub-rede de acesso ao serviço, escolha a sub-rede privada que foi criada quando você criou a VPC.

e. Para Grupo de segurança - opcional, você pode escolher até dois grupos de segurança que controlam a comunicação entre o plano de controle do Amazon EVS e a VPC. O Amazon EVS usa o grupo de segurança padrão se nenhum grupo de segurança for escolhido.

> **Note**
>
> Certifique-se de que os grupos de segurança que você escolher forneçam conectividade aos seus servidores DNS e sub-redes VLAN do Amazon EVS.

f. Em Conectividade de gerenciamento, insira os blocos CIDR a serem usados nas sub-redes de VLAN do Amazon EVS. Para o bloco CIDR de VLAN de uplink HCX, se estiver configurando uma VLAN HCX pública, você deverá especificar um bloco CIDR com um comprimento de máscara de rede de exatamente /28. O Amazon EVS gera um erro de validação se qualquer outro tamanho de bloco CIDR for especificado para a VLAN pública HCX. Para uma VLAN HCX privada e todos os outros blocos VLANs CIDR, o comprimento mínimo da máscara de rede que você pode usar é /28 e o máximo é /24.

> **Important**
>
> As sub-redes de VLAN do Amazon EVS só podem ser criadas durante a criação do ambiente Amazon EVS e não podem ser modificadas após a criação do ambiente. Você deve garantir que os blocos CIDR da sub-rede da VLAN estejam dimensionados adequadamente antes de criar o ambiente. Você não poderá adicionar sub-redes de VLAN após a implantação do ambiente. Para obter mais informações, consulte the section called “Considerações sobre a rede Amazon EVS”.

g. Em Expansão VLANs, insira os blocos CIDR para sub-redes VLAN adicionais do Amazon EVS que podem ser usadas para expandir os recursos do VCF no Amazon EVS, como ativar o NSX Federation.

h. Em Conectividade de carga de trabalho/VCF, insira o bloco CIDR para a VLAN de uplink do NSX e escolha dois VPC Route Server pares que se conectam aos endpoints do Route Server IDs pelo uplink do NSX.

> **Note**
>
> O Amazon EVS exige uma instância do VPC Route Server associada a dois endpoints do Route Server e dois pares do Route Server antes da implantação do EVS. Essa configuração permite o roteamento dinâmico baseado em BGP pelo

uplink do NSX. Para obter mais informações, consulte the section called “Configurar uma instância do VPC Route Server com endpoints e pares”.

i. Escolha Próximo.

7. Na página Especificar nomes de host DNS de gerenciamento, faça o seguinte.

   a. Em Nomes de host DNS do dispositivo de gerenciamento, insira os nomes de host DNS das máquinas virtuais para hospedar dispositivos de gerenciamento VCF. Se estiver usando o Route 53 como seu provedor de DNS, escolha também a zona hospedada que contém seus registros DNS.

   b. Em Credenciais, escolha se você gostaria de usar a chave KMS AWS gerenciada para o Secrets Manager ou uma chave KMS gerenciada pelo cliente que você fornece. Essa chave é usada para criptografar as credenciais do VCF necessárias para usar os dispositivos SDDC Manager, NSX Manager e vCenter.

   > **Note**
   >
   > Há custos de uso associados às chaves KMS gerenciadas pelo cliente. Para obter mais informações, consulte a página de preços do AWS KMS.

   c. Escolha Próximo.

8. (Opcional) Na página Adicionar tags, adicione as tags que você gostaria de atribuir a esse ambiente e escolha Avançar.

   > **Note**
   >
   > Os hosts criados como parte desse ambiente receberão a seguinte tag:`DoNotDelete-EVS-<environmentid>-<hostname>`.

   > **Note**
   >
   > As tags associadas ao ambiente Amazon EVS não se propagam para AWS recursos subjacentes, como EC2 instâncias. Você pode criar tags nos AWS recursos subjacentes usando o respectivo console de serviço ou AWS CLI o.

9. Na página Revisar e criar, revise sua configuração e escolha Criar ambiente.

> **Important**
>
> Durante a implantação do ambiente, o Amazon EVS cria as sub-redes EVS VLAN e as associa implicitamente à tabela de rotas principal. Após a conclusão da implantação, você deve associar explicitamente as sub-redes de VLAN do Amazon EVS a uma tabela de rotas para fins de conectividade do NSX. Para obter mais informações, consulte the section called “Associe explicitamente as sub-redes de VLAN do Amazon EVS a uma tabela de rotas da VPC”.

> **Note**
>
> O Amazon EVS implanta uma versão recente do pacote do VMware Cloud Foundation que pode não incluir atualizações individuais de produtos, conhecidas como patches assíncronos. Após a conclusão dessa implantação, é altamente recomendável que você revise e atualize produtos individuais usando a ferramenta de patch assíncrono (ferramenta AP) da Broadcom ou a automação de LCM no produto SDDC Manager. Os upgrades do NSX devem ser feitos fora do SDDC Manager.

> **Note**
>
> A criação do ambiente pode levar várias horas.

AWS CLI

1. Abra uma sessão do terminal.
2. Crie um ambiente Amazon EVS. Abaixo está um exemplo de `aws evs create-environment` solicitação.

> **Important**
>
> Antes de executar o `aws evs create-environment` comando, verifique se todos os pré-requisitos do Amazon EVS foram atendidos. A implantação do ambiente falhará

se os pré-requisitos não forem atendidos. Para obter mais informações, consulte Configurando o Amazon Elastic VMware Service.

Important

Durante a implantação do ambiente, o Amazon EVS cria as sub-redes EVS VLAN e as associa implicitamente à tabela de rotas principal. Após a conclusão da implantação, você deve associar explicitamente as sub-redes de VLAN do Amazon EVS a uma tabela de rotas para fins de conectividade do NSX. Para obter mais informações, consulte the section called “Associe explicitamente as sub-redes de VLAN do Amazon EVS a uma tabela de rotas da VPC”.

Note

O Amazon EVS implanta uma versão recente do pacote do VMware Cloud Foundation que pode não incluir atualizações individuais de produtos, conhecidas como patches assíncronos. Após a conclusão dessa implantação, é altamente recomendável que você revise e atualize produtos individuais usando a ferramenta de patch assíncrono (ferramenta AP) da Broadcom ou a automação de LCM integrada no produto SDDC Manager. Os upgrades do NSX devem ser feitos fora do SDDC Manager.

Note

A implantação do ambiente pode levar várias horas.

- Para `--vpc-id`, especifique a VPC que você criou anteriormente com um intervalo IPv4 CIDR mínimo de /22.
- Para `--service-access-subnet-id`, especifique o ID exclusivo da sub-rede privada que foi criada quando você criou a VPC.
- Para `--vcf-version`, consulte as the section called “Versões e EC2 instâncias do VCF” versões do VCF fornecidas pelo Amazon EVS,

- Com `--terms-accepted`, você confirma que comprou e continuará mantendo o número necessário de licenças de software VCF para cobrir todos os núcleos físicos do processador no ambiente Amazon EVS. As informações sobre seu software VCF no Amazon EVS serão compartilhadas com a Broadcom para verificar a conformidade da licença.
- Para `--license-info`, insira a chave da solução VCF (VMware vSphere 8 Enterprise Plus for VCF) e a chave de licença do vSAN.

> **Note**
>
> A chave da solução VCF deve ter pelo menos 256 núcleos. A chave de licença do vSAN deve ter pelo menos 110 TiB de capacidade do vSAN.

> **Note**
>
> O Amazon EVS exige que você mantenha uma chave de solução VCF válida e uma chave de licença vSAN no SDDC Manager para que o serviço funcione adequadamente. Se você gerenciar essas chaves de licença usando o vSphere Client após a implantação, deverá garantir que elas também apareçam na tela de licenciamento da interface de usuário do SDDC Manager.

> **Note**
>
> A chave da solução VCF e a chave de licença do vSAN não podem ser usadas por um ambiente Amazon EVS existente.

- Para `--initial-vlans` especificar os intervalos de CIDR para as sub-redes de VLAN do Amazon EVS que o Amazon EVS cria em seu nome. Eles VLANs são usados para implantar dispositivos de gerenciamento de VCF. Ao configurar uma VLAN HCX pública, você deve especificar um bloco CIDR com um comprimento de máscara de rede de exatamente /28. O Amazon EVS gera um erro de validação se qualquer outro tamanho de bloco CIDR for especificado para a VLAN pública HCX. Para uma VLAN HCX privada e todos os outros blocos VLANs CIDR, o comprimento mínimo da máscara de rede que você pode usar é /28 e o máximo é /24.

- `hcxNetworkAclId`é usado ao configurar a conectividade HCX com a Internet. Especifique uma ACL de rede personalizada para a VLAN HCX pública.

  > **Important**
  >
  > É altamente recomendável que você crie uma ACL de rede personalizada dedicada à VLAN HCX. Para obter mais informações, consulte the section called “Configurar ACL de rede”.

  > **Important**
  >
  > As sub-redes de VLAN do Amazon EVS só podem ser criadas durante a criação do ambiente Amazon EVS e não podem ser modificadas após a criação do ambiente. Você deve garantir que os blocos CIDR da sub-rede da VLAN estejam dimensionados adequadamente antes de criar o ambiente. Você não poderá adicionar sub-redes de VLAN após a implantação do ambiente. Para obter mais informações, consulte the section called “Considerações sobre a rede Amazon EVS”.

- Para`--hosts`, especifique detalhes do host para os hosts que o Amazon EVS exige para a implantação do ambiente. Inclua nome do host DNS, nome da chave EC2 SSH e tipo de EC2 instância para cada host. O ID do host dedicado é opcional.

  > **Important**
  >
  > Não interrompa nem encerre as EC2 instâncias que o Amazon EVS implanta. Essa ação resulta em perda de dados.

  > **Note**
  >
  > No momento, o Amazon EVS só oferece suporte a EC2 instâncias i4i.metal.

- Para`--connectivity-info`, especifique os 2 VPC Route Server peer IDs que você criou na etapa anterior.

> **Note**
>
> O Amazon EVS exige uma instância do VPC Route Server associada a dois endpoints do Route Server e dois pares do Route Server antes da implantação do EVS. Essa configuração permite o roteamento dinâmico baseado em BGP pelo uplink do NSX. Para obter mais informações, consulte the section called “Configurar uma instância do VPC Route Server com endpoints e pares”.

- Para `--vcf-hostnames`, insira os nomes de host DNS das máquinas virtuais para hospedar os dispositivos de gerenciamento do VCF.
- Para `--site-id`, insira seu ID exclusivo do site da Broadcom. Esse ID permite acesso ao portal da Broadcom e é fornecido a você pela Broadcom no fechamento do contrato de software ou na renovação do contrato.
- (Opcional) Para `--region`, insira a região na qual seu ambiente será implantado. Se a região não for especificada, sua região padrão será usada.

```
aws evs create-environment \
--environment-name testEnv \
--vpc-id vpc-1234567890abcdef0 \
--service-access-subnet-id subnet-01234a1b2cde1234f \
--vcf-version VCF-5.2.2 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"isHcxPublic\": true,
      \"hcxNetworkAclId\": \"nacl-abcd1234\",
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
```

```
        \"cidr\": \"10.10.3.0/24\"
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07879acf49EXAMPLE\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07878bde50EXAMPLE\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07877eio51EXAMPLE\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
```

```
      \"dedicatedHostId\": \"h-07863ghi52EXAMPLE\"
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

Veja a seguir uma resposta de exemplo.

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATING",
        "stateDetails": "The environment is being initialized, this operation
 may take some time to complete.",
        "createdAt": "2025-04-13T12:03:39.718000+00:00",
        "modifiedAt": "2025-04-13T12:03:39.718000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-1234567890abcdef0",
        "serviceAccessSubnetId": "subnet-01234a1b2cde1234f",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
```

```
        ],
        "siteId": "my-site-id",
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-1234567890abcdef0",
                "rsp-abcdef01234567890"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        }
    }
}
```

Verifique a criação do ambiente Amazon EVS

Example

Amazon EVS console

1. Acesse o console do Amazon EVS.
2. No painel de navegação, escolha Ambientes.
3. Selecione o ambiente.
4. Selecione a guia Detalhes.
5. Verifique se o status do ambiente foi aprovado e se o estado do ambiente foi criado. Isso permite que você saiba que o ambiente está pronto para uso.

> **Note**
>
> A criação do ambiente pode levar várias horas. Se o estado Ambiente ainda mostrar Criando, atualize a página.

AWS CLI

1. Abra uma sessão do terminal.
2. Execute o comando a seguir, usando o ID do ambiente do seu ambiente e o nome da região que contém seus recursos. O ambiente está pronto para uso quando `environmentState` necessárioCREATED.

> **Note**
>
> A criação do ambiente pode levar várias horas. Se `environmentState` ainda aparecerCREATING, execute o comando novamente para atualizar a saída.

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

Veja a seguir uma resposta de exemplo.

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATED",
        "createdAt": "2025-04-13T13:39:49.546000+00:00",
        "modifiedAt": "2025-04-13T13:40:39.355000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-0c6def5b7b61c9f41",
        "serviceAccessSubnetId": "subnet-06a3c3b74d36b7d5e",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "checks": [],
        "connectivityInfo": {
            "privateRouteServerPeerings": [
```

```
                "rsp-056b2b1727a51e956",
                "rsp-07f636c5150f171c3"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        },
        "credentials": []
    }
}
```

Associe explicitamente as sub-redes de VLAN do Amazon EVS a uma tabela de rotas da VPC

Associe explicitamente cada uma das sub-redes de VLAN do Amazon EVS a uma tabela de rotas em sua VPC. Essa tabela de rotas é usada para permitir que AWS os recursos se comuniquem com máquinas virtuais em segmentos de rede do NSX, em execução com o Amazon EVS. Se você criou uma VLAN HCX pública, certifique-se de associar explicitamente a sub-rede da VLAN HCX pública a uma tabela de rotas pública em sua VPC que encaminha para um gateway da Internet.

Example

Amazon VPC console

1. Acesse o console da VPC.
2. No painel de navegação, escolha Route tables.
3. Escolha a tabela de rotas que você deseja associar às sub-redes de VLAN do Amazon EVS.
4. Selecione a guia Associações de sub-rede.
5. Em Associações explícitas de sub-rede, selecione Editar associações de sub-rede.
6. Selecione todas as sub-redes de VLAN do Amazon EVS.

7. Selecione Salvar associações.

AWS CLI

1. Abra uma sessão do terminal.
2. Identifique a sub-rede VLAN do Amazon EVS. IDs

```
aws ec2 describe-subnets
```

3. Associe suas sub-redes de VLAN do Amazon EVS a uma tabela de rotas em sua VPC.

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

Associe-se EIPs à sub-rede VLAN pública HCX (para conectividade HCX com a Internet)

Siga estas etapas para associar o endereço IP elástico (EIPs) do pool IPAM à VLAN pública HCX para conectividade com a Internet HCX. É necessário associar pelo menos dois EIPs aos dispositivos HCX Manager e HCX Interconnect (HCX-IX). Associe um EIP adicional para cada dispositivo de rede HCX que você precisa implantar. Você pode ter até 13 EIPs do pool IPAM associado à VLAN pública HCX.

Important

A conectividade de Internet pública HCX falhará se você não associar pelo menos dois EIPs do pool IPAM a uma sub-rede VLAN pública HCX.

Note

No momento, o Amazon EVS só oferece suporte EIPs à associação à VLAN HCX.

> **Note**
>
> Você não pode associar os dois primeiros EIPs ou o último EIP do bloco CIDR IPAM público à sub-rede da VLAN. Eles EIPs são reservados como rede, gateway padrão e endereços de transmissão. O Amazon EVS gera um erro de validação se você tentar EIPs associá-los à sub-rede da VLAN.

Amazon EVS console

1. Acesse o console do Amazon EVS.
2. No menu de navegação, escolha Ambientes.
3. Selecione o ambiente.
4. Na guia Redes e conectividade, selecione a VLAN pública HCX.
5. Escolha Associar EIP à VLAN.
6. Selecione o (s) endereço (s) IP elástico (s) a serem associados à VLAN pública HCX.
7. Selecione Associar EIPs.
8. Verifique as associações EIP para confirmar se elas EIPs foram associadas à VLAN pública HCX.

AWS CLI

1. Para associar um endereço IP elástico a uma VLAN, use o `associate-eip-to-vlan` comando de exemplo.
   - `environment-id`- O ID do seu ambiente Amazon EVS.
   - `vlan-name`- O nome da VLAN a ser associada ao endereço IP elástico.
   - `allocation-id`- O ID de alocação do endereço IP elástico.

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

   O comando retorna detalhes sobre a VLAN, incluindo a nova associação EIP:

   ```
   {
   ```

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


A `eipAssociations` matriz mostra a nova associação, incluindo:

- `associationId`- O ID exclusivo dessa associação EIP, usado para dissociação.
- `allocationId`- O ID de alocação do endereço IP elástico associado.
- `ipAddress`- O endereço IP atribuído à VLAN.

2. Repita a etapa para associar mais EIPs.

Configure tabelas de rotas do Transit Gateway e prefixos do Direct Connect para conectividade local (opcional)

Se você estiver configurando a conectividade de rede local usando Direct Connect ou AWS Site-to-Site VPN com um gateway de trânsito, deverá atualizar as tabelas de rotas do gateway de trânsito com a VPC criada CIDRs no ambiente Amazon EVS. Para obter mais informações, consulte Tabelas de rotas do Transit Gateway no Amazon VPC Transit Gateways.

Se você estiver usando o AWS Direct Connect, talvez também precise atualizar seus prefixos do Direct Connect para enviar e receber rotas atualizadas da VPC. Para obter mais informações, consulte Permite interações de prefixos para gateways AWS Direct Connect.

Recupere as credenciais do VCF e acesse os dispositivos de gerenciamento do VCF

O Amazon EVS usa o AWS Secrets Manager para criar, criptografar e armazenar segredos gerenciados em sua conta. Esses segredos contêm as credenciais do VCF necessárias para instalar e acessar os dispositivos de gerenciamento do VCF, como vCenter Server, NSX e SDDC Manager, bem como a senha raiz do ESX. Para obter mais informações sobre como recuperar segredos, consulte Obter AWS segredos do Secrets Manager no Guia do usuário do AWS Secrets Manager.

> **Note**
>
> O Amazon EVS não oferece alternância gerenciada de seus segredos. Recomendamos que você alterne seus segredos regularmente em uma janela de definição de alternância para garantir que os segredos não sejam de longa duração.

Depois de recuperar suas credenciais de VCF do AWS Secrets Manager, você pode usá-las para fazer login em seus dispositivos de gerenciamento de VCF. Para obter mais informações, consulte Faça login na interface de usuário do SDDC Manager e Como usar e configurar seu cliente vSphere na documentação VMware do produto.

Configurar o console EC2 serial (opcional)

Por padrão, o Amazon EVS habilita o ESX Shell em hosts Amazon EVS recém-implantados. Essa configuração permite o acesso à porta serial da EC2 instância Amazon por meio do console EC2 serial, que você pode usar para solucionar problemas de inicialização, configuração de rede e outros problemas. O console de série não exige que sua instância tenha recursos de rede. Com o console serial, você pode inserir comandos em uma EC2 instância em execução como se o teclado e o monitor estivessem conectados diretamente à porta serial da instância.

O console EC2 serial pode ser acessado usando o EC2 console ou AWS CLI o. Para obter mais informações, consulte Console EC2 serial para instâncias no Guia EC2 do usuário da Amazon.

> **Note**
>
> O console EC2 serial é o único mecanismo compatível com o Amazon EVS para acessar a Direct Console User Interface (DCUI) para interagir com um host ESX localmente.

> **Note**
>
> O Amazon EVS desativa o SSH remoto por padrão. Para obter mais informações sobre como habilitar o SSH para acessar o ESX Shell remoto, consulte Remote ESX Shell Access with SSH na documentação do produto VMware vSphere.

Conecte-se ao console EC2 serial

Para se conectar ao console EC2 serial e usar a ferramenta escolhida para solucionar problemas, algumas tarefas de pré-requisito devem ser concluídas. Para obter mais informações, consulte Pré-requisitos para o console EC2 serial e Connect to the EC2 Serial Console no Guia do usuário da Amazon EC2 .

> **Note**
>
> Para se conectar ao console EC2 serial, o estado da EC2 instância deve ser`running`. Você não pode se conectar ao console serial se a instância estiver no `terminated` estado `pending` `stopping``stopped`,`shutting-down`,, ou. Para obter mais informações sobre mudanças no estado da instância, consulte Alteração do estado da EC2 instância da Amazon no Guia EC2 do usuário da Amazon.

Configurar o acesso ao console EC2 serial

Para configurar o acesso ao console EC2 serial, você ou seu administrador devem conceder acesso ao console serial no nível da conta e, em seguida, configurar as políticas do IAM para conceder acesso aos seus usuários. Para instâncias Linux, você também deve configurar um usuário baseado em senha em cada instância para que seus usuários possam usar o console serial para solucionar problemas. Para obter mais informações, consulte Configurar o acesso ao console EC2 serial no Guia EC2 do usuário da Amazon.

Limpeza

Siga estas etapas para excluir os AWS recursos que foram criados.

Exclua os hosts e o ambiente do Amazon EVS

Siga estas etapas para excluir os hosts e o ambiente do Amazon EVS. Essa ação exclui a instalação do VMware VCF que é executada em seu ambiente Amazon EVS.

> **Note**
>
> Para excluir um ambiente Amazon EVS, você deve primeiro excluir todos os hosts dentro do ambiente. Um ambiente não pode ser excluído se houver hosts associados ao ambiente.

Example

Amazon EVS console

1. Acesse o console do Amazon EVS.
2. No painel de navegação, escolha Ambiente.
3. Selecione o ambiente que contém os hosts a serem excluídos.
4. Selecione a guia Hosts.
5. Selecione o host e escolha Excluir na guia Hosts. Repita essa etapa para cada host no ambiente.
6. Na parte superior da página Ambientes, escolha Excluir e, em seguida, Excluir ambiente.

   > **Note**
   >
   > A exclusão do ambiente também exclui as sub-redes VLAN do Amazon EVS e os AWS segredos do Secrets Manager que o Amazon EVS criou. AWS os recursos que você cria não são excluídos. Esses recursos podem continuar gerando custos.

7. Se você tiver reservas EC2 de capacidade da Amazon em vigor e não precisar mais, certifique-se de cancelá-las. Para obter mais informações, consulte Cancelar uma reserva de capacidade no Guia EC2 do usuário da Amazon.

AWS CLI

1. Abra uma sessão do terminal.
2. Identifique o ambiente que contém o host a ser excluído.

```
aws evs list-environments
```

Veja a seguir uma resposta de exemplo.

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

3. Exclua os hosts do ambiente. Abaixo está um exemplo de `aws evs delete-environment-host` solicitação.

> **Note**
>
> Para poder excluir um ambiente, você deve primeiro excluir todos os hosts contidos no ambiente.

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

```
--host esx01
```

4. Repita as etapas anteriores para excluir os hosts restantes em seu ambiente.
5. Exclua o ambiente.

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

> **Note**
>
> A exclusão do ambiente também exclui as sub-redes VLAN do Amazon EVS e os AWS segredos do Secrets Manager que o Amazon EVS criou. Outros AWS recursos que você cria não são excluídos. Esses recursos podem continuar gerando custos.

6. Se você tiver reservas EC2 de capacidade da Amazon em vigor e não precisar mais, certifique-se de cancelá-las. Para obter mais informações, consulte Cancelar uma reserva de capacidade no Guia EC2 do usuário da Amazon.

Excluir recursos IPAM (para conectividade HCX com a Internet)

Se você configurou a conectividade HCX com a Internet, siga estas etapas para excluir seus recursos IPAM.

1. Libere as alocações de EIP do pool público do IPAM. Para obter mais informações, consulte Liberar uma alocação no Guia do usuário do VPC IP Address Manager.
2. Desprovisione o IPv4 CIDR público do pool IPAM. Para obter mais informações, consulte Desprovisionamento CIDRs de um pool no Guia do usuário do VPC IP Address Manager.
3. Exclua o pool IPAM público. Para obter mais informações, consulte Excluir um pool no Guia do usuário do VPC IP Address Manager.
4. Exclua o IPAM Para obter mais informações, consulte Excluir um IPAM no Guia do usuário do VPC IP Address Manager.

Exclua os componentes do VPC Route Server

Para ver as etapas para excluir os componentes do Amazon VPC Route Server que você criou, consulte Route Server cleanup no Guia do usuário do Amazon VPC.

Excluir a lista de controle de acesso à rede (ACL)

Para ver as etapas para excluir uma lista de controle de acesso à rede, consulte Excluir uma ACL de rede para sua VPC no Guia do usuário da Amazon VPC.

Desassociar e excluir tabelas de rotas de sub-rede

Para ver as etapas para desassociar e excluir tabelas de rotas de sub-rede, consulte Tabelas de rotas de sub-rede no Guia do usuário da Amazon VPC.

Exclusão de sub-redes

Exclua as sub-redes VPC, incluindo a sub-rede de acesso ao serviço. Para ver as etapas para excluir sub-redes VPC, consulte Excluir uma sub-rede no Guia do usuário da Amazon VPC.

> **Note**
>
> Se você estiver usando o Route 53 para DNS, remova os endpoints de entrada antes de tentar excluir a sub-rede de acesso ao serviço. Caso contrário, você não poderá excluir a sub-rede de acesso ao serviço.

> **Note**
>
> O Amazon EVS exclui as sub-redes da VLAN em seu nome quando o ambiente é excluído. As sub-redes de VLAN do Amazon EVS só podem ser excluídas quando o ambiente é excluído.

Exclusão da VPC

Para ver as etapas para excluir a VPC, consulte Excluir sua VPC no Guia do usuário da Amazon VPC.

Próximas etapas

Migre suas cargas de trabalho para o Amazon EVS usando o VMware Hybrid Cloud Extension (VMware HCX). Para obter mais informações, consulte Migração.

Migre cargas de trabalho para o Amazon EVS usando o HCX VMware

Depois que o Amazon EVS for implantado, você poderá implantar o VMware HCX com conectividade à Internet pública ou privada para facilitar a migração de cargas de trabalho para o Amazon EVS. Para obter mais informações, consulte Introdução ao VMware HCX no Guia do Usuário do VMware HCX.

Important

A migração HCX baseada na Internet geralmente não é recomendada para:

- Aplicativos sensíveis à instabilidade ou latência da rede.
- Operações urgentes do VMotion.
- Migrações em grande escala com requisitos rígidos de desempenho.

Para esses cenários, recomendamos o uso da conectividade privada HCX. Uma conexão privada dedicada oferece um desempenho mais confiável em comparação com as conexões baseadas na Internet.

Opções de conectividade HCX

Você pode migrar cargas de trabalho para o Amazon EVS usando conectividade privada com AWS Direct Connect ou conexão Site-to-Site VPN, ou usando conectividade pública.

Dependendo da sua situação e das opções de conectividade, você pode preferir usar a conectividade pública ou privada com o HCX. Por exemplo, alguns sites podem ter conectividade privada com maior consistência de desempenho, mas menor taxa de transferência devido à criptografia de VPN ou velocidades de link limitadas. Da mesma forma, você pode ter uma conectividade pública à Internet de alta taxa de transferência que tenha mais variação no desempenho. Com o Amazon EVS, você tem a opção de usar qualquer opção de conectividade que funcione melhor para você.

A tabela a seguir compara as diferenças entre a conectividade pública e a HCX privada.

Conectividade privada	Conectividade pública
Visão geral	Visão geral
Usa somente conexões privadas dentro da VPC. Opcionalmente, você pode usar o AWS Direct Connect ou a Site-to-Site VPN com um gateway de trânsito para conectividade de rede externa.	Usa conectividade pública à Internet com endereços IP elásticos, permitindo migrações sem uma conexão privada dedicada.
Mais adequado para	Mais adequado para
• Operações do vMotion sensíveis ao tempo. • Migrações em grande escala. • Aplicativos sensíveis à latência/instabilidade. • Transferências de dados de alto volume. • Organizações com AWS Direct Connect/VPN AWS Site-to-Site existente.	• Locais sem conexão AWS direta/VPN AWS Site-to-Site . • Projetos sensíveis ao custo.
Benefícios principais	Benefícios principais
• Conectividade consistente de baixa latência. • Alocação de largura de banda dedicada. • Desempenho de rede mais confiável. • A criptografia HCX padrão pode ser desativada em ambientes privados para otimizar o desempenho. • Não é necessário gerenciamento público de IP.	• Configuração mais rápida do que a conectividade privada. • Econômico para migrações menores.
Considerações importantes	Considerações importantes
• Configuração inicial mais complexa. • Custos iniciais de infraestrutura mais altos. • Cronograma de implementação mais longo.	• Desempenho de rede mais variável. • Limitações de largura de banda são possíveis.

Conectividade privada	Conectividade pública
• Sem conectividade direta com a Internet para nenhum componente HCX.	• Maior latência do que a conectividade privada. • Cada componente requer um endereço IP elástico dedicado alocado do pool IPAM público. • As associações EIP permitem conectividade direta com a Internet para cada componente HCX.

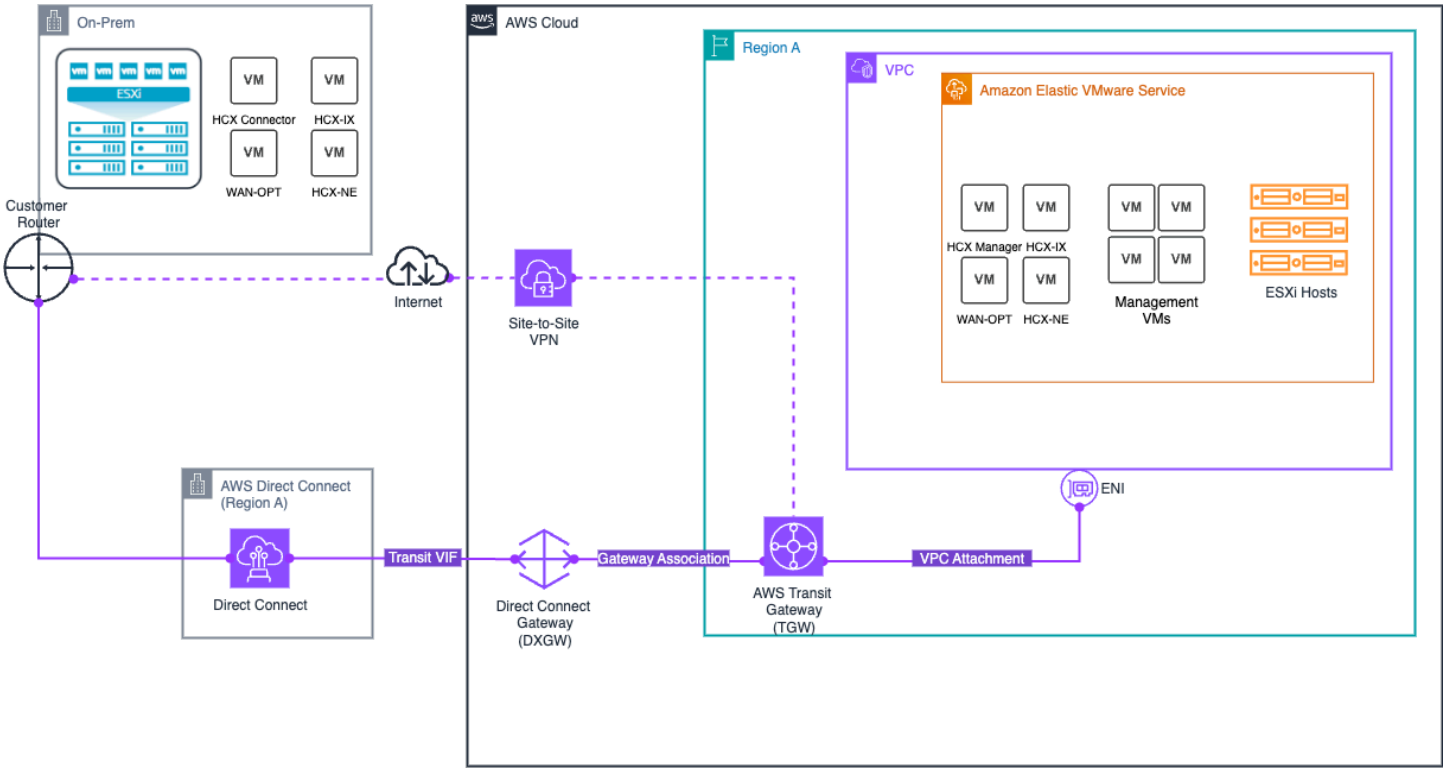
Arquitetura de conectividade privada HCX

A solução de conectividade privada HCX integra vários componentes:

- Componentes de rede Amazon EVS
  - Usa somente sub-redes de VLAN privadas para comunicação segura, incluindo uma VLAN HCX privada.
  - Suporta rede ACLs para controle de tráfego.
  - Oferece suporte à propagação dinâmica de rotas por BGP por meio de um servidor de rotas VPC privado.
- AWS opções gerenciadas de trânsito de rede para conectividade local
  - AWS O Direct Connect + AWS Transit Gateway permite que você conecte sua rede local ao Amazon EVS por meio de uma conexão privada dedicada. Para obter mais informações, consulte AWS Direct Connect + AWS Transit Gateway.
  - AWS Site-to-Site O VPN + AWS Transit Gateway oferece a opção de criar uma conexão IPsec VPN entre sua rede remota e o gateway de trânsito pela Internet. Para obter mais informações, consulte AWS Transit Gateway + AWS Site-to-Site VPN.

> **Note**
>
> O Amazon EVS não oferece suporte à conectividade por meio de uma interface virtual privada (VIF) do AWS Direct Connect ou por meio de uma conexão AWS Site-to-Site VPN que termina diretamente na VPC subjacente.

O diagrama a seguir ilustra a arquitetura de conectividade privada do HCX, mostrando como você pode usar o AWS Direct Connect e a Site-to-Site VPN com o gateway de trânsito para permitir a migração segura da carga de trabalho por meio de uma conexão privada dedicada.



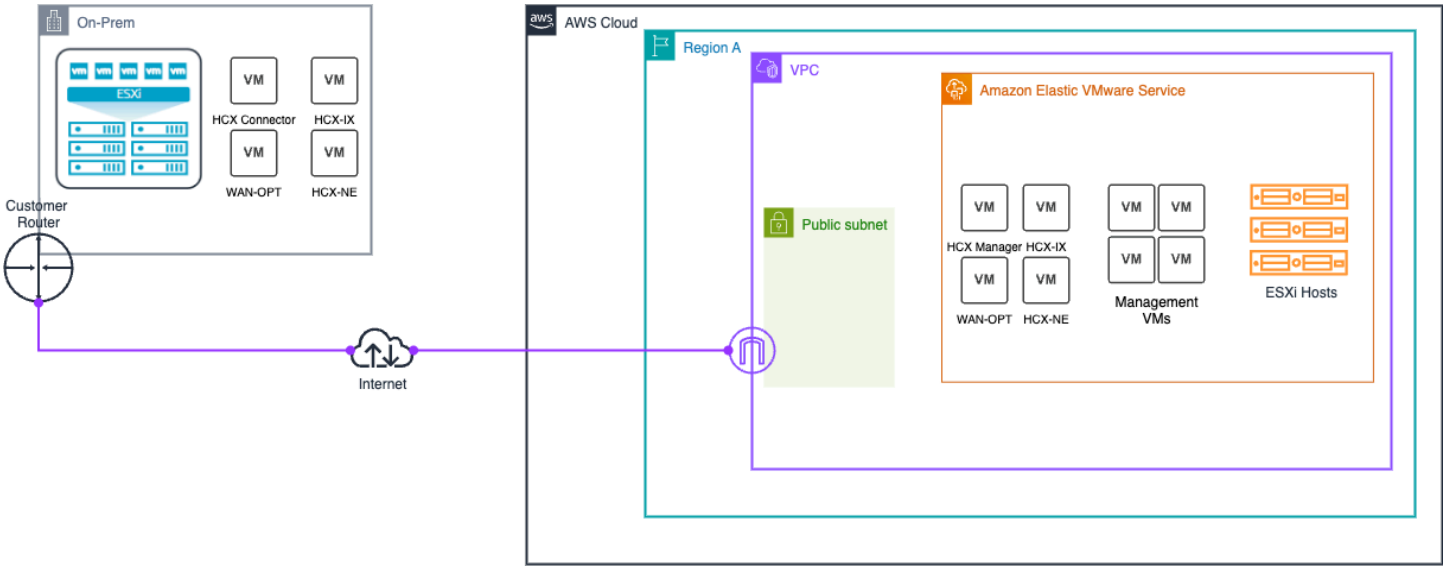
Arquitetura de conectividade à Internet HCX

A solução de conectividade com a Internet HCX consiste em vários componentes trabalhando juntos:

- Componentes de rede Amazon EVS
  - Usa uma sub-rede VLAN HCX pública isolada para habilitar a conectividade com a Internet entre o Amazon EVS e seus dispositivos HCX locais.
  - Suporta rede ACLs para controle de tráfego.
  - Oferece suporte à propagação dinâmica de rotas por BGP por meio de um servidor de rotas VPC público.
- IPAM e gerenciamento público de IP
  - O Amazon VPC IP Address Manager (IPAM) gerencia a alocação de IPv4 endereços públicos do pool IPAM público de propriedade da Amazon.
  - O bloco CIDR VPC secundário (/28) é alocado do pool IPAM, criando uma sub-rede pública isolada separada do CIDR VPC principal.

Para obter mais informações, consulte the section called “Conectividade pública HCX”.

O diagrama a seguir ilustra a arquitetura de conectividade com a Internet HCX.



Configuração de migração HCX

Este tutorial descreve como configurar o VMware HCX para migrar suas cargas de trabalho para o Amazon EVS.

Pré-requisitos

Antes de usar o VMware HCX com o Amazon EVS, verifique se os pré-requisitos do HCX foram atendidos. Para obter mais informações, consulte the section called “VMware Pré-requisitos do HCX”.

Important

O Amazon EVS tem requisitos exclusivos para conectividade pública HCX com a Internet. Se você precisar de conectividade pública HCX, deverá atender aos seguintes requisitos:

- Crie um IPAM e um pool IPv4 IPAM público com CIDR que tenha um comprimento mínimo de máscara de rede de /28.
- Aloque pelo menos dois endereços IP elásticos (EIPs) do pool IPAM para os dispositivos HCX Manager e HCX Interconnect (HCX-IX). Aloque um endereço IP elástico adicional para cada dispositivo de rede HCX que você precisa implantar.
- Adicione o bloco IPv4 CIDR público como um CIDR adicional à sua VPC.

Para obter mais informações, consulte the section called “Configuração de conectividade com a Internet HCX”.

Verifique o status da sub-rede HCX VLAN

Uma VLAN é criada para o HCX como parte da implantação padrão do Amazon EVS. Siga estas etapas para verificar se a sub-rede da VLAN HCX está configurada corretamente.

Example

Amazon EVS console

1. Acesse o console do Amazon EVS.
2. No painel de navegação, escolha Ambientes.
3. Selecione o ambiente Amazon EVS.
4. Selecione a guia Redes e conectividade.
5. Em VLANs, identifique a VLAN HCX e verifique se o estado foi criado e se o público é verdadeiro.

AWS CLI

1. Execute o comando a seguir, usando o ID do ambiente do seu ambiente e o nome da região que contém seus recursos.

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

2. Na saída de resposta, identifique a VLAN com um `functionName` de `hcx` e verifique se o `vlanState` é `CREATED` e `isPublic` está definido como. `true` Veja a seguir uma resposta de exemplo.

```
{
    "environmentVlans": [{
            "vlanId": 50,
            "cidr": "10.10.4.0/24",
            "availabilityZone": "us-east-2b",
```

```
            "functionName": "vTep",
            "subnetId": "subnet-0ce640ac79e7f4dbc",
            "createdAt": "2025-09-09T12:09:37.526000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.596000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [],
            "isPublic": false
        },
        {
            "vlanId": 80,
            "cidr": "18.97.141.240/28",
            "availabilityZone": "us-east-2b",
            "functionName": "hcx",
            "subnetId": "subnet-0f080c94782cc74b4",
            "createdAt": "2025-09-09T12:09:37.675000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.359000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [{
                    "assocationId": "eipassoc-0be981accbbdf443a",
                    "allocationId": "eipalloc-0cef80396f4a0cc24",
                    "ipAddress": "18.97.141.245"
                },
                {
                    "assocationId": "eipassoc-0d5572f66b7952e9d",
                    "allocationId": "eipalloc-003fc9807d35d1ad3",
                    "ipAddress": "18.97.141.244"
                }
            ],
            "isPublic": true
        }
    ]
}
```


Verifique se a sub-rede HCX VLAN está associada a uma rede ACL

Siga estas etapas para verificar se a sub-rede da VLAN HCX está associada a uma rede ACL. Para obter mais informações sobre associação de ACL de rede, consultethe section called “Crie uma rede ACL para controlar o tráfego de sub-rede VLAN do Amazon EVS”.

> **Important**
>
> Se você estiver se conectando pela Internet, associar um endereço IP elástico a uma VLAN fornece acesso direto à Internet a todos os recursos dessa VLAN. Certifique-se de ter listas de controle de acesso à rede apropriadas configuradas para restringir o acesso conforme necessário para seus requisitos de segurança.

> **Important**
>
> EC2 os grupos de segurança não funcionam em interfaces de rede elásticas conectadas às sub-redes VLAN do Amazon EVS. Para controlar o tráfego de e para as sub-redes VLAN do Amazon EVS, você deve usar uma lista de controle de acesso à rede (ACL).

Example

Amazon VPC console

1. Vá para o Amazon VPC console.
2. No painel de navegação, escolha Rede ACLs.
3. Selecione a ACL de rede à qual suas sub-redes de VLAN estão associadas.
4. Selecione a guia Associações de sub-rede.
5. Verifique se a sub-rede HCX VLAN está listada entre as sub-redes associadas.

AWS CLI

1. Execute o comando a seguir, usando o ID de sub-rede da VLAN HCX no filtro. `Values`

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

2. Verifique se a ACL de rede correta foi retornada na resposta.

Verifique se as sub-redes EVS VLAN estão explicitamente associadas a uma tabela de rotas

O Amazon EVS exige que todas as sub-redes de VLAN do EVS sejam explicitamente associadas a uma tabela de rotas em sua VPC. Para conectividade HCX com a Internet, sua sub-rede VLAN pública HCX deve estar explicitamente associada a uma tabela de rotas pública em sua VPC que é roteada para um gateway de Internet. Siga estas etapas para verificar a associação explícita da tabela de rotas.

Example

Amazon VPC console

1. Acesse o console da VPC.
2. No painel de navegação, escolha Route tables.
3. Escolha a tabela de rotas à qual suas sub-redes EVS VLAN devem ser explicitamente associadas.
4. Selecione a guia Associações de sub-rede.
5. Em Associações explícitas de sub-rede, verifique se todas as sub-redes EVS VLAN estão listadas. Se uma sub-rede de VLAN não estiver listada aqui, a sub-rede de VLAN está implicitamente associada à tabela de rotas principal. Para que o Amazon EVS funcione corretamente, você deve associar explicitamente todas as sub-redes da VLAN a uma tabela de rotas. Para a sub-rede VLAN pública HCX, você deve ter uma tabela de rotas pública associada com um gateway de Internet como destino. Para resolver esse problema, escolha Editar associações de sub-rede e adicione as sub-redes de VLAN ausentes.

AWS CLI

1. Abra uma sessão do terminal.
2. Execute o comando de exemplo a seguir para recuperar detalhes sobre todas as suas sub-redes EVS VLAN, incluindo associação à tabela de rotas. Se uma sub-rede de VLAN não estiver listada aqui, a sub-rede de VLAN está implicitamente associada à tabela de rotas principal. Para que o Amazon EVS funcione corretamente, você deve associar explicitamente todas as sub-redes da VLAN a uma tabela de rotas. Para a sub-rede VLAN pública HCX, você deve ter uma tabela de rotas pública associada com um gateway de Internet como destino.

```
aws ec2 describe-subnets
```

3. Associe explicitamente suas sub-redes EVS VLAN a uma tabela de rotas em sua VPC. Abaixo está um exemplo de comando.

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

(Para conectividade HCX com a Internet) Verifique se EIPs estão associados à sub-rede VLAN HCX

Para cada dispositivo de rede HCX que você implanta, você deve ter um EIP do pool IPAM associado a uma sub-rede VLAN pública HCX. É necessário associar pelo menos dois EIPs à sub-rede VLAN pública HCX para os dispositivos HCX Manager e HCX Interconnect (HCX-IX). Siga estas etapas para verificar se as associações EIP necessárias existem.

Important

A conectividade de Internet pública HCX falhará se você não associar pelo menos dois EIPs do pool IPAM a uma sub-rede VLAN pública HCX.

Note

Você não pode associar os dois primeiros EIPs ou o último EIP do bloco CIDR IPAM público a uma sub-rede VLAN. Eles EIPs são reservados como rede, gateway padrão e endereços de transmissão. O Amazon EVS gera um erro de validação se você tentar EIPs associá-los a uma sub-rede de VLAN.

Example

Amazon EVS console

1. Acesse o console do Amazon EVS.
2. No menu de navegação, escolha Ambientes.

3. Selecione o ambiente.
4. Na guia Redes e conectividade, selecione a VLAN pública HCX.
5. Verifique a guia Associações EIP para confirmar se elas EIPs foram associadas à VLAN pública HCX.

AWS CLI

1. Para verificar quais EIPs estão associados à sub-rede da VLAN HCX, use o comando. `list-environment-vlans` Para`environment-id`, use o ID exclusivo para o ambiente EVS que contém a VLAN HCX.

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

O comando retorna detalhes sobre suas VLANs, incluindo associações EIP:

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

```
          "associationId": "eipassoc-23456789012abcdef",
          "allocationId": "eipalloc-2345678901abcdef2",
          "ipAddress": "18.97.137.5"
        }
      ],
      "isPublic": true,
      "networkAclId": "acl-0123456789abcdef0"
    },
    ...
  ]
}
```

A `eipAssociations` matriz mostra a associação EIP, incluindo:

- `associationId`- O ID exclusivo dessa associação EIP.
- `allocationId`- O ID de alocação do endereço IP elástico associado.
- `ipAddress`- O endereço IP atribuído à VLAN.

Crie um grupo de portas distribuídas com o ID de VLAN de uplink público HCX

Acesse a interface do vSphere Client e siga as etapas em Adicionar um grupo de portas distribuídas para adicionar um grupo de portas distribuídas a um switch distribuído do vSphere.

Ao configurar o failback na interface do vSphere Client, certifique-se de que o uplink1 seja um uplink ativo e o uplink2 seja um uplink em espera para ativar o failover. Active/Standby Para a configuração de VLAN na interface do vSphere Client, insira o ID da VLAN HCX que você identificou anteriormente.

(Opcional) Configurar a otimização de WAN HCX

> **Note**
>
> O recurso de otimização de WAN não está mais disponível no HCX 4.11.3. Para obter mais informações, consulte as notas de versão do HCX 4.11.3.

O serviço de otimização de WAN HCX (HCX-WO) melhora as características de desempenho das linhas privadas ou do caminho da Internet aplicando técnicas de otimização da WAN, como

redução de dados e condicionamento do caminho da WAN. O serviço de otimização de WAN HCX é recomendado em implantações que não conseguem dedicar caminhos de 10 Gbit para migrações. Em implantações de 10 Gbit e baixa latência, o uso da otimização de WAN pode não gerar um melhor desempenho de migração. Para obter mais informações, consulte Considerações e melhores VMware práticas de implantação do HCX.

O serviço de otimização de WAN HCX é implantado em conjunto com o dispositivo de serviço de interconexão de WAN HCX (HCX-IX). O HCX-IX é responsável pela replicação de dados entre o ambiente corporativo e o ambiente Amazon EVS.

Para usar o serviço de otimização de WAN HCX com o Amazon EVS, você precisa usar um grupo de portas distribuídas na sub-rede da VLAN HCX. Use o grupo de portas distribuídas que foi criado na etapa anterior.

(Opcional) Ative a rede otimizada para mobilidade HCX

O HCX Mobility Optimized Networking (MON) é um recurso do HCX Network Extension Service. As extensões de rede habilitadas para MON melhoram os fluxos de tráfego para máquinas virtuais migradas, permitindo o roteamento seletivo em seu ambiente Amazon EVS. O MON permite que você configure o caminho ideal para migrar o tráfego da carga de trabalho para o Amazon EVS ao estender redes de camada 2, evitando um longo caminho de rede de ida e volta pelo gateway de origem. Esse recurso está disponível para todas as implantações do Amazon EVS. Para obter mais informações, consulte Configurando redes otimizadas para mobilidade no Guia do usuário do VMware HCX.

> **Important**
>
> Antes de habilitar o HCX MON, leia as seguintes limitações e configurações não suportadas para o HCX Network Extension.
> Restrições e limitações para extensão de rede
> Restrições e limitações para topologias de rede otimizadas para mobilidade

> **Important**
>
> Antes de habilitar o HCX MON, verifique se na interface do NSX você configurou a redistribuição de rotas para o CIDR da rede de destino. Para obter mais informações, consulte Configurar o BGP e a redistribuição de rotas na documentação do VMware NSX.

Verifique a conectividade HCX

VMware O HCX inclui ferramentas de diagnóstico integradas que podem ser usadas para testar a conectividade. Para obter mais informações, consulte Solução de problemas do VMware HCX no Guia do usuário do VMware HCX.

Configurar a conectividade pública com a Internet HCX

Você pode configurar o acesso público à Internet para sua VLAN pública HCX associando endereços IP elásticos à sua VLAN. Isso permite a conectividade direta com a Internet para dispositivos e cargas de trabalho VMware HCX que exigem acesso à Internet para operações de migração.

Tópicos relacionados

Este tópico aborda o gerenciamento do acesso à Internet para a VLAN pública HCX. Para uma implementação completa:

1. Preencha os pré-requisitos em. Configurando o Amazon Elastic VMware Service
2. Configure a configuração inicial emIntrodução.
3. Configurar o acesso à Internet (este tópico).

Sobre o acesso à Internet HCX VLAN

Você pode configurar o acesso à Internet para dispositivos VMware HCX, permitindo que você realize a migração HCX de suas cargas de trabalho para o Amazon EVS pela Internet.

Essa abordagem:

- Permite migrações de máquinas virtuais sem exigir conectividade privada dedicada.
- Fornece uma solução flexível e econômica para migração.

> **Important**
>
> A migração HCX baseada na Internet geralmente não é recomendada para:
>
> - Aplicativos sensíveis à instabilidade ou latência da rede.
> - Operações urgentes do VMotion.

- Migrações em grande escala com requisitos rígidos de desempenho.

Para esses cenários, recomendamos o uso da conectividade privada HCX. Uma conexão privada dedicada oferece um desempenho mais confiável em comparação com as conexões baseadas na Internet.

Visão geral da conectividade com a Internet

Analise as seguintes considerações.

Requisitos de rede HCX e DNAT

O HCX tem restrições de rede específicas que afetam a forma como você configura o acesso público à Internet.

O HCX não suporta a Tradução de Endereços de Rede de Destino (DNAT). Em vez disso, o HCX exige que a rede de uplink seja roteável com um endereço IP de gateway padrão.

As sub-redes VLAN do Amazon EVS incluem um endereço IP de gateway padrão, como outras sub-redes VPC. No entanto, essas sub-redes são sempre sub-redes privadas, mesmo quando você usa blocos CIDR fora do intervalo de endereços. RFC1918

Habilitando a conectividade HCX com a Internet

Para habilitar a conectividade com a Internet sem DNAT, o Amazon EVS usa uma abordagem de configuração CIDR específica:

- Requisito de CIDR roteável pela Internet: O Amazon EVS exige um CIDR roteável pela Internet que corresponda ao CIDR de sub-rede da sua VLAN HCX.
- Alocação de IPAM: o Amazon EVS usa um CIDR público alocado por IPAM com um comprimento mínimo de máscara de rede de /28 como o CIDR roteável da Internet.
- Configuração da VPC: você deve adicionar manualmente o CIDR público alocado por IPAM à sua VPC como um CIDR secundário da VPC.
- Implantação de sub-rede de VLAN: após a configuração do IPAM e da VPC, você pode usar o CIDR público alocado por IPAM na sub-rede da VLAN HCX durante a implantação do Amazon EVS.

- Configuração de IP elástico: o Amazon EVS exige a seguinte configuração:
  - Aloque o Elastic IPs: Você aloca o Elastic a IPs partir do CIDR alocado pelo IPAM. Você deve alocar pelo menos dois endereços IP elásticos (EIPs) do pool IPAM para os dispositivos HCX Manager e HCX Interconnect (HCX-IX). Aloque um endereço IP elástico adicional para cada dispositivo de rede HCX que você precisa implantar.
  - Associar à VLAN: você associa cada IP elástico que deseja usar com um dispositivo HCX à sub-rede da VLAN HCX. Use o console Amazon EVS ou AWS CLI para essa associação.
  - Configurar endereço de gateway: O primeiro endereço utilizável do CIDR se torna o endereço de gateway que você configura em seu dispositivo HCX.
  - Roteamento de tráfego: o tráfego de cada IP elástico associado é roteado diretamente para o dispositivo HCX de destino com o mesmo endereço IP, sem DNAT.

Para obter as etapas de configuração do HCX com conectividade à Internet para implantação do ambiente Amazon EVS, consulte e. Configurando o Amazon Elastic VMware Service Introdução

Considerações sobre a operação

- O bloco CIDR da VLAN pública HCX deve ter um comprimento de máscara de rede /28.
- EIPs podem ser associados ou desassociados da VLAN pública HCX após a implantação usando o console Amazon EVS ou AWS CLI, mas devem ser do mesmo pool IPAM.
- Cada associação EIP tem seu próprio ID de associação exclusivo.
- Você pode ter até 13 EIPs de um pool IPAM público associado à VLAN pública /28 HCX. Você não pode associar os dois primeiros EIPs ou o último EIP do bloco CIDR público alocado por IPAM à sub-rede VLAN pública HCX. Eles EIPs são reservados como rede, gateway padrão e endereços de transmissão. O Amazon EVS gera um erro de validação se você tentar EIPs associá-los à VLAN.

Considerações sobre segurança

- As listas de controle de acesso à rede (ACLs) ainda se aplicam ao tráfego que flui pela sub-rede VLAN pública HCX.
- As regras do grupo de segurança não se aplicam ao tráfego em sub-redes de VLAN públicas HCX. Use a rede ACLs para controle de tráfego.

> **Important**
>
> Se você estiver se conectando pela Internet, associar um endereço IP elástico a uma VLAN fornece acesso direto à Internet a todos os recursos dessa VLAN. Certifique-se de ter listas de controle de acesso à rede apropriadas configuradas para restringir o acesso conforme necessário para seus requisitos de segurança.

Gerenciando endereços IP elásticos para VLANs

Você pode associar e desassociar endereços IP elásticos com uma VLAN pública HCX usando o console Amazon EVS ou. AWS CLI

> **Note**
>
> No momento, o Amazon EVS só oferece suporte à associação e desassociação de endereços IP elásticos a uma VLAN pública HCX.

Associar um endereço IP elástico a uma VLAN

Pré-requisitos

Certifique-se de que você tenha o seguinte:

- O endereço IP elástico é alocado a partir do pool IPAM público de propriedade da Amazon.
- O ambiente Amazon EVS já foi criado.

Example

Amazon EVS console

1. Acesse o console do Amazon EVS.
2. No menu de navegação, escolha Ambientes.
3. Selecione o ambiente.
4. Na guia Redes e conectividade, selecione a VLAN pública HCX.

> **Note**
>
> No momento, o Amazon EVS só oferece suporte EIPs à associação à VLAN HCX.

5. Escolha Associar EIP à VLAN.
6. Selecione os endereços IP elásticos a serem associados à VLAN pública HCX.
7. Selecione Associar EIPs. Você pode ter até 13 EIPs associados à VLAN pública HCX.

> **Note**
>
> Você não pode associar os dois primeiros EIPs do bloco IPAM CIDR público à sub-rede da VLAN. Eles EIPs são reservados como endereços de rede e de gateway padrão.

8. Verifique as associações EIP para confirmar se elas EIPs foram associadas à VLAN pública HCX.

AWS CLI

1. Para associar um endereço IP elástico a uma VLAN, use o `associate-eip-to-vlan` comando de exemplo.
   - `environment-id`- O ID do seu ambiente Amazon EVS.
   - `vlan-name`- Deve ser`hcx`. No momento, o Amazon EVS só oferece suporte à associação de EIP com a VLAN HCX.
   - `allocation-id`- O ID de alocação do endereço IP elástico.

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

   O comando retorna detalhes sobre a VLAN, incluindo a nova associação EIP:

   ```
   {
       "vlan": {
           "vlanId": 80,
           "cidr": "18.97.137.0/28",
   ```

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


A `eipAssociations` matriz mostra a nova associação, incluindo:

- `associationId`- O ID exclusivo dessa associação EIP, usado para dissociação.
- `allocationId`- O ID de alocação do endereço IP elástico associado.
- `ipAddress`- O endereço IP atribuído à VLAN.

2. Repita a etapa para associar mais EIPs. Você pode ter até 13 EIPs associados à VLAN pública HCX.

Desassociar um endereço IP elástico de uma VLAN

Pré-requisitos

Certifique-se de que você tenha o seguinte:

- O ambiente Amazon EVS já foi criado.
- O EIP está associado ao ambiente Amazon EVS.

Example

Amazon EVS console

1. Acesse o console do Amazon EVS.
2. No menu de navegação, escolha Ambientes.
3. Selecione o ambiente.
4. Na guia Redes e conectividade, selecione a VLAN pública HCX.
5. Escolha Dissociar EIP da VLAN.
6. Selecione os endereços IP elásticos a serem desassociados da VLAN pública HCX.

> **Important**
>
> A dissociação EIPs pode causar perda de conectividade com a Internet para dispositivos que usam sub-redes de VLAN públicas.

7. Escolha Desassociar EIPs.
8. Verifique as associações EIP para confirmar se elas EIPs foram desassociadas da VLAN pública HCX.

AWS CLI

Para dissociar um endereço IP elástico de uma VLAN, use o comando de exemplo`disassociate-eip-from-vlan`.

- `environment-id`- O ID do seu ambiente Amazon EVS.
- `vlan-name`- Deve ser`hcx`. No momento, o Amazon EVS só oferece suporte à associação de EIP com a VLAN HCX.
- `association-id`- O ID de associação da associação EIP a ser removida.

> **Important**
>
> A dissociação EIPs pode causar perda de conectividade com a Internet para dispositivos que usam sub-redes de VLAN públicas.

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

O comando retorna detalhes sobre a VLAN com a associação EIP removida:

```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:48:49.846000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

A `eipAssociations` matriz vazia confirma que o endereço IP elástico foi desassociado com sucesso da VLAN.

Sobre a otimização de WAN HCX para migrações baseadas na Internet

> **Note**
>
> O recurso de otimização de WAN não está mais disponível no HCX 4.11.3. Para obter mais informações, consulte as notas de versão do HCX 4.11.3.

Ao realizar migrações pela Internet, o HCX WAN Optimization (HCX-WO) pode melhorar o desempenho da migração. O serviço funciona em conjunto com o dispositivo de interconexão HCX (HCX-IX) para:

- Aplique técnicas de redução de dados para minimizar o uso da largura de banda.
- Implemente o condicionamento do caminho da WAN para otimizar o desempenho da rede.
- Melhore as velocidades de migração em conexões de internet de alta latência.
- Aumente a confiabilidade das migrações baseadas na Internet.

A otimização de WAN HCX é particularmente útil para migrações baseadas na Internet em que:

- A latência da rede pode ser maior do que as opções de conectividade privada.
- A largura de banda disponível pode ser limitada ou variável.
- As condições da rede podem flutuar devido aos padrões de tráfego da Internet.

Para obter instruções detalhadas sobre como configurar a otimização de WAN HCX após configurar a conectividade com a Internet, consulte. the section called “(Opcional) Configurar a otimização de WAN HCX”

> **Note**
>
> Embora a otimização de WAN possa melhorar significativamente o desempenho da migração baseada na Internet, ela pode não oferecer benefícios adicionais em ambientes com conexões dedicadas de 10 Gbit e baixa latência. Considere as características da sua rede ao decidir se deseja ativar esse recurso.

Gerenciando ambientes Amazon EVS

Este capítulo inclui os tópicos a seguir para ajudá-lo a gerenciar seu ambiente.

- the section called “Assinaturas VCF”- Descreve como as assinaturas do VCF funcionam com o Amazon EVS e as responsabilidades do cliente pelo gerenciamento de assinaturas do VCF.
- the section called “Versões e EC2 instâncias do VCF”- Descreve as versões compatíveis do VCF e do ESX e como verificar a disponibilidade das versões no Amazon EVS.
- the section called “Gerenciamento de ciclo de vida”- Descreve as responsabilidades de gerenciamento do ciclo de vida em um ambiente Amazon EVS, incluindo o gerenciamento da infraestrutura subjacente, o gerenciamento de upgrade do VCF e o gerenciamento do ciclo de vida do host ESX.
- the section called “Manutenção do ambiente”- Descreve como realizar tarefas de manutenção comuns para seu ambiente Amazon EVS, incluindo configuração de rede, manutenção do host ESX, verificação do status do ambiente e gerenciamento de programações secretas de rotação para suas credenciais de VCF.
- the section called “Criar host”- Descreve como criar um host Amazon EVS após a implantação do ambiente e adicionar o host ao cluster.
- the section called “Excluir host”- Descreve como excluir um host Amazon EVS e removê-lo do cluster.

Assinaturas VCF

> **Note**
>
> O Amazon EVS não oferece suporte a licenças perpétuas do vSphere. Você deve ter uma assinatura válida e ativa do VMware Cloud Foundation para usar o Amazon EVS.

O Amazon EVS usa assinaturas do VMware Cloud Foundation (VCF) com direitos de portabilidade de licenças que você traz para (BYOS). AWS Para implantar com sucesso um ambiente Amazon EVS, você precisa fornecer uma chave de solução VCF válida e uma chave de licença vSAN na solicitação de criação do ambiente. A chave de licença do vSphere serve como a chave da solução para o VCF. Cada chave de licença do VCF só pode ser usada para um ambiente Amazon EVS. A

criação do ambiente falhará se você tentar usar uma chave de licença VCF que já esteja em uso em outro ambiente.

Sua chave de solução VCF deve ter pelo menos 256 núcleos para fornecer capacidade de núcleo adequada para os quatro EC2 hosts i4i.metal iniciais que o Amazon EVS implanta na criação do ambiente. Cada host i4i.metal requer 64 núcleos. A chave de licença do vSAN deve ter pelo menos 110 TiB de capacidade do vSAN. A criação do ambiente falhará se você tentar usar chaves de licença subdimensionadas.

> **Note**
>
> Sua assinatura do VCF estará disponível para o Amazon EVS em todas as AWS regiões para fins de conformidade com as licenças. O Amazon EVS não valida as chaves de licença. Para validar as chaves de licença, visite o suporte da Broadcom.

> **Note**
>
> As informações sobre seu software VCF no Amazon EVS serão compartilhadas com a Broadcom para verificar a conformidade da licença.

Gerenciamento de assinaturas

Você é responsável por gerenciar suas assinaturas do VCF. Suas assinaturas do VCF devem ser gerenciadas no SDDC Manager. Remover suas chaves de licença do SDDC Manager ou substituí-las por uma chave de licença em uso resultará em uma falha na verificação do status do ambiente, impedindo que você adicione hosts ao seu ambiente Amazon EVS. Para obter mais informações sobre verificações de status do ambiente the section called “Monitore o status do ambiente” the section called “Solucionar problemas nas verificações de status do ambiente que falharam” e. Para obter mais informações sobre as chaves de licença do VCF, consulte Gerenciamento de chaves de licença no VMware Cloud Foundation na documentação do VMware Cloud Foundation.

> **Important**
>
> Use a interface de usuário do SDDC Manager para gerenciar a solução VCF e as chaves de licença do vSAN. O Amazon EVS exige que você mantenha uma solução VCF válida e as chaves de licença do vSAN no SDDC Manager para que o serviço funcione adequadamente.

Embora as chaves devam ser atribuídas aos seus hosts e ao cluster vSAN usando o vSphere Client, você deve garantir que essas chaves também apareçam na tela de licenciamento da interface de usuário do SDDC Manager.

Adicionando chaves de licença VCF

No portal de suporte da Broadcom, você pode comprar chaves de licença VCF adicionais, dividir chaves de licença se já tiver chaves grandes ou mesclar várias chaves de licença. Isso permite licenciar os hosts que você adicionou ao seu ambiente após a implantação inicial ou licenciar ambientes adicionais. Certifique-se de que as chaves de licença compradas sejam adicionadas ao inventário do vCenter Sever e do SDDC Manager. Ao adicionar hosts, certifique-se de que suas licenças estejam atribuídas aos hosts corretos no vSphere e tenham núcleos e capacidade de armazenamento vSAN adequados. O Amazon EVS não oferece suporte a hosts não licenciados. Para obter mais informações, consulte Definindo configurações de licença para ativos no vSphere Client na VMware documentação.

Novas chaves de licença não expiradas devem ser atribuídas ao vCenter Server antes que o período de avaliação da chave de licença expire para permanecerem ativas. As chaves de licença ativas são necessárias para configurar com sucesso um ambiente Amazon EVS. Seu ambiente falhará na implantação se uma chave de licença expirada for fornecida. Para obter mais informações sobre a criação da chave de licença VCF, consulte Criar uma nova licença na VMware documentação. Se você estiver enfrentando problemas com as chaves de licença adicionadas, consultethe section called “Falha na verificação da cobertura da chave”.

Removendo as chaves de licença do VCF

Você pode remover as chaves de licença do VCF do inventário do SDDC Manager para reduzir sua capacidade principal e do vSAN depois de excluir os hosts em seu ambiente. Para permanecer em conformidade com os modelos de licenciamento dos produtos que você usa com o vSphere, você deve remover todas as chaves de licença não atribuídas do inventário. Se você dividiu, mesclou ou atualizou as chaves de licença no Portal de Suporte da Broadcom, você deve remover as chaves de licença antigas. Para obter mais informações, consulte Remover uma licença na VMware documentação.

Versões e tipos de EC2 instância do VCF fornecidos pelo Amazon EVS

O Amazon EVS fornece várias versões do VMware Cloud Foundation (VCF), ESX e tipos de EC2 instância que você pode selecionar ao criar um ambiente e criar um host.

Verificando as versões do VCF, as versões do ESX e EC2 os tipos de instância fornecidos

O AWS console mostra a lista de versões do VCF fornecidas pelo Amazon EVS no assistente de criação de ambiente. As versões disponíveis do ESX são visíveis quando você seleciona um tipo de instância ao adicionar um host a um ambiente existente. Você também pode visualizar as versões do VCF, as versões do ESX e os tipos de EC2 instância usando a CLI.

Example

Amazon EVS console

1. Acesse o console do Amazon EVS.
2. No menu de navegação, escolha Ambientes.
3. Execute um destes procedimentos:

   Para verificar as versões do VCF:

   a. Selecione Criar ambiente.

   b. Nos requisitos de Validar Amazon EVS, escolha sua versão do VCF para ver se o status está disponível ou restrito para você.

   Para verificar as versões do ESX:

   a. Selecione um ambiente existente.

   b. Escolha Create host (Criar host).

   c. Selecione um tipo de instância para ver as versões disponíveis do ESX.

AWS CLI

Execute o comando a seguir para recuperar informações sobre as versões do VCF e do ESX:

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

Exemplo de resposta:

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

> **Note**
>
> Se a versão de que você precisa aparecer `RESTRICTED` e você tiver uma necessidade específica, consulte the section called “Solicitar acesso a versões restritas do VCF” para obter mais informações sobre como obter acesso a essa versão.

Versões atuais do VCF no Amazon EVS

Atualmente, o Amazon EVS fornece as seguintes versões do VCF para criação de ambientes:

Versão do VCF	Versão padrão do ESX	Status	EC2 tipos de instância
VCF-5.2.2	ESXi-8,0 U3G-24859861	DISPONÍVEL	i4i.metal
VCF-5.2.1	ESXi-8.0U3B-24280767	RESTRITO	i4i.metal

> **Note**
>
> Ao criar um novo ambiente Amazon EVS, você deve especificar uma versão do VCF.

Considerações sobre a versão ESX

Cada versão do VCF tem uma versão padrão do ESX com base na lista de materiais (BOM) do VCF da Broadcom. Ao criar um novo ambiente, você não pode escolher uma versão específica do ESX. A versão padrão do ESX para a versão selecionada do VCF é aplicada automaticamente.

No entanto, ao adicionar um host ao seu ambiente, você pode selecionar uma versão do ESX disponível para o tipo de instância escolhido. Se você não especificar uma, o Amazon EVS usa a versão padrão do ESX associada à versão do VCF do seu ambiente.

Depois que um host é adicionado, sua versão ESX só pode ser atualizada usando o vCenter Lifecycle Manager.

> **Note**
>
> O Amazon EVS não fornece todas as versões do VCF e do ESX lançadas pela Broadcom. Para obter informações sobre interoperabilidade de software, consulte a Matriz de interoperabilidade da Broadcom. Para obter total compatibilidade de hardware com AWS EC2 instâncias, consulte o Guia de compatibilidade da Broadcom.

Solicitar acesso a versões restritas do VCF

Se você precisar acessar uma versão do VCF com `RESTRICTED` status, entre em contato com o AWS Support com as seguintes informações:

- ID AWS da sua conta
- A AWS região
- A versão específica do VCF que você precisa
- Seu caso de uso e justificativa comercial (por exemplosecurity/compliance, compatibility/dependency, e outros)

AWS O Support analisará sua solicitação e aprovará ou solicitará informações adicionais. Após a aprovação, o status da versão mudará para `AVAILABLE` no AWS console ou na resposta `get-versions` da API.

Gerenciamento do ciclo de vida do ambiente Amazon EVS

Esta página descreve suas responsabilidades de gerenciamento do ciclo de vida em um ambiente Amazon EVS.

Um dos principais benefícios do Amazon EVS é que você tem controle total sobre sua VMware arquitetura na nuvem. Você pode otimizar a pilha de software VMware Cloud Foundation (VCF) para atender às demandas exclusivas de seus aplicativos. Como o Amazon EVS é um serviço autogerenciado, você é responsável pelo gerenciamento do ciclo de vida e pela manutenção do VMware software usado no ambiente do Amazon EVS, como ESX, vSphere, vSAN, NSX e SDDC Manager. Você também é responsável por manter todas as integrações de terceiros, como soluções de proteção de dados que você integra aos seus hosts Amazon EVS.

Você é responsável pela configuração dos componentes de AWS rede subjacentes que o Amazon EVS usa, incluindo tabelas de rotas de VPC, grupos de segurança e regras de lista de controle de acesso (ACL) à rede, configuração do VPC Route Server, gateways de internet, gateways NAT e gateways de trânsito (para conectividade local).

AWS é responsável por implantar o ambiente Amazon EVS com as configurações de rede que você fornece. A implantação do ambiente inclui o seguinte:

- Inicializando a configuração de rede do seu ambiente Amazon EVS.
- Habilitando o roteamento norte-sul com a instância do VPC Route Server que você fornece.

- Implantação das sub-redes EVS VLAN, interfaces de rede elásticas e quatro hosts ESX iniciais necessários.
- Configurando uma rede de sobreposição NSX com um gateway de nível 0 e um gateway de nível 1.
- Implantação de um cluster NSX Edge com dois nós do NSX Edge no modo. Active/Standby
- Criação e configuração do cluster vSAN inicial e montagem do armazenamento de dados.

Você é responsável pela configuração do VMware NSX, incluindo segmentos de rede, regras de firewall distribuído e balanceadores de carga. Você também é responsável pela configuração de todas as soluções integradas que você implementa com o Amazon EVS após a implantação do ambiente EVS, incluindo a configuração VMware HCX e gateways NSX Tier-1 adicionais.

Para obter mais informações AWS e responsabilidades do cliente, consulte o modelo de responsabilidade AWS compartilhada.

> **Note**
>
> Um gateway de nível 0 e um gateway de nível 1 são criados e configurados como parte da implantação do ambiente Amazon EVS. No momento, o Amazon EVS só oferece suporte a um único gateway de nível 0. Qualquer modificação nesses roteadores lógicos ou no nó de borda do NSX VMs pode afetar a conectividade e deve ser evitada.

VMware atualizações de software

> **Warning**
>
> Se você atualizou sua versão do ESX após a implantação do ambiente Amazon EVS, o SDDC Manager pode falhar durante a validação do host do VCF na etapa de comissão de hosts. Para obter as etapas para solucionar esse problema, consultethe section called “O SDDC Manager falha na validação do host VCF durante o comissionamento do host”.

Para obter informações sobre as versões do VCF fornecidas pelo Amazon EVS, consulte. the section called “Versões e EC2 instâncias do VCF” De acordo com o modelo de responsabilidade AWS compartilhada, você é responsável por aplicar quaisquer patches, atualizações ou upgrades ao software VCF, incluindo ESX, vCenter Server, vSAN, NSX, SDDC Manager e outras soluções

integradas, em seu ambiente EVS. Após a implantação, recomendamos que você revise a versão do software VCF implantada pelo Amazon EVS e atualize conforme necessário. Você pode obter atualizações do VCF por meio do portal de suporte da Broadcom. Também recomendamos que você estabeleça e siga um cronograma de manutenção regular para atualizações e patches.

> **Note**
>
> O Amazon EVS não é compatível com o VMware Cloud Foundation 9 no momento.

> **Note**
>
> O Amazon EVS não fornece todas as versões do VCF e do ESX lançadas pela Broadcom. Para obter informações sobre interoperabilidade de software, consulte a Matriz de interoperabilidade da Broadcom. Para obter total compatibilidade de hardware com AWS EC2 instâncias, consulte o Guia de compatibilidade da Broadcom.

Certos patches, atualizações ou upgrades podem ter impacto nas cargas de trabalho em execução em seu ambiente. Antes de aplicar patches, atualizar ou atualizar seu software VCF, recomendamos que você revise o Guia de gerenciamento do ciclo de vida do VCF para entender como essas mudanças afetarão seu ambiente. Também recomendamos que você teste as alterações em um ambiente de preparação antes de implantá-las na produção. Você pode revisar as notas de lançamento do VCF 5.2.x para entender as atualizações mais recentes do VCF 5.2.x.

Ciclo de vida e manutenção do host ESX

Você é responsável pelo gerenciamento e manutenção do ciclo de vida do host ESX no ambiente Amazon EVS, incluindo o monitoramento da integridade do host e a correção de problemas do host. Para obter mais informações, consulte the section called “Manutenção do ambiente”.

AWS realiza manutenção programada nas EC2 instâncias i4i.metal subjacentes para garantir confiabilidade, disponibilidade e desempenho da infraestrutura. Para obter mais informações, consulte the section called “Sobre a manutenção AWS programada para EC2 instâncias”.

Realizando manutenção em seu ambiente

Esta seção descreve como realizar tarefas comuns de manutenção para seu ambiente Amazon EVS.

Tópicos

Monitore o status e os recursos do seu ambiente

Você pode monitorar vários aspectos do seu ambiente Amazon EVS e dos AWS recursos subjacentes usando o console do Amazon EVS ou. AWS CLI

> **Note**
>
> VMware Os componentes do Cloud Foundation (VCF) são monitorados no SDDC Manager. Você não pode monitorar componentes do VCF usando o console Amazon EVS ou. AWS CLI Para obter informações sobre como usar o SDDC Manager para monitorar os componentes do VMware Cloud Foundation (VCF), consulte Introdução ao SDDC Manager.

Visualize o status e os recursos do ambiente

O status do ambiente ajuda você a determinar se seu ambiente está enfrentando problemas que exigem atenção. Siga este procedimento para verificar o status do seu ambiente e visualizar os recursos subjacentes.

Example

Amazon EVS console

1. Abra o console do Amazon EVS.
2. No painel de navegação, escolha Ambientes.
3. Escolha sua ID do ambiente para abrir a página de detalhes do ambiente.
4. Em Detalhes, visualize o status do ambiente.

Se seu ambiente estiver íntegro, o status será exibido como Aprovado. Se houver problemas, o status será exibido como Falha. Quando o status for Falha, você poderá visualizar um popover que mostra os resultados de quatro verificações de status do ambiente:

- Reutilização da chave - Mostra que foi aprovada ou falhou para indicar se a chave de licença do VCF é válida.
- Contagem de hosts - mostra Desconhecido, Aprovado ou Falha para indicar o status da conectividade do host.
- Cobertura da chave - Mostra a opção aprovada ou reprovada para indicar se a chave de licença do VCF cobre todos os hosts.
- Acessibilidade - Mostra aprovação ou falha para indicar a acessibilidade ao SDDC Manager.

Para obter informações sobre como solucionar problemas de falhas na verificação do status do ambiente, consulteSolução de problemas.

Para visualizar os recursos em seu ambiente

Escolha uma das seguintes guias:

- Hosts - Mostra os hosts em seu ambiente.
- Redes e conectividade — Mostra os recursos de VPC, sub-redes EVS e VPC Route Server associados ao seu ambiente.
- Dispositivos de gerenciamento - Mostra os dispositivos de gerenciamento do VCF em seu ambiente com seus nomes de host DNS e credenciais relacionadas.
- Tags - Mostra as tags associadas ao seu ambiente.

AWS CLI

Você pode usar o AWS CLI para verificar o status e os recursos do seu ambiente.

Para listar todos os ambientes e seus status

```
aws evs list-environments
```

> **Tip**
>
> Use o `--query` parâmetro para filtrar a saída. Por exemplo:

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

Para listar os hosts do ambiente

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

Para listar o ambiente VLANs

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

Para obter mais informações sobre as operações de API, consulte o seguinte no Guia de referência de API do Amazon EVS:

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

Manutenção da AMI

O Amazon EVS implanta hosts ESX com um EVS Amazon Machine Image (AMI) personalizado. A AMI contém um complemento personalizado do fornecedor contendo os pacotes necessários para executar o ESX na Amazon. EC2

Solucionar problemas de falha na adição de host devido à imagem de cluster incompatível

Quando você adiciona um host ao seu ambiente, o host tem a versão mais recente disponível do complemento EVS Custom Vendor. Se seu ambiente usa hosts com uma versão complementar mais antiga, a adição de novos hosts falhará com um erro de que o novo host não é compatível com sua imagem de cluster. Para obter etapas detalhadas para corrigir esse problema, consultethe section called “Falha na adição do host devido à imagem de cluster incompatível”.

Manutenção do host Amazon EVS

Como o Amazon EVS é um serviço autogerenciado, você é responsável pela manutenção do software VMware Cloud Foundation (VCF) executado no host, monitorando a integridade do host

e remediando problemas do host, incluindo a substituição do host em caso de falha do host. Para obter mais informações sobre o gerenciamento de hosts ESX no VMware Cloud Foundation (VCF), consulte Gerenciamento de host na documentação do VMware Cloud Foundation.

Verificando a integridade da EC2 instância subjacente

A Amazon EC2 realiza verificações automatizadas em cada EC2 instância em execução para identificar problemas de hardware e software. Você pode ver os resultados dessas verificações de status no EC2 console ou AWS CLI identificar problemas específicos e detectáveis. Para obter mais informações, consulte Exibir verificações de status da EC2 instância da Amazon no Guia EC2 do usuário da Amazon e describe-instance-statusna Referência da linha de AWS CLI comando.

Você pode criar um CloudWatch alarme para avisá-lo se as verificações de status falharem em uma instância específica. Para obter mais informações, consulte Criar CloudWatch alarmes para EC2 instâncias da Amazon que falham nas verificações de status no Guia EC2 do usuário da Amazon.

Sobre a manutenção AWS programada para EC2 instâncias

AWS executa a manutenção programada nas EC2 instâncias subjacentes para garantir confiabilidade, disponibilidade e desempenho. EC2 instâncias bare metal estão sujeitas aos mesmos tipos de eventos programados que outras EC2 instâncias. AWS pode programar eventos para reinicializar, interromper e desativar suas instâncias devido a problemas de hardware subjacentes ou manutenção programada. Esses eventos não ocorrem com frequência. Para obter mais informações, consulte Tipos de eventos programados no Guia EC2 do usuário da Amazon.

> **Note**
>
> Você deve colocar seus hosts no modo de manutenção no vSphere Client antes de qualquer evento de reinicialização agendado.

Se uma de suas instâncias for afetada por um evento programado, AWS notificará você com antecedência por e-mail, usando o endereço de e-mail associado ao seu Conta da AWS. AWS também envia um evento AWS Health, que você pode monitorar e gerenciar usando a Amazon EventBridge. Para obter mais informações, consulte Monitoramento de eventos em AWS Health with Amazon EventBridge e Eventos programados para EC2 instâncias da Amazon no Guia EC2 do usuário da Amazon.

A qualquer momento, você pode reagendar o evento para que ele ocorra em uma data e hora específicas que sejam adequadas para você. O evento pode ser reprogramado até a data de prazo

do evento. Para obter mais informações, consulte Reagendar um evento programado para uma EC2 instância no Guia do usuário da Amazon EC2 .

Usando reservas EC2 de capacidade sob demanda

Você pode usar reservas de capacidade EC2 sob demanda para garantir que seu cluster tenha capacidade suficiente durante os períodos de manutenção. Você pode reservar capacidade em uma zona de disponibilidade específica por qualquer período. Para obter mais informações, consulte Reservar capacidade computacional com reservas de capacidade EC2 sob demanda no Guia EC2 do usuário da Amazon.

Para ver as etapas para criar uma reserva de capacidade, consulte Criar uma reserva de capacidade no Guia EC2 do usuário da Amazon.

> **Note**
>
> Se você usa reservas de capacidade EC2 sob demanda ou hosts EC2 dedicados, recomendamos que você mantenha um host extra para cargas de trabalho de missão crítica. Embora as reservas de capacidade garantam que você tenha acesso a uma quantidade específica de capacidade de EC2 instância em uma determinada zona de disponibilidade, ter um host extra fornece uma camada adicional de redundância que é crucial para cargas de trabalho de missão crítica. Para hosts dedicados, ter um host extra garante que você mantenha o ambiente para cargas de trabalho essenciais, mesmo que um host principal exija manutenção ou tenha algum problema.

Preparação para AWS **`system-maintenance`** programações e **`instance-retirement`** eventos

AWS agenda dois tipos de `system-maintenance` eventos: manutenção de rede e manutenção de energia.

- Durante a manutenção de rede, instâncias programadas perdem a conectividade de rede durante um breve período. A conectividade de rede normal com a instância é restaurada depois que a manutenção for concluída.
- Durante a manutenção de energia, as instâncias programadas ficam offline durante um breve período e depois são reinicializadas. Quando uma reinicialização é executada em instâncias EC2 bare metal, os dados do volume do armazenamento de instâncias não são preservados.

AWS agenda EC2 `instance-retirement` eventos quando a degradação do hardware subjacente que hospeda suas EC2 instâncias é detectada.

Para remediar `system-maintenance` os `instance-retirement` eventos, substitua o host com falha por um novo host usando o console Amazon EVS ou AWS CLI o SDDC Manager antes que o evento de manutenção ocorra. Se você esperar que o evento de manutenção ocorra e a reinicialização da EC2 instância seja necessária, você perderá os dados do vSAN que estão armazenados no volume de armazenamento da instância. Para obter detalhes das etapas, consulte, the section called “Substitua um host Amazon EVS”.

> **Important**
>
> O EC2 console não deve ser usado para gerenciar o estado dos seus hosts do Amazon EVS, incluindo interrupção, início e encerramento. Não tente iniciar, interromper ou encerrar as EC2 instâncias que o Amazon EVS implanta. Essa ação resulta na perda de dados do vSAN.

Substitua um host Amazon EVS

Siga este procedimento para substituir um host Amazon EVS.

> **Warning**
>
> Os anfitriões do Amazon EVS usam um complemento personalizado do fornecedor para fornecer funcionalidades importantes do host. Quando você adiciona um host ao seu ambiente, ele terá a versão mais recente disponível do complemento personalizado do Amazon EVS. Se seu ambiente usa hosts com uma versão complementar mais antiga, adicionar um host ao seu cluster vSphere fará com que a correção da imagem do cluster falhe. Para obter as etapas para solucionar esse problema, consultethe section called “Solucionar problemas de falha na adição de host devido à imagem de cluster incompatível”.

> **Warning**
>
> Se você atualizou sua versão do ESX após a implantação, o SDDC Manager pode falhar durante a validação do host VCF na etapa de comissionamento de hosts. Para obter as etapas para solucionar esse problema, consultethe section called “O SDDC Manager falha na validação do host VCF durante o comissionamento do host”.

> **Note**
>
> Certifique-se de que sua contagem de hosts do Amazon EVS por cota de ambiente EVS esteja definida corretamente para garantir a criação bem-sucedida do host. A criação do host falhará se esse valor de cota for menor que o número de hosts que você está tentando provisionar em um único ambiente Amazon EVS. Talvez seja necessário solicitar um aumento de cota para operações de manutenção que exijam a substituição do host. Para obter mais informações, consulte Cotas de serviço.

Example

Amazon EVS console and SDDC Managuer UI

1. Acesse o console do Amazon EVS.
2. No painel de navegação, escolha Ambiente.
3. Selecione o ambiente que contém o host a ser substituído.
4. Selecione a guia Hosts.
5. Escolha Create host (Criar host).
6. Especifique os detalhes do host e escolha Criar host.
7. Para verificar a conclusão, verifique se o estado do host foi alterado para Criado.
8. Recupere as credenciais da senha raiz do ESX no Secrets Manager AWS . Para obter mais informações sobre como recuperar segredos, consulte Obter AWS segredos do Secrets Manager no Guia do usuário do AWS Secrets Manager.
9. Acesse o SDDC Manager.
10. Comissione o novo host no SDDC Manager, usando as credenciais raiz do ESX que você recuperou na etapa anterior. Para obter mais informações, consulte Commission Hosts na documentação da VMware Cloud Foundation.
11. Adicione o novo host ao cluster. Para obter mais informações, consulte Como adicionar um host ESX ao seu cluster do vSphere usando o fluxo de trabalho de início rápido na documentação do vSphere.
12. Desative o host antigo no SDDC Manager que você deseja remover do SDDC Manager. Para obter mais informações, consulte Descomissionar hosts na documentação do VMware Cloud Foundation.
13. Retorne ao console do Amazon EVS.

14. Na guia Hosts, selecione o host com falha e escolha Excluir > Excluir host.

AWS CLI and SDDC Manager UI

1. Abra uma nova sessão de terminal.
2. Crie um novo host. Veja o exemplo de comando abaixo para referência.

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

3. Recupere as credenciais da senha raiz do ESX no Secrets Manager AWS . Para obter mais informações sobre como recuperar segredos, consulte Obter AWS segredos do Secrets Manager no Guia do usuário do AWS Secrets Manager.
4. Acesse o SDDC Manager.
5. Comissione o novo host no SDDC Manager, usando as credenciais raiz do ESX que você recuperou na etapa anterior. Para obter mais informações, consulte Commission Hosts na documentação da VMware Cloud Foundation.
6. Adicione o novo host ao cluster que contém o host danificado.
7. Desative o host com defeito no SDDC Manager. Para obter mais informações, consulte Descomissionar hosts na documentação do VMware Cloud Foundation.
8. Retorne ao terminal.
9. Exclua o host com falha. Veja o exemplo de comando abaixo para referência.

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

Solução de problemas

Para obter ajuda sobre a resolução de problemas, consulte Solução de problemas. Se você continuar enfrentando problemas depois de analisar as orientações de solução de problemas, entre em contato com o AWS Support para obter mais assistência.

Configurar uma tabela de rotas personalizada para sub-redes Amazon EVS

O Amazon EVS suporta o uso de uma tabela de rotas personalizada somente após a criação do ambiente Amazon EVS. Para permitir a criação bem-sucedida do ambiente, você deve configurar a tabela de rotas principal para permitir o tráfego para serviços dependentes, como DNS e sistemas locais. Isso ocorre porque as sub-redes VLAN do Amazon EVS estão implicitamente associadas à tabela de rotas principal da nossa VPC durante a implantação do ambiente.

Depois que seu ambiente for implantado, você deverá associar explicitamente cada uma das sub-redes de VLAN do Amazon EVS a uma tabela de rotas em sua VPC. A conectividade do NSX falhará se suas sub-redes de VLAN não estiverem explicitamente associadas a uma tabela de rotas da VPC. É altamente recomendável que você associe explicitamente suas sub-redes a uma tabela de rotas personalizada. Uma tabela de rotas personalizada fornece um controle mais granular sobre o roteamento do tráfego de rede em sua VPC, permitindo regras de roteamento personalizadas para sub-redes ou gateways específicos. Para obter mais informações sobre a criação de uma tabela de rotas personalizada, consulte Criar uma tabela de rotas para sua VPC no Guia do usuário da Amazon VPC.

Configurar uma lista de controle de acesso à rede para controlar o tráfego de sub-rede VLAN do Amazon EVS

Uma lista de controle de acesso (ACL) de rede permite ou não determinado tráfego de entrada ou de saída no nível da sub-rede. Você pode usar ACLs a rede para controlar o tráfego de entrada e saída para suas sub-redes de VLAN do Amazon EVS. Para obter mais informações, consulte Criar uma rede ACL para sua VPC no Guia do usuário da Amazon VPC.

> **Important**
>
> EC2 os grupos de segurança não funcionam em interfaces de rede elásticas conectadas às sub-redes VLAN do Amazon EVS. Para controlar o tráfego de e para as sub-redes VLAN do Amazon EVS, você deve usar uma lista de controle de acesso à rede.

> **Warning**
>
> O Amazon EVS exige acesso à sua implantação do VCF. Você deve configurar seus grupos de segurança e listas de controle de acesso à rede (ACLs) para permitir que o Amazon EVS se comunique com:

- Servidores DNS na TCP/UDP porta 53.
- Sub-rede VLAN de gerenciamento de host via HTTPS e SSH.
- Gerenciamento da sub-rede VM VLAN por HTTPS e SSH.

Se seus grupos de segurança e sua rede ACLs não permitirem esse acesso, a implantação do ambiente Amazon EVS falhará e os ambientes existentes poderão ter um status de conformidade degradado.

Ciclo de vida do gerenciamento secreto

O Amazon EVS usa o AWS Secrets Manager para criar, criptografar e armazenar segredos em sua conta na implantação inicial do ambiente. Esses segredos contêm as credenciais do VCF necessárias para instalar e acessar os dispositivos de gerenciamento do VCF, como vCenter Server, NSX e SDDC Manager, bem como a senha raiz do host ESX. O Amazon EVS também exclui segredos gerenciados em seu nome quando o ambiente EVS é excluído.

Você é responsável pelo gerenciamento do ciclo de vida secreto, incluindo a rotação secreta. O Amazon EVS não oferece alternância gerenciada de seus segredos. Recomendamos que você alterne os segredos regularmente em uma janela de rotação definida para garantir que os segredos não durem muito. Para obter mais informações, consulte Cronogramas de rotação no Guia do Usuário do AWS Secrets Manager.

Crie um host Amazon EVS

Depois que um ambiente Amazon EVS é implantado, você pode adicionar hosts para aumentar a capacidade e a resiliência da carga de trabalho. O Amazon EVS oferece suporte de 4 a 16 hosts por ambiente. Essa ação só pode ser usada após a implantação do ambiente Amazon EVS.

> **Note**
>
> Você deve atribuir e comissionar o host na interface de usuário do SDDC Manager.

Para criar um host Amazon EVS

Siga estas etapas para criar um host Amazon EVS.

Warning

Os anfitriões do Amazon EVS usam um complemento personalizado do fornecedor para fornecer funcionalidades importantes do host. Quando você adiciona um host ao seu ambiente, ele terá a versão mais recente disponível do complemento personalizado Amazon EVS. Se seu ambiente usa hosts com uma versão complementar mais antiga, adicionar um host ao seu cluster vSphere fará com que a correção da imagem do cluster falhe. Para obter as etapas para solucionar esse problema, consultethe section called “Solucionar problemas de falha na adição de host devido à imagem de cluster incompatível”.

Warning

Se você atualizou sua versão do ESX após a implantação do ambiente Amazon EVS, o SDDC Manager pode falhar durante a validação do host do VCF na etapa de comissão de hosts. Para obter as etapas para solucionar esse problema, consultethe section called “O SDDC Manager falha na validação do host VCF durante o comissionamento do host”.

Note

Certifique-se de que sua contagem de hosts do Amazon EVS por cota de ambiente EVS esteja definida corretamente para garantir a criação bem-sucedida do host. A criação do host falhará se esse valor de cota for menor que o número de hosts que você está tentando provisionar em um único ambiente Amazon EVS. Para aumentar a cota, você pode solicitar um aumento de cota. Para obter mais informações, consulte Cotas de serviço.

Note

Se você não especificar uma versão do ESX ao adicionar hosts ao seu ambiente, o Amazon EVS usa automaticamente a versão padrão do ESX associada à versão do VCF do seu ambiente. Consulte the section called “Versões e EC2 instâncias do VCF” para obter mais informações.

> **Important**
>
> Ao adicionar um host ESX, selecione uma versão do ESX que corresponda ao seu cluster vSphere de destino. Se a mesma versão não estiver disponível, implante uma versão mais antiga e atualize usando o vSphere Lifecycle Manager. Para obter mais informações, consulte the section called “O SDDC Manager falha na validação do host VCF durante o comissionamento do host”. As atualizações podem exigir a reinicialização do host e aumentar o tempo necessário para comissionar o host.
> Um host com uma versão ESX mais recente que a versão ESX da imagem de cluster do vSphere não pode ser rebaixada. Você precisará excluir o host e recriá-lo com a versão correta do ESX.

Example

Amazon EVS console and SDDC Managuer UI

1. Acesse o console do Amazon EVS.
2. No painel de navegação, escolha Ambiente.
3. Selecione o ambiente em que você deseja criar o host.
4. Selecione a guia Hosts.
5. Escolha Create host (Criar host).
6. Especifique os detalhes do host e escolha Criar host.
7. Para verificar a conclusão, verifique se o estado do host foi alterado para Criado.
8. Acesse o SDDC Manager.
9. Comissione o novo host no SDDC Manager. Para obter mais informações, consulte Commission Hosts na documentação da VMware Cloud Foundation.
10. Adicione o novo host ao cluster usando o SDDC Manager. Para obter mais informações, consulte Como adicionar um host ESX ao seu cluster do vSphere usando o fluxo de trabalho de início rápido na documentação do vSphere.

AWS CLI and SDDC Manager UI

1. Abra uma nova sessão de terminal.
2. Crie um novo host. Veja o exemplo de comando abaixo para referência.

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

3. Acesse o SDDC Manager.
4. Comissione o novo host no SDDC Manager. Para obter mais informações, consulte Commission Hosts na documentação da VMware Cloud Foundation.
5. Adicione o novo host ao cluster usando o SDDC Manager. Para obter mais informações, consulte Como adicionar um host ESX ao seu cluster do vSphere usando o fluxo de trabalho de início rápido na documentação do vSphere.

Excluir um host Amazon EVS

Você pode excluir um host Amazon EVS do seu ambiente quando o host não for mais necessário. O Amazon EVS exige que seu ambiente tenha no mínimo quatro hosts. O Amazon EVS não oferece suporte a ambientes com menos de quatro hosts.

> **Warning**
>
> Excluir um host sem descomissionar deixará dados obsoletos no vCenter e no SDDC Manager, o que pode exigir esforços adicionais de limpeza. Certifique-se de que seus hosts sejam desativados antes de excluir os hosts no console ou na API do Amazon EVS.

> **Warning**
>
> Sempre use o console ou a API do Amazon EVS para remover seus hosts do Amazon EVS. A exclusão de hosts do EC2 console pode deixar seu ambiente em um estado inconsistente.

Para excluir um host Amazon EVS

Siga estas etapas para excluir um host Amazon EVS.

Example

SDDC Managuer UI and Amazon EVS console

1. Acesse o SDDC Manager.
2. Remova o cluster do SDDC Manager.
3. Desative o host no SDDC Manager. Para obter mais informações, consulte Descomissionar hosts na documentação do VMware Cloud Foundation.
4. Acesse o console do Amazon EVS.
5. No painel de navegação, escolha Ambiente.
6. Selecione o ambiente que contém o host a ser excluído.
7. Selecione a guia Hosts.
8. Escolha Excluir host.
9. Selecione o host e escolha Excluir na guia Hosts. Repita essa etapa para cada host que você deseja excluir.

SDDC Manager UI and AWS CLI

1. Acesse o SDDC Manager.
2. Remova o cluster do SDDC Manager.
3. Desative o host no SDDC Manager. Para obter mais informações, consulte Descomissionar hosts na documentação do VMware Cloud Foundation.
4. Abra uma nova sessão de terminal.
5. Exclua o host. Veja o exemplo de comando abaixo para referência.

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

Segurança no Amazon Elastic VMware Service

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que é executada Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Elastic VMware Service (Amazon EVS), consulte Serviços da AWS Escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon EVS. Ele mostra como configurar o Amazon EVS para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros Serviços da AWS que ajudam você a monitorar e proteger seus recursos do Amazon EVS.

Conteúdo

Proteção de dados no Amazon EVS

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon Elastic VMware Service. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa toda a AWS nuvem. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura, incluindo os componentes do VMware Cloud Foundation (VCF).

Você também é responsável pelas tarefas de configuração e gerenciamento de segurança do Serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management. Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.

  > **Note**
  >
  > O Amazon EVS não registra a atividade do usuário para não AWS componentes, como a atividade em seu ambiente VCF. Essas atividades são registradas em vários VMware consoles, como o vSphere e o NSX Manager. Se desejar um registro centralizado de VCF, você pode configurar soluções de monitoramento de VCF, como VMware Aria Operations ou VMware Tanzu Observability, para alcançar esse resultado. Para obter mais informações, consulte VMware Cloud Foundation com VMware Tanzu e VMware Aria Suite Lifecyle no modo VMware Cloud Foundation na documentação do VCF.

- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços de segurança gerenciados avançados Amazon Macie, como, que ajudam a descobrir e proteger dados confidenciais armazenados em. Amazon S3
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como os endereços de e-mail de seus clientes, em tags ou campos de texto de formato livre, como o campo Nome. Isso inclui quando você trabalha com o Amazon EVS ou outro Serviços da AWS usando o console, a API ou AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia em repouso

O Amazon EVS implanta EC2 instâncias i4i.metal que usam criptografia AES-256 transparente por padrão para dados armazenados no volume de armazenamento de instâncias. No momento, o Amazon EVS não oferece suporte à criptografia do volume de inicialização do EBS.

Volume de inicialização do Amazon EBS

As instâncias i4i.metal do Amazon EVS usam um volume de inicialização do Amazon EBS. O volume de inicialização contém o sistema operacional e outros arquivos necessários para que a EC2 instância seja inicializada e executada. O volume de inicialização não está criptografado. No momento, o Amazon EVS não oferece suporte à criptografia do volume de inicialização. O volume de inicialização não contém dados do usuário de suas máquinas virtuais.

Volumes de armazenamento de instâncias

As EC2 instâncias i4i.metal do Amazon EVS vêm com armazenamento NVMe SSD local, que faz parte do hardware da instância. O Amazon EVS usa volumes de armazenamento de NVMe instâncias como discos para datastores vSAN. O armazenamento de dados vSAN mantém suas máquinas virtuais de gerenciamento e carga de trabalho depois que você implanta seu ambiente Amazon EVS.

Os dados nos volumes de armazenamento da NVMe instância são criptografados usando uma cifra XTS-AES-256, implementada em um módulo de hardware na instância. As chaves usadas para criptografar dados gravados em dispositivos de NVMe armazenamento conectados localmente são por cliente e por volume. Para obter mais informações, consulte Criptografia em repouso no Guia EC2 do usuário da Amazon.

Depois de implantar o ambiente Amazon EVS, você pode habilitar a criptografia data-at-rest vSAN para todos os dados armazenados no datastore vSAN, para máquinas virtuais individuais VMs () ou para arquivos individuais contidos nele. VMs Esse controle granular pode ser útil quando alguns VMs exigem criptografia e outros não, ou quando discos ou arquivos específicos em uma VM precisam

ser criptografados. Para obter mais informações, consulte Como funciona a Data-At-Rest criptografia do vSAN na documentação do vSAN VMware .

Criptografia em trânsito

O Amazon EVS não criptografa seu tráfego em trânsito por padrão. Para criptografar os dados em trânsito que atravessam o Amazon EVS, você pode usar a criptografia da camada de aplicação com um protocolo como o Transport Layer Security (TLS). Para saber mais sobre a criptografia de tráfego de EC2 instâncias, consulte Criptografia em trânsito no Guia EC2 do usuário da Amazon.

> **Note**
>
> A criptografia de rede Nitro não se aplica às EC2 instâncias que o Amazon EVS implanta. O Amazon EVS não oferece suporte à criptografia em trânsito do tráfego entre hosts.

Opções de criptografia em trânsito para conectividade local

Para criptografar o tráfego entre seu datacenter local e o Amazon EVS, você pode combinar o uso do AWS Direct Connect e da AWS Site-To-Site VPN com o Transit Gateway AWS . Essa combinação fornece uma conexão privada IPsec criptografada que também reduz os custos da rede, aumenta a taxa de transferência da largura de banda e fornece uma experiência de rede mais consistente do que as conexões VPN baseadas na Internet. Para obter mais informações, consulte AWS Site-to-Site VPN IP privada com AWS Direct Connect.

> **Note**
>
> O Amazon EVS não oferece suporte à conectividade por meio de uma interface virtual privada (VIF) do AWS Direct Connect ou por meio de uma conexão AWS Site-to-Site VPN que termina diretamente na VPC subjacente. O Amazon EVS oferece suporte à terminação de IPSec VPN no gateway NSX Edge de nível 0 ou nível 1. Para obter mais informações, consulte Adicionar um serviço NSX IPSec VPN na documentação do VMware NSX.

O MAC Security (MACsec) é um padrão IEEE que fornece confidencialidade, integridade e autenticidade da origem dos dados. Você pode usar conexões AWS Direct Connect que oferecem suporte MACsec para criptografar seus dados do data center corporativo até o local do AWS Direct Connect. Para obter mais informações, consulte Segurança MAC no AWS Direct Connect no Guia do usuário do AWS Direct Connect.

Criptografia em trânsito para dados VMware de rede

Após a implantação do ambiente Amazon EVS, você tem várias opções para aplicar a criptografia de dados em trânsito na camada VCF: VMware

- VMware Firewall distribuído vDefend - permite que você implemente uma segmentação de rede refinada e imponha a criptografia entre TLS/SSL máquinas virtuais. Para obter mais informações, consulte Definir configurações de segurança para firewall distribuído usando a interface do usuário na documentação do VMware VCF.
- data-in-transitCriptografia vSAN - pode ser usada para criptografar todos os dados e metadados entre os hosts em seu cluster vSAN. Para obter mais informações, consulte vSAN Data-In-Transit Encryption na documentação do vSAN VMware .
- vSphere vMotion criptografado - garante a confidencialidade, integridade e autenticidade dos dados que são transferidos com o vSphere vMotion. Para obter mais informações, consulte O que é o vSphere vMotion criptografado na documentação do vSphere.

Gerenciamento de chaves e segredos

Durante a implantação do ambiente Amazon EVS, o Amazon EVS usa o AWS Secrets Manager para criar, criptografar e armazenar segredos que contêm as credenciais do VCF necessárias para instalar e acessar os dispositivos de gerenciamento do VMware VCF, bem como a senha raiz do ESX. O Amazon EVS também exclui segredos gerenciados em seu nome quando o ambiente EVS é excluído. Para obter mais informações, consulte O que há em um segredo do Secrets Manager no Guia do usuário do AWS Secrets Manager.

O Secrets Manager usa criptografia de envelope com AWS KMS chaves e chaves de dados para proteger cada valor secreto. A chave AWS gerenciada padrão do Secrets Manager é usada, a menos que especificado de outra forma. Como alternativa, você pode especificar uma chave gerenciada pelo cliente durante a criação do ambiente para criptografar seus segredos. Para obter mais informações, consulte Criptografia e descriptografia secretas no AWS Secrets Manager no Guia do usuário do AWS Secrets Manager.

> **Note**
>
> Há cobranças adicionais de uso das chaves gerenciadas pelo cliente. A chave AWS gerenciada padrão é fornecida sem nenhum custo. Para obter mais informações, consulte Preços no Guia do Usuário do AWS Secrets Manager.

O Amazon EVS não sincroniza credenciais entre o AWS Secrets Manager e seu software VCF após a implantação. Você é responsável por garantir que os segredos associados ao seu ambiente Amazon EVS sejam mantidos em sincronia com as credenciais no SDDC Manager para evitar a expiração da senha do VCF e a perda de acesso ao software do VCF.

O Amazon EVS não troca segredos em seu nome. Você é responsável por alternar os segredos associados ao seu ambiente. É altamente recomendável alternar seus segredos assim que o ambiente for criado e implementar um cronograma de rotação para atualizá-los em intervalos regulares. Para obter mais informações sobre a rotação de AWS segredos do Secrets Manager, consulte a função Rotation by Lambda no Guia do usuário AWS do Secrets Manager. Para obter mais informações sobre o gerenciamento de senhas do VCF, consulte Gerenciamento de senhas na documentação do VMware Cloud Foundation.

Important

O Amazon EVS não sincroniza credenciais entre o AWS Secrets Manager e seu software VCF após a implantação. Se estiver usando o AWS Secrets Manager após a implantação, você deve manter as credenciais entre o AWS Secrets Manager e o SDDC Manager sincronizadas para evitar problemas de expiração da senha do VCF. Você pode perder o acesso ao software VCF se as credenciais do SDDC Manager não forem mantidas atualizadas.

Note

O Amazon EVS não fornece rotação gerenciada de segredos.

Note

Há custos em usar uma função Lambda para a rotação secreta do AWS Secrets Manager. Para obter mais informações, consulte Preços no Guia do Usuário do AWS Secrets Manager.

Privacidade do tráfego entre redes

O Amazon EVS usa uma VPC fornecida pelo cliente para criar limites entre os recursos no ambiente do Amazon EVS e controlar o tráfego entre eles, sua rede local e a Internet. Para obter mais

informações sobre Amazon VPC segurança, consulte Garantir a privacidade do tráfego entre redes Amazon VPC no Guia do Amazon VPC usuário.

Por padrão, o Amazon EVS cria sub-redes de VLAN privadas durante a criação do ambiente que negam acesso direto à Internet. Para adicionar outra camada de segurança à sua VPC, você pode criar uma lista personalizada de controle de acesso à rede para sua VPC com regras que restringem ainda mais a conectividade com a Internet. Para obter mais informações, consulte Criar uma ACL de rede para sua VPC no Guia do usuário da Amazon VPC.

> **Important**
>
> EC2 os grupos de segurança não funcionam em interfaces de rede elásticas conectadas às sub-redes VLAN do Amazon EVS. Para controlar o tráfego de e para as sub-redes VLAN do Amazon EVS, você deve usar uma lista de controle de acesso à rede.

Se você for administrador do NSX, poderá configurar os seguintes recursos do NSX para proteger o tráfego de rede:

- VMware Firewall vDefend Gateway - Protege o perímetro da rede, protegendo contra ameaças externas (tráfego norte-sul). Para obter mais informações, consulte Adicionar uma política e regra de firewall de gateway na documentação do VMware NSX.
- VMware Firewall distribuído vDefend - Protege contra ataques originados de uma rede interna (tráfego leste-oeste). Para obter mais informações, consulte Adicionar um firewall distribuído na documentação do VMware NSX.

Gerenciamento de identidade e acesso para o Amazon Elastic VMware Service

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAM os administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar os recursos do Amazon Elastic VMware Service (Amazon EVS). IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como o Amazon EVS funciona com IAM
- Exemplos de políticas baseadas em identidade do Amazon EVS
- Solução de problemas de identidade e acesso ao Amazon EVS
- AWS políticas gerenciadas para Amazon EVS
- Usando funções vinculadas a serviços para o Amazon EVS

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Amazon EVS.

Usuário do serviço — Se você usa o serviço Amazon EVS para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Amazon EVS para fazer seu trabalho, você pode precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador.

Se você não conseguir acessar um recurso no Amazon EVS, consultethe section called “Solução de problemas de identidade e acesso ao Amazon EVS”.

Administrador de serviços - Se você é responsável pelos recursos do Amazon EVS em sua empresa, provavelmente tem acesso total ao Amazon EVS. É seu trabalho determinar quais recursos e recursos do Amazon EVS seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar IAM com o Amazon EVS, consultethe section called “Como o Amazon EVS funciona com IAM”.

IAM administrador - Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Amazon EVS. Para ver exemplos de políticas baseadas em identidade do Amazon EVS que você pode usar, consulte. IAMthe section called “Exemplos de políticas baseadas em identidade do Amazon EVS”

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como usuário raiz da AWS conta Usuário do IAM, ou assumindo uma IAM função.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. Centro de Identidade do AWS IAM (Centro de Identidade do IAM) usuários, a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no Console de gerenciamento da AWS ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do usuário AWS de login.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte Processo de assinatura do Signature versão 4 na Referência AWS geral.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte o Guia do usuário da autenticação multifator no AWS IAM Identity Center (sucessor do AWS Single Sign-On) e Como usar a autenticação multifator (MFA) AWS no Guia do usuário do IAM.

AWS usuário raiz da conta

Ao criar um Conta da AWS, você começa com uma única identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário raiz da AWS conta e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente o usuário raiz possa executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz,

consulte Tarefas que exigem credenciais de usuário raiz no Guia de referência de gerenciamento de contas.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o Centro de Identidade do AWS IAM. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no Guia do AWS usuário do IAM Identity Center (sucessor do AWS Single Sign-On).

Usuários do IAM e grupos

An Usuário do IAMé uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar Usuários do IAM credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo Usuários do IAM, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um IAM grupo é uma identidade que especifica uma coleção de Usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários

têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar uma Usuário do IAM (em vez de uma função) no Guia do usuário do IAM.

IAM funções

Uma IAM função é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um Usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no Console de gerenciamento da AWS trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos de uso de funções, consulte Como usar IAM funções no Guia do usuário do IAM.

IAM funções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões com uma função no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário AWS do IAM Identity Center (sucessor do AWS Single Sign-On).
- Usuário do IAM Permissões temporárias — Um Usuário do IAM pode assumir uma IAM função para assumir temporariamente diferentes permissões para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Como as IAM funções diferem das políticas baseadas em recursos no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos Amazon EC2 ou armazene objetos em Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.

- Permissões principais — Quando você usa uma função Usuário do IAM or para realizar ações em AWS, você é considerado diretor. Permissões concedidas por políticas a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, acionar outra ação em outro serviço. Nesse caso, você precisa ter permissões para executar ambas as ações.
- Função de serviço — Uma função de serviço é uma IAM função que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamente IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma Amazon EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível ao armazenamento de chaves de acesso na Amazon EC2 instância. Para atribuir uma AWS função a uma Amazon EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na Amazon EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em Amazon EC2 instâncias no Guia do usuário do IAM.

Para saber se usar IAM funções, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Cada IAM entidade (usuário ou função) começa sem permissões. Por padrão, os usuários não podem fazer nada, nem mesmo alterar sua própria senha. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou o administrador pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo recebem essas permissões.

IAM as políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da Console de gerenciamento da AWS AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como uma Usuário do IAM função ou grupo. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais atributos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de política JSON que você anexa a um recurso, como um bucket. Amazon S3 Os administradores do serviço podem usar essas políticas para definir quais ações um principal especificado (função, usuário ou membro da conta) pode executar nesse recurso e sob quais condições. As políticas baseadas em recursos são políticas em linha. Não há políticas baseadas em recursos gerenciadas.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) são um tipo de política que controla quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON. Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte ACLs. Para saber mais ACLs, consulte a visão geral da Lista de Controle de Acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (Usuário do IAM ou função). Você pode definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade da entidade e seus limites de permissões. As políticas baseadas em recursos que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada usuário raiz AWS da conta. Para obter mais informações sobre Organizations e SCPs, consulte How SCPs work in the AWS Organizations User Guide.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e as políticas da sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o Amazon EVS funciona com IAM

Antes de usar IAM para gerenciar o acesso ao Amazon EVS, saiba quais IAM recursos estão disponíveis para uso com o Amazon EVS.

IAM recurso	Suporte ao Amazon EVS
the section called “Políticas baseadas em identidade para Amazon EVS”	Sim
the section called “Políticas baseadas em recursos no Amazon EVS”	Não
the section called “Ações políticas para o Amazon EVS”	Sim
the section called “Recursos de política para o Amazon EVS”	Parcial
the section called “Chaves de condição de política para Amazon EVS”	Sim
the section called “Listas de controle de acesso (ACLs) no Amazon EVS”	Não
the section called “Controle de acesso baseado em atributos (ABAC) com o Amazon EVS”	Sim
the section called “Usando credenciais temporárias com o Amazon EVS”	Sim
the section called “Sessões de acesso direto para o Amazon EVS”	Sim

IAM recurso	Suporte ao Amazon EVS
the section called “Funções de serviço para Amazon EVS”	Não
the section called “Funções vinculadas a serviços para Amazon EVS”	Sim

Para obter uma visão de alto nível de como o Amazon EVS e outros Serviços da AWS trabalham com IAM, consulte Serviços da AWS esse trabalho IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para Amazon EVS

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você usa em uma política JSON, consulte a referência aos elementos da política IAM JSON no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para Amazon EVS

Para ver exemplos de políticas baseadas em identidade do Amazon EVS, consulte. the section called “Exemplos de políticas baseadas em identidade do Amazon EVS”

Políticas baseadas em recursos no Amazon EVS

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos,

os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para o Amazon EVS

Suporta ações Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O `Action` elemento de uma política IAM baseada em identidade descreve a ação ou ações específicas que serão permitidas ou negadas pela política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. A ação é usada em uma política para conceder permissões para executar a operação associada.

As ações de política no Amazon EVS usam o seguinte prefixo antes da ação:. `evs:` Por exemplo, para conceder permissão a alguém para criar um ambiente com a operação da `CreateEnvironment` API Amazon EVS, você inclui a `evs:CreateEnvironment` ação na política dessa pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Amazon EVS define seu próprio conjunto de ações que descrevem as tarefas que você pode realizar com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

```
"Action": [
```

```
      "evs:action1",
      "evs:action2"
```

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a seguinte ação:

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

Para ver uma lista de ações do Amazon EVS, consulte Ações definidas pelo Amazon EVS na Referência de autorização de serviço.

Recursos de política para o Amazon EVS

Suporte a recursos de políticas: parcial

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos do Amazon EVS e seus ARNs, consulte Recursos definidos pelo Amazon Elastic VMware Service na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon Elastic VMware Service.

Algumas ações da API do Amazon EVS oferecem suporte a vários recursos. Por exemplo, vários ambientes podem ser referenciados ao chamar a ação da `ListEnvironments` API. Para especificar vários recursos em uma única instrução, separe-os ARNs com vírgulas.

```
"Resource": [
```

```
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

Por exemplo, o recurso de ambiente Amazon EVS tem o seguinte ARN:

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

Para especificar os ambientes `my-environment-1` e `my-environment-2` em sua declaração, use o exemplo a seguir ARNs:

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

Para especificar todos os ambientes que pertencem a uma conta específica, use o caractere curinga (*):

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

Chaves de condição de política para Amazon EVS

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O `Condition` elemento (ou `Condition` bloco) permite especificar as condições nas quais uma declaração está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder uma Usuário do IAM permissão para acessar um recurso somente se ele estiver

marcado com o Usuário do IAM nome dele. Para obter mais informações, consulte elementos IAM de política: variáveis e tags no Guia do usuário do IAM.

O Amazon EVS define seu próprio conjunto de chaves de condição e também oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Todas as Amazon EC2 ações oferecem suporte às teclas de `ec2:Region` condição `aws:RequestedRegion` e de condição. Para obter mais informações, consulte Example: Restricting access to a specific region.

Para ver uma lista das chaves de condição do Amazon EVS, consulte Chaves de condição do Amazon EVS na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon EVS.

Listas de controle de acesso (ACLs) no Amazon EVS

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso baseado em atributos (ABAC) com o Amazon EVS

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Você pode anexar tags aos recursos do Amazon EVS ou passar tags em uma solicitação para o Amazon EVS. Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/<key-name>`, `aws:RequestTag/<key-name>` ou chaves de condição `aws:TagKeys`. Para obter mais

informações sobre com quais ações você pode usar tags em chaves de condição, consulte Ações definidas pelo Amazon EVS na Referência de Autorização de Serviço.

Usando credenciais temporárias com o Amazon EVS

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS "Trabalhe com o IAM" no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login Console de gerenciamento da AWS usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para o Amazon EVS

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para Amazon EVS

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Funções vinculadas a serviços para Amazon EVS

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do Amazon EVS, consulte. the section called “Uso de perfis vinculados ao serviço”

Exemplos de políticas baseadas em identidade do Amazon EVS

Por padrão, Usuários do IAM as funções não têm permissão para criar ou modificar recursos do Amazon EVS. Eles também não podem realizar tarefas usando a AWS API Console de gerenciamento da AWS AWS CLI, ou. Um IAM administrador deve criar IAM políticas que concedam aos usuários e funções permissão para realizar operações de API específicas nos recursos especificados de que precisam. O administrador deve então anexar essas políticas aos grupos Usuários do IAM ou grupos que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Como criar políticas usando o editor JSON no Guia do usuário do IAM.

Tópicos

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon EVS em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e passe para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar IAM para aplicar permissões, consulte Políticas e permissões IAM no Guia do usuário do IAM.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para obter mais informações, consulte Elementos da política IAM JSON: condição no Guia do usuário do IAM.
- Use IAM Access Analyzer para validar suas IAM políticas para garantir permissões seguras e funcionais — IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem de políticas (JSON) e IAM as melhores práticas. IAM IAM Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte a validação de IAM Access Analyzer políticas no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que Usuários do IAM exija ou faça root de usuários em sua conta, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Usando o console Amazon EVS

Para acessar o console do Amazon EVS, um diretor do IAM deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que o diretor liste e visualize detalhes sobre os recursos do Amazon EVS em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para as entidades principais com essa política anexada.

Para garantir que seus diretores do IAM ainda possam usar o console do Amazon EVS, crie uma política com seu próprio nome exclusivo, como. `AmazonEVSAdminPolicy` Anexe a política às entidades principais. Para obter mais informações, consulte Adição de permissões a um usuário no Guia do usuário do 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"
                }
            }
        }
    ]
}
```

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita visualizar Usuários do IAM as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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": "*"
        }
    ]
```

```
}
```

Crie e gerencie um ambiente Amazon EVS

Este exemplo de política inclui as permissões necessárias para criar e excluir um ambiente Amazon EVS e adicionar ou excluir hosts após a criação do ambiente.

Você pode Região da AWS substituir o pelo no Região da AWS qual deseja criar um ambiente. Se sua conta já tiver o perfil `AWSServiceRoleForAmazonEVS`, você poderá remover a ação `iam:CreateServiceLinkedRole` da política. Se você já criou um ambiente Amazon EVS em sua conta, já existe uma função com essas permissões, a menos que você a tenha excluído.

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

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

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

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

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

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

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

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

```
        },
        {
            "Sid": "SecretsManagerTagging",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true",
                    "aws:ResourceTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsManagerOps",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DeleteSecret",
                "secretsmanager:GetSecretValue",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "SecretsManagerRandomPassword",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "EVSPermissions",
            "Effect": "Allow",
            "Action": [
                "evs:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyAccessInConsole",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:*:*:key/*"
        },

        {
            "Sid": "KMSKeyAliasAccess",
            "Effect": "Allow",
            "Action": [
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
}
```

Obtenha e liste ambientes, hosts e hosts do Amazon EVS VLANs

Esse exemplo de política inclui as permissões mínimas exigidas para que um administrador obtenha e liste todos os ambientes e hosts do Amazon EVS VLANs dentro de uma determinada conta no Região da AWS us-east-2.

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

```
    }
  ]
}
```

Solução de problemas de identidade e acesso ao Amazon EVS

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Amazon EVS e. IAM

Tópicos

- AccessDeniedException
- Quero permitir que pessoas de fora da minha Conta da AWS acessem meus recursos do Amazon EVS

AccessDeniedException

Se você receber um `AccessDeniedException` ao chamar uma operação de AWS API, as credenciais principais do IAM que você está usando não têm as permissões necessárias para fazer essa chamada.

```
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
```

Na mensagem de exemplo anterior, o usuário não tem permissão para chamar a operação da `CreateEnvironment` API Amazon EVS. Para fornecer permissões de administrador do Amazon EVS a um diretor do IAM, consultethe section called “Exemplos de políticas baseadas em identidade do Amazon EVS”.

Para obter mais informações gerais sobre o IAM, consulte Controlar o acesso aos AWS recursos usando políticas no Guia do usuário do IAM.

Quero permitir que pessoas de fora da minha Conta da AWS acessem meus recursos do Amazon EVS

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para

serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon EVS oferece suporte a esses recursos, consultethe section called “Como o Amazon EVS funciona com IAM”.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um Usuário do IAM em outro Conta da AWS de sua propriedade no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Como as IAM funções diferem das políticas baseadas em recursos no Guia do usuário do IAM.

AWS políticas gerenciadas para Amazon EVS

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes. Para obter mais informações, consulte políticas AWS gerenciadas no Guia IAM do usuário.

AWS política gerenciada: Amazon EVSService RolePolicy

Não é possível anexar `AmazonEVSServiceRolePolicy` às entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite que o Amazon EVS execute ações em seu nome. Para obter mais informações, consulte the section called “Uso de perfis vinculados ao serviço”. Quando você cria um ambiente usando um diretor do IAM que tem a `iam:CreateServiceLinkedRole` permissão, a função `AWSServiceRoleforAmazonEVS` vinculada ao serviço é criada automaticamente para você com essa política anexada a ela.

Essa política permite que a função `AWSServiceRoleForAmazonEVS` vinculada ao serviço ligue Serviços da AWS em seu nome.

Detalhes das permissões

Essa política inclui as seguintes permissões que permitem que o Amazon EVS conclua as seguintes tarefas.

- `ec2`- Descubra os componentes da rede VPC, incluindo sub-redes e. VPCs Crie, modifique, marque e exclua interfaces de rede elástica que são usadas para estabelecer uma conexão persistente entre o Amazon EVS e o dispositivo SDDC Manager da VMware Virtual Cloud Foundation (VCF) em sua sub-rede VPC. Essa conectividade é necessária para que o Amazon EVS implante, gerencie e monitore a implantação do VCF.
- `ec2`- Exclua as instâncias do EC2 que o Amazon EVS cria quando você faz uma solicitação de exclusão do host do EVS. Descreva e modifique os atributos da instância EC2 para que o encerramento padrão da instância EC2 e a proteção contra interrupção possam ser desativados, se necessário, para oferecer suporte à exclusão do host EVS.
- `ec2`- Gerencie volumes do EBS para instalação e limpeza do Cloud Builder. Durante a criação do ambiente, o Cloud Builder é instalado em um dos hosts implantados do Amazon EVS para realizar alterações na configuração do VCF. Após a conclusão, o Amazon EVS remove o Cloud Builder desanexando e excluindo o volume do EC2 em que ele está armazenado.
- `ec2`- Exclua as sub-redes EVS VLAN em seu nome se você solicitar a exclusão do ambiente.
- `secretsmanager`- Exclua as senhas do VCF que o Amazon EVS cria e armazena no AWS Secrets Manager durante a criação do ambiente. O Amazon EVS exclui todos os segredos que o serviço cria em sua conta se a criação do ambiente falhar ou se você solicitar a exclusão do ambiente. Recupere as credenciais do vCenter do Secrets AWS Manager ao configurar um conector vCenter fornecendo um ARN secreto. A permissão tem como escopo uma condição de tag de recurso `EvsAccess=true` para garantir que o Amazon EVS acesse somente segredos explicitamente marcados para acesso ao Amazon EVS vCenter.

- `kms`- Descriptografe segredos e descreva chaves KMS quando as credenciais do vCenter armazenadas no Secrets Manager são criptografadas com chaves KMS. A permissão tem como escopo uma condição de tag de recurso `EvsAccess=true` para garantir que o Amazon EVS acesse somente as chaves KMS marcadas explicitamente para acesso ao vCenter.
- `cloudwatch`- Publique métricas de AWS uso CloudWatch para recursos do Amazon EVS que tenham cotas.

Para ver mais detalhes sobre a política, incluindo a versão mais recente do documento de política JSON, consulte Amazon EVSService RolePolicy no Guia de referência de políticas AWS gerenciadas.

Atualizações do Amazon EVS para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Amazon EVS desde que esse serviço começou a monitorar essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento.

Alteração	Descrição	Data
Amazon EVSService RolePolicy — Política atualizada	O Amazon EVS atualizou a política para permitir que o serviço recupere as credencia is do vCenter do Secrets AWS Manager e decodifiq ue segredos criptografados com chaves KMS. Para saber mais, consulte the section called “AWS política gerenciad a: Amazon EVSService RolePolicy”.	23 de março de 2026
Amazon EVSService RolePolicy — Política atualizada	O Amazon EVS atualizou a política para adicionar recursos abrangentes de gerenciamento de recursos, incluindo gerenciamento de instâncias EC2, operações de	14 de agosto de 2025

Alteração	Descrição	Data
	volume do EBS e integração com o AWS Secrets Manager. Para saber mais, consulte the section called “AWS política gerenciada: Amazon EVSService RolePolicy”.	
Amazon EVSService RolePolicy — Política atualizada	O Amazon EVS atualizou a política para permitir que o serviço exclua sub-redes de VLAN do EVS, bem como publique métricas de uso do Amazon EVS no. CloudWatch Para saber mais, consulte the section called “AWS política gerenciada: Amazon EVSService RolePolicy”.	14 de julho de 2025
Amazon EVSService RolePolicy — Nova política adicionada	O Amazon EVS adicionou uma nova política que permite que o serviço se conecte a uma sub-rede VPC na conta do cliente. Essa conexão é necessária para a funcionalidade do serviço. Para saber mais, consulte the section called “AWS política gerenciada: Amazon EVSService RolePolicy”.	9 de junho de 2025
O Amazon EVS começou a monitorar as mudanças	O Amazon EVS começou a monitorar as mudanças em suas políticas AWS gerenciadas.	9 de junho de 2025

Usando funções vinculadas a serviços para o Amazon EVS

O Amazon Elastic VMware Service usa AWS funções vinculadas ao serviço Identity and Access Management (IAM). Uma função vinculada a serviços é um tipo exclusivo de função do IAM vinculada diretamente ao Amazon EVS. As funções vinculadas ao serviço são predefinidas pelo Amazon EVS e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do Amazon EVS porque você não precisa adicionar manualmente as permissões necessárias. O Amazon EVS define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o Amazon EVS pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos do Amazon EVS porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas aos serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Permissões de função vinculadas ao serviço para Amazon EVS

O Amazon EVS usa a função vinculada ao serviço chamada. `AWSServiceRoleForAmazonEVS` A função permite que o Amazon EVS gerencie ambientes em sua conta. A política anexada permite que a função gerencie os seguintes recursos: interfaces de rede elástica EVS, sub-redes EVS VLAN, hosts EVS e métricas. VPCs CloudWatch

O perfil vinculado ao serviço `AWSServiceRoleForAmazonEVS` confia nos seguintes serviços para aceitar o perfil:

- `evs.amazonaws.com`

A política de permissões de função permite que o Amazon EVS conclua as seguintes ações nos recursos especificados:

- AmazonEVSServiceRolePolicy

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM.

Criação de uma função vinculada a serviços para o Amazon EVS

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria um ambiente na Console de gerenciamento da AWS AWS CLI ou na AWS API, o Amazon EVS cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria um ambiente, o Amazon EVS cria novamente a função vinculada ao serviço para você.

Editando uma função vinculada ao serviço para o Amazon EVS

O Amazon EVS não permite que você edite a função vinculada ao `AWSServiceRoleForAmazonEVS` serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para saber mais, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para o Amazon EVS

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir qualquer recurso usado pelo perfil. Para ver as etapas para excluir um ambiente Amazon EVS com hosts, consultethe section called “Exclua os hosts e o ambiente do Amazon EVS”.

> **Note**
>
> Se o serviço Amazon EVS estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM, a AWS CLI ou a AWS API para excluir a função vinculada ao `AWSServiceRoleForAmazonEVS` serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas ao serviço do Amazon EVS

O Amazon EVS oferece suporte ao uso de funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte endpoints e cotas do Amazon Elastic VMware Service no Guia de referência AWS geral.

Resiliência no Amazon EVS

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, que são conectadas por meio de redes de baixa latência, alta taxa de transferência e altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Os ambientes Amazon EVS estão disponíveis em uma única zona de AWS disponibilidade. Para garantir a alta disponibilidade da infraestrutura Single-AZ do Amazon EVS, o Amazon EVS oferece os seguintes recursos:

> **Note**
>
> No momento, o Amazon EVS só oferece suporte a implantações Single-AZ.

- O Amazon EVS suporta o uso do AWS Elastic Disaster Recovery para automatizar o backup e a recuperação de seus dados.
- O Amazon EVS implanta um cluster NSX Edge com dois nós Active/Standby NSX Edge de acordo com os requisitos do VCF. Os nós do NSX Edge são executados em diferentes hosts para garantir alta disponibilidade e permitir um rápido failover no caso raro de um nó do NSX Edge falhar.
- O Amazon EVS implanta um ambiente mínimo de quatro hosts ESX, exigido pelo VCF. Hosts adicionais podem ser adicionados após a implantação. Esse é um requisito de VMware design para garantir o quorum adequado do vSAN e manter a disponibilidade durante as operações de

manutenção e falhas do host. Para obter mais informações, consulte vSphere Cluster Design for VMware Cloud Foundation na documentação do VMware Cloud Foundation.

- O Amazon EVS oferece suporte ao uso de um grupo de posicionamento de EC2 partições ou de um grupo de posicionamento de clusters para EC2 hosts. O grupo de posicionamento de partições distribui suas EC2 instâncias em partições lógicas, de forma que grupos de instâncias em uma partição não compartilhem o hardware subjacente com grupos de instâncias em partições diferentes. Essa estratégia ajuda a reduzir a probabilidade de falhas de hardware correlacionadas para grandes cargas de trabalho distribuídas. Grupos de posicionamento de clusters são usados para colocar suas EC2 instâncias no mesmo rack físico para garantir baixa latência. Para obter mais informações, consulte Grupos de posicionamento de partições no Guia Amazon EC2 do usuário.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

VMware resiliência de componentes

Os clientes do Amazon EVS são responsáveis por configurar os VMware componentes em execução no Amazon EVS para garantir a alta disponibilidade de suas máquinas virtuais (VMs) e a resiliência da carga de trabalho.

O Amazon EVS oferece suporte aos seguintes recursos de resiliência do VMware Cloud Foundation (VCF):

- Replicação do vSphere - fornece replicação assíncrona e baseada em host para fins de recuperação de desastres e migração de carga de trabalho. VMs Para obter mais informações, consulte Como funciona a replicação do vSphere na documentação do vSphere VMware Replication.
- Proteção de dados do vSAN — permite que você se recupere rapidamente VMs de falhas operacionais causadas por ataques de ransomware, usando instantâneos nativos armazenados localmente no cluster do vSAN. Para obter mais informações, consulte Usando a proteção de dados do vSAN na documentação do vSAN.
- vSphere HA - Fornece failover automático VMs em caso de falha do host. Para obter mais informações, consulte Design de alta disponibilidade para o vCenter Server for VMware Cloud Foundation na documentação do VCF.
- vSphere Fault Tolerance (FT) — fornece disponibilidade contínua para missões críticas VMs criando e mantendo outra VM idêntica e continuamente disponível para substituí-la no caso de

uma situação de failover. Para obter mais informações, consulte Como funciona a tolerância a falhas na documentação do vSphere.

- Falha de tolerância do vSAN (FTT) — Uma configuração do vSAN que determina quantas falhas de host uma VM pode suportar antes de se tornar inacessível. Isso define o nível de redundância e tolerância a falhas para suas máquinas virtuais no cluster vSAN. Para obter mais informações, consulte Tolerar falhas adicionais com domínio de falha no cluster do vSAN na documentação do vSAN.

Usando o Amazon EVS com outros serviços AWS

O Amazon EVS é integrado Serviços da AWS a outros para fornecer soluções adicionais. Este tópico identifica alguns dos serviços com os quais o Amazon EVS trabalha para adicionar funcionalidade.

Tópicos

Crie recursos do Amazon EVS com AWS CloudFormation

O Amazon EVS é integrado com AWS CloudFormation um serviço que ajuda você a modelar e configurar seus AWS recursos para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja, um ambiente Amazon EVS, por exemplo, e AWS CloudFormation se encarrega de provisionar e configurar esses recursos para você.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus recursos do Amazon EVS de forma consistente e repetida. Basta descrever seus recursos uma vez e, em seguida, provisionar os mesmos recursos repetidamente em várias Contas da AWS regiões.

Amazon EVS e modelos AWS CloudFormation

Para provisionar e configurar recursos para o Amazon EVS e serviços relacionados, você deve entender os AWS CloudFormation modelos. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation Para obter mais informações, consulte O que é AWS CloudFormation Designer? no Guia do AWS CloudFormation usuário.

O Amazon EVS oferece suporte à criação de ambientes em AWS CloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para seus ambientes, consulte a referência de tipo de recurso do Amazon EVS no Guia do AWS CloudFormation usuário.

Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- AWS CloudFormation Guia do usuário
- AWS CloudFormation Guia do usuário da interface de linha de comando

Execute cargas de trabalho de alto desempenho com a Amazon FSx for ONTAP NetApp

O Amazon FSx for NetApp ONTAP é um serviço de armazenamento que permite iniciar e executar sistemas de arquivos ONTAP totalmente gerenciados na nuvem. O ONTAP NetApp é a tecnologia de sistema de arquivos que fornece um conjunto amplamente adotado de recursos de acesso e gerenciamento de dados. FSx for ONTAP fornece os recursos, o desempenho e os sistemas APIs de NetApp arquivos locais com a agilidade, escalabilidade e simplicidade de um serviço totalmente gerenciado. AWS Para obter mais informações, consulte o FSx Guia do usuário do ONTAP.

O Amazon EVS oferece suporte ao uso do Amazon FSx for NetApp ONTAP como armazenamento de NFS/iSCSI dados e como armazenamento conectado ao convidado para VMware máquinas virtuais executadas no Amazon EVS.

Configurar FSx o NetApp ONTAP como um armazenamento de dados NFS

O procedimento a seguir detalha as etapas mínimas necessárias FSx para configurar o NetApp ONTAP como um armazenamento de dados NFS para o Amazon EVS usando o FSx console e a interface do cliente VMware vSphere que é executada no Amazon EVS.

Pré-requisitos

Antes de usar o Amazon EVS com o Amazon FSx for NetApp ONTAP, certifique-se de que as seguintes tarefas de pré-requisito tenham sido concluídas.

- Um ambiente Amazon EVS é implantado em sua Virtual Private Cloud (VPC). Para obter mais informações, consulte Introdução.
- Você tem acesso ao seu cliente vSphere em execução no Amazon EVS.
- Você ou seu administrador de armazenamento devem ter as permissões necessárias para criar e gerenciar os FSx sistemas de arquivos ONTAP em sua VPC. Para obter mais informações, consulte Gerenciamento de identidade e acesso da Amazon FSx para NetApp ONTAP.

Seu diretor do IAM tem as permissões apropriadas para criar e gerenciar FSx sistemas de arquivos ONTAP em sua VPC. Para obter mais informações, consulte the section called “Crie e gerencie um ambiente Amazon EVS”.

Crie um sistema FSx de arquivos para NetApp ONTAP

1. Acesse o FSx console da Amazon.
2. Escolha Create file system (Criar sistema de arquivos).
3. Selecione Amazon FSx para NetApp ONTAP.
4. Escolha Próximo.
5. Selecione Criação padrão.
6. Em Tipo de implantação, selecione uma opção de implantação Single-AZ.

> **Note**
>
> No momento, o Amazon EVS só oferece suporte a implantações Single-AZ.

7. Para capacidade de armazenamento SSD, especifique 1024 GiB.
8. Em Capacidade de taxa de transferência, escolha Especificar capacidade de taxa de transferência. Escolha pelo menos 512 MB/s para Single-AZ 1 ou pelo menos 768 MB/s para Single-AZ 2.
9. Selecione a VPC do Amazon EVS que tenha conectividade com suas sub-redes de VLAN do Amazon EVS.
10. Selecione um grupo de segurança que permita todo o tráfego NFS do ONTAP necessário FSx para a sub-rede VLAN de gerenciamento de host VMkernel do Amazon EVS.
11. Selecione a sub-rede de acesso ao serviço Amazon EVS na qual seu sistema de arquivos será implantado. Para obter mais informações, consulte the section called “Sub-rede de acesso ao serviço”.
12. Para Junction path, especifique um nome significativo, `/vol1` para identificar esse volume no vSphere.
13. Na Configuração de volume padrão, defina a eficiência de armazenamento como Ativada.
14. Deixe a configuração restante em seus valores padrão e escolha Avançar.
15. Examine os atributos do sistema de arquivos e escolha Criar sistema de arquivos.

Recupere o nome DNS do NFS para a máquina virtual de armazenamento

1. Acesse o FSx console da Amazon.
2. No menu à esquerda, selecione Sistemas de arquivos.
3. Escolha o sistema de arquivos recém-criado.
4. Selecione a guia Máquinas virtuais de armazenamento.
5. Escolha a máquina virtual de armazenamento.
6. Selecione a guia Endpoints.
7. Copie o nome DNS do sistema de arquivos de rede (NFS) para uso posterior no VMware Vsphere.

Crie um armazenamento de dados NFS no vSphere usando o volume for ONTAP FSx

Siga as instruções em Criar um armazenamento de dados NFS no ambiente vSphere para configurar o Amazon FSx for NetApp ONTAP como armazenamento externo para o vSphere. VMware Para a configuração do servidor na interface do cliente vSphere, use o nome DNS NFS da máquina virtual de armazenamento (SVM) que você copiou na etapa anterior.

Configurar o FSx NetApp ONTAP FSx como um armazenamento de dados iSCSI

O procedimento a seguir detalha as etapas mínimas necessárias FSx para configurar o NetApp ONTAP como um armazenamento de dados iSCSI para o Amazon EVS usando FSx o console VMware e a interface do cliente vSphere que são executados no Amazon EVS.

Pré-requisitos

Antes de usar o Amazon EVS com o Amazon FSx for NetApp ONTAP, certifique-se de que as seguintes tarefas de pré-requisito tenham sido concluídas.

- Um ambiente Amazon EVS é implantado em sua Virtual Private Cloud (VPC). Para obter mais informações, consulte Introdução.
- Você tem acesso ao seu cliente vSphere em execução no Amazon EVS.
- Você ou seu administrador de armazenamento devem ter as permissões necessárias para criar e gerenciar os FSx sistemas de arquivos ONTAP em sua VPC. Para obter mais informações, consulte Gerenciamento de identidade e acesso da Amazon FSx para NetApp ONTAP.

Crie um sistema FSx de arquivos para NetApp ONTAP

1. Acesse o FSx console da Amazon.
2. Escolha Create file system (Criar sistema de arquivos).
3. Selecione Amazon FSx para NetApp ONTAP.
4. Escolha Próximo.
5. Selecione Criação padrão.
6. Em Tipo de implantação, selecione uma opção de implantação Single-AZ.

> **Note**
>
> No momento, o Amazon EVS só oferece suporte a implantações Single-AZ.

7. Para capacidade de armazenamento SSD, especifique 1024 GiB.
8. Em Capacidade de taxa de transferência, escolha Especificar capacidade de taxa de transferência. Escolha pelo menos 512 MB/s para Single-AZ 1 ou pelo menos 768 MB/s para Single-AZ 2.
9. Selecione a VPC do Amazon EVS que tenha conectividade com suas sub-redes de VLAN do Amazon EVS.
10. Selecione um grupo de segurança que permita todo o tráfego iSCSI do ONTAP necessário FSx para a sub-rede VLAN de gerenciamento de host do Amazon EVS. VMkernel
11. Selecione a sub-rede de acesso ao serviço Amazon EVS na qual seu sistema de arquivos será implantado. Para obter mais informações, consulte the section called “Sub-rede de acesso ao serviço”.
12. Na Configuração de volume padrão, defina a eficiência de armazenamento como Ativada.
13. Deixe a configuração restante em seus valores padrão e escolha Avançar.
14. Examine os atributos do sistema de arquivos e escolha Criar sistema de arquivos.

Configurar um adaptador iSCSI de software no vSphere para armazenamento de host ESX

Para cada host ESX, você deve configurar o adaptador iSCSI de software para que seus hosts ESX possam usá-lo para acessar o armazenamento iSCSI. Para obter instruções sobre como

configurar o adaptador iSCSI de software para hosts ESX no vSphere, consulte Adicionar ou remover o adaptador iSCSI de software na documentação do produto vSphere. VMware

Depois de configurar o adaptador iSCSI de software, copie o nome qualificado iSCSI (IQN) associado a um adaptador iSCSI. Esses valores serão usados posteriormente.

Criar um LUN iSCSI

FSx for ONTAP permite que você crie Números de Unidade Lógica (LUNs) especificamente destinados ao acesso iSCSI, fornecendo armazenamento em blocos compartilhado para seus hosts ESX. Você usa a CLI do NetApp ONTAP para criar um LUN.

Abaixo está um exemplo de comando.

> **Note**
>
> É recomendável configurar o tamanho do LUN para 90% do tamanho do volume.

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

Para obter mais informações, consulte Criação de um LUN iSCSI no Guia do usuário do FSx for ONTAP.

Configurar e mapear um grupo de iniciadores para o LUN iSCSI

Agora que você criou um LUN iSCSI, a próxima etapa do processo é criar um grupo iniciador (`igroup`) para conectar o volume ao cluster e mapear o LUN para o grupo iniciador. Você usa a CLI do NetApp ONTAP para realizar essas ações.

1. Configure o grupo de iniciadores.

   Abaixo está um exemplo de comando. Para`--initiator`, use o adaptador iSCSI IQNs que você copiou na etapa anterior.

   ```
   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. Confirme se `igroup` existe.

```
lun igroup show
```

3. Mapeie o LUN para o grupo de iniciadores. Abaixo está um exemplo de comando.

```
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. Use o `lun show -path` comando para confirmar se o LUN foi criado, on-line e mapeado.

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

Para obter mais informações, consulte Provisionamento de iSCSI para Linux ou Provisionamento de iSCSI para Windows no Guia do usuário do ONTAP. FSx

Configurar a descoberta dinâmica do iSCSI LUN no vSphere

Para permitir que os hosts ESX vejam o iSCSI LUN, você deve configurar a descoberta dinâmica para cada host na interface do cliente vSphere. No campo do servidor iSCSI, insira o nome DNS (NFS) que você copiou na etapa anterior. Para obter mais informações, consulte Configurar a descoberta dinâmica ou estática para iSCSI e iSER no ESX Host na documentação do produto vSphere VMware .

Crie um armazenamento de dados VMFS no VMware vSphere usando o iSCSI LUN

Os armazenamentos de dados do Virtual Machine File System (VMFS) servem como repositórios para máquinas virtuais. VMware Siga as instruções em Criar um armazenamento de dados vSphere VMFS para configurar o armazenamento de dados VMFS no vSphere usando o iSCSI LUN que você configurou anteriormente. VMware

Solução de problemas

Este capítulo detalha alguns problemas comuns encontrados ao criar ou gerenciar ambientes Amazon EVS.

Solucionar problemas nas verificações de status do ambiente que falharam

O Amazon EVS realiza verificações automatizadas em seu ambiente para identificar problemas. É possível visualizar o status do seu ambiente para identificar problemas específicos e detectáveis.

Revise as informações de verificação do status do ambiente

Para investigar ambientes prejudicados usando o console Amazon EVS

1. Abra o console do Amazon EVS.
2. No painel de navegação, escolha Ambientes e selecione seu ambiente.
3. Selecione a guia Detalhes para ter uma visão geral do ambiente.
4. Verifique o status do ambiente. Passe o mouse sobre esse campo para expandir um popover com resultados individuais para cada verificação de status do ambiente.

Falha na verificação de acessibilidade

A verificação de acessibilidade verifica se o Amazon EVS tem uma conexão persistente com o SDDC Manager. Se o Amazon EVS não conseguir acessar o ambiente, essa verificação falhará.

Se essa verificação falhar, o Amazon EVS não poderá mais acessar o SDDC Manager para validar o status do ambiente e não será mais possível adicionar hosts ao ambiente. A falha na acessibilidade também fará com que a reutilização da chave de licença e as verificações de cobertura da chave falhem e a verificação da contagem de hosts exiba a resposta Desconhecido.

Para garantir a acessibilidade, verifique o seguinte:

- Verifique se seus certificados são válidos e não expiraram. É possível usar a interface de usuário do SDDC Manager ou o cliente do vSphere para gerenciar certificados em um ambiente do VCF.

Após a implantação, é recomendável substituir todos os certificados do domínio de gerenciamento do VMware Cloud Foundation. Para obter mais informações, consulte Gerenciamento de certificados no VMware Cloud Foundation na documentação do VMware Cloud Foundation.

- Certifique-se de que seus servidores DNS possam ser acessados pela sub-rede de acesso ao serviço, que os registros DNS sejam válidos e que não existam nomes de host ou endereços IP duplicados.
- Se você quiser criar suas próprias regras de firewall, siga estas diretrizes:
  - Permita o TCP/UDP acesso aos servidores DNS.
  - Permita o HTTPS/SSH acesso à sub-rede da VLAN de gerenciamento do host.
  - Permita o HTTPS/SSH acesso à sub-rede VLAN da VM de gerenciamento.

Se você ainda não conseguir resolver o problema depois de seguir essas orientações, recomendamos que entre em contato com o AWS Support para obter mais assistência.

Falha na verificação da contagem de hosts

Essa verificação verifica se seu ambiente tem no mínimo quatro hosts, o que é um requisito para o VCF 5.2.x.

Se essa verificação falhar, será necessário adicionar hosts para que seu ambiente atenda a esse requisito mínimo. O Amazon EVS só aceita ambientes com 4 a 16 hosts.

Falha na verificação da reutilização da chave

Essa verificação verifica se a chave de licença do VCF não está sendo usada por outro ambiente Amazon EVS. As licenças do VCF só podem ser usadas para um único ambiente do Amazon EVS. Essa verificação falhará se você fornecer chaves de licença VCF em uma solicitação de criação de ambiente que já esteja sendo usada por outro ambiente.

Se essa verificação falhar, você receberá uma resposta de erro informando que não foi possível criar o ambiente do Amazon EVS. Para resolver o problema, analise suas configurações de licença no SDDC Manager e substitua todas as licenças usadas anteriormente por licenças não utilizadas.

> **Important**
>
> Use a interface de usuário do SDDC Manager para gerenciar a solução VCF e as chaves de licença do vSAN. O Amazon EVS exige que você mantenha uma solução VCF válida e as

chaves de licença do vSAN no SDDC Manager para que o serviço funcione adequadamente. Embora as chaves devam ser atribuídas aos seus hosts e ao cluster vSAN usando o vSphere Client, você deve garantir que essas chaves também apareçam na tela de licenciamento da interface de usuário do SDDC Manager.

Falha na verificação da cobertura da chave

Essa verificação examina se sua chave de licença do VCF atribuída ao vCenter Server aloca núcleos de vCPU e capacidade de armazenamento (TiB) vSAN suficientes para todos os hosts implantados.

Se essa verificação falhar, você receberá uma resposta de erro informando que não foi possível criar o ambiente do Amazon EVS. A falha na cobertura da chave pode indicar um dos seguintes problemas:

- As licenças do VCF não estão atribuídas corretamente ao vCenter Server. É necessário atribuir uma licença ao vCenter Server antes que o período de avaliação expire ou a licença atribuída no momento expire. Se esse for o problema, analise as atribuições de licença no SDDC Manager.
- As licenças atuais do VCF não cobrem as necessidades de capacidade de armazenamento do núcleo do vCPU e do vSAN. A chave da solução VCF deve ter pelo menos 256 núcleos. A chave de licença do vSAN deve ter pelo menos 110 TiB de capacidade do vSAN. Se esse for o problema, adicione licenças do vSAN no SDDC Manager até que suas necessidades de uso sejam atendidas.

Se as ações acima não resolverem o problema, entre em contato com o AWS Support para obter mais assistência.

Important

Use a interface de usuário do SDDC Manager para gerenciar a solução VCF e as chaves de licença do vSAN. O Amazon EVS exige que você mantenha uma solução VCF válida e as chaves de licença do vSAN no SDDC Manager para que o serviço funcione adequadamente. Embora as chaves devam ser atribuídas aos seus hosts e ao cluster vSAN usando o vSphere Client, você deve garantir que essas chaves também apareçam na tela de licenciamento da interface de usuário do SDDC Manager.

O agente vSphere HA neste host não conseguiu alcançar o endereço de isolamento

Na interface de usuário do vCenter, com o host ESX selecionado, você vê a mensagem “O agente vSphere HA neste host não pôde alcançar o endereço de isolamento < endereço>”. IPv6

Essa mensagem de erro indica que o agente vSphere HA em um host não consegue acessar o endereço de IPv6 isolamento padrão que o vSphere HA usa para verificações de pulsação. A mensagem de erro não é indicativa de um problema e só ocorre porque o Amazon EVS não oferece suporte IPv6 no momento. A ausência de IPV6 suporte para o Amazon EVS não afeta a funcionalidade principal do vSphere HA.

As pré-verificações de atualização do vSAN falham para o cluster de host ESX

Ao tentar atualizar o cluster de host ESX usando o SDDC Manager, as pré-verificações relacionadas ao disco do vSAN podem falhar. Isso ocorre porque o Amazon EVS usa o vSAN Express Storage Architecture (ESA) e as pré-verificações de atualização não se aplicam ao vSAN ESA. Para obter mais informações, consulte o artigo da base de conhecimento da Broadcom sobre esse tópico.

Falha na adição do host devido à imagem de cluster incompatível

Problema

Quando você adiciona um host ao seu ambiente, o host tem a versão mais recente disponível do complemento EVS Custom Vendor. Se seu ambiente usa hosts com uma versão complementar mais antiga, a adição de novos hosts falhará com um erro de que o novo host não é compatível com sua imagem de cluster. Para corrigir esse problema, você deve usar o vSphere Lifecyle Manager para extrair a versão mais recente do complemento disponível do host recém-adicionado.

Solução

Siga estas etapas.

1. Acesse o inventário de hosts e clusters no VMware vCenter Server.
2. Extraia o complemento do host recém-adicionado criando um cluster vazio temporário.

3. Em Noções básicas, selecione Importar imagem de um host existente no inventário do vCenter e crie o cluster. Deixe todas as outras configurações como padrão.
4. Depois que esse cluster temporário for criado com a imagem extraída, você poderá excluí-lo. O complemento agora estará disponível em seu depósito do vSphere Lifecycle Manager.
5. Acesse seu cluster de ambiente e selecione a guia Atualizações.
6. Edite sua imagem de cluster e altere a versão complementar para a versão recém-extraída.
7. Escolha Salvar.
8. No SDDC Manager, repita a tarefa de adição de host que falhou. Isso remediará seus hosts de cluster, atualizando todos os hosts para a versão complementar mais recente. A correção da imagem do cluster exigirá a reinicialização do host.

O SDDC Manager falha na validação do host VCF durante o comissionamento do host

Problema

Se você atualizou sua versão do ESX após a implantação do ambiente Amazon EVS, o SDDC Manager pode falhar durante a validação do host do VCF na etapa de comissão de hosts. Para corrigir esse problema, você precisará usar o vSphere Lifecyle Manager para atualizar o ESX no host recém-adicionado.

Solução

Siga estas etapas.

> **Important**
>
> Essas etapas exigem a adição temporária do host ao vCenter fora do SDDC Manager. Usar o vSphere Lifecyle Manager para qualquer operação que não seja a atualização do ESX pode tornar seu host inutilizável e exigir que você exclua e crie um novo host Amazon EVS.

1. Acesse o inventário de hosts e clusters no VMware vCenter Server.
2. Adicione o host temporariamente ao seu data center virtual, garantindo a seleção de gerenciar o host com uma imagem. O host será removido em uma etapa posterior após a conclusão do

upgrade do ESX. Para obter mais informações, consulte Como adicionar um host ao seu data center ou pasta do vSphere na documentação do vSphere.

3. Depois que o host for adicionado ao vSphere, atualize a versão ESX no host. Isso pode ser feito na guia Atualizações do seu host. Edite a imagem do host para corresponder à versão ESX do seu cluster.
4. Após a conclusão da atualização, remova o host do seu inventário do vCenter. Para obter mais informações, consulte Como remover um host ESX da sua instância do vCenter Server na documentação do vSphere.
5. Comissione seu anfitrião no SDDC Manager. Para obter mais informações, consulte Commission Hosts na documentação da VMware Cloud Foundation.
6. Depois que o host for comissionado, adicione-o ao seu cluster usando o SDDC Manager.

Registrando chamadas de API do Amazon EVS usando AWS CloudTrail

O Amazon EVS é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário do IAM, uma função do IAM ou um AWS serviço no Amazon EVS. CloudTrail captura todas as chamadas de AWS API para o Amazon EVS como eventos. As chamadas capturadas incluem chamadas do console do Amazon EVS e chamadas de código para as operações da API do Amazon EVS. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon EVS. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Amazon EVS, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

> **Note**
>
> O Amazon EVS não registra a atividade do usuário para não AWS componentes, como a atividade em seu ambiente VCF. Essas atividades são registradas em vários VMware consoles, como o vSphere e o NSX Manager.
> Se desejar um registro centralizado de VCF, você pode configurar soluções de monitoramento de VCF, como o VMware Cloud Foundation Operations, para alcançar esse resultado.

Informações sobre o Amazon EVS em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no Amazon EVS, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do Amazon EVS, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3.

Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões
- Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Amazon EVS são registradas CloudTrail e documentadas na Referência de API do Amazon EVS. Por exemplo, chamadas para o `CreateEnvironment` `GetEnvironment` e `DeleteEnvironment` as ações geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou de usuário do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Entendendo as entradas do arquivo de log do Amazon EVS

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Cotas do serviço Amazon EVS

O Amazon EVS se integrou ao Service Quotas, e você pode usar para visualizar e gerenciar suas cotas a partir de AWS service (Serviço da AWS) um local central. Para obter mais informações, consulte O que é o Service Quotas? no Guia do usuário do Service Quotas.

Com a integração do Service Quotas, você pode usar o Console de gerenciamento da AWS or AWS CLI para pesquisar o valor de suas cotas do Amazon EVS e solicitar um aumento de cota para cotas ajustáveis. Para obter mais informações, consulte Solicitando um aumento de cota no Service Quotas User Guide request-service-quota-increasee na AWS CLI Command Reference.

Para obter mais informações sobre as cotas de serviços do Amazon EVS, consulte as cotas do Amazon EVS no Guia de referência geral. AWS

Important

Certifique-se de que sua cota de instância padrão em EC2 execução sob demanda reflita o número de v CPUs necessário para todas as EC2 instâncias que você usará no Amazon EVS. Cada instância i4i.metal usa 128 v. CPUs Para obter informações sobre o aumento das cotas de EC2 serviço, consulte Solicitar um aumento no Guia do EC2 usuário da Amazon.

Note

Se você planeja usar hosts EC2 dedicados para seu ambiente Amazon EVS, certifique-se de que sua cota de hosts i4i EC2 dedicados reflita o número de hosts dedicados que você pretende usar na região desejada. Para obter informações sobre o aumento das cotas de EC2 serviço, consulte Solicitar um aumento no Guia do EC2 usuário da Amazon.

Note

Se estiver configurando a conectividade HCX com a Internet, sua cota de IPAM para o comprimento da máscara de rede de blocos IPv4 CIDR públicos contíguos fornecidos pela Amazon deve ser /28 ou maior. Para obter mais informações, consulte Cotas para seu IPAM.

> **Note**
>
> A Amazon CloudWatch coleta métricas AWS de uso para recursos do Amazon EVS que têm cotas (ambiente e hosts). Para obter mais informações, consulte Métricas de CloudWatch uso no Guia CloudWatch do usuário da Amazon.

Veja as cotas de serviço do Amazon EVS no Console de gerenciamento da AWS

1. Abra o console do Service Quotas.
2. No painel de navegação esquerdo, escolha AWS serviços.
3. Na lista de AWS serviços, pesquise e selecione Amazon Elastic VMware Service.
4. Escolha Visualizar cotas.

   Na lista de cotas de serviço, você pode ver o nome da cota de serviço, o valor aplicado (se disponível), a cota AWS padrão e se o valor da cota é ajustável.
5. Para visualizar informações adicionais sobre uma service quota, como descrição, escolha o nome da cota.
6. (Opcional) Para solicitar um aumento de cota, selecione a cota que você deseja aumentar, selecione Solicitar aumento no nível da conta, insira ou selecione as informações necessárias e selecione Solicitar.

Para trabalhar mais com cotas de serviço usando o Console de gerenciamento da AWS, consulte o Guia do usuário de cotas de serviço. Para solicitar o aumento da cota, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas.

Veja as cotas de serviço do Amazon EVS com a CLI AWS

Execute o comando a seguir para visualizar suas cotas do Amazon EVS.

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code evs \
```

```
    --output table
```

> **Note**
>
> A cota retornada é o número de ambientes ou hosts do Amazon EVS que podem ser criados nessa conta na região atual AWS .

Para trabalhar mais com cotas de serviço usando a AWS CLI, consulte service-quotas na AWS Referência de Comandos da CLI. Para solicitar um aumento de cota, consulte o request-service-quota-increasecomando na Referência de Comandos da AWS CLI.

Histórico de documentos do Amazon Elastic VMware Service User Guide

A tabela a seguir descreve os lançamentos da documentação do Amazon Elastic VMware Service.

Alteração	Descrição	Data
Amazon atualizada EVSServic e RolePolicy	O Amazon EVS atualizou a política gerenciada `AmazonEVSServiceRo lePolicy` para permitir que o serviço recupere as credenciais do vCenter do Secrets AWS Manager e decodifique segredos criptogra fados com chaves KMS gerenciadas pelo cliente.	23 de março de 2026
Amazon atualizada EVSServic e RolePolicy	O Amazon EVS atualizou a política gerenciada `AmazonEVSServiceRo lePolicy` para adicionar recursos abrangentes de gerenciamento de recursos, incluindo gerenciamento de instâncias EC2, operações de volume do EBS e integração com o AWS Secrets Manager. Para obter informações, consulte as atualizações do Amazon EVS para políticas AWS gerenciadas.	14 de agosto de 2025
Amazon atualizada EVSServic e RolePolicy	Atualizou a política AWS gerenciada da Amazon EVSServiceRolePolicy.	4 de agosto de 2025

Liberada a contagem de ambientes por cota de AWS conta	O Amazon EVS liberou a contagem de ambientes por cota de AWS conta. A contagem de ambientes por cota de AWS conta represent a o número máximo de ambientes Amazon EVS que podem ser criados em uma determinada conta e região.	8 de julho de 2025
Amazon EVS lançado na região da Europa (Irlanda)	O Amazon EVS foi lançado na região da Europa (Irlanda).	18 de junho de 2025
Lançou a Amazon EVSService RolePolicy	A política AWS gerenciad a da Amazon EVSService RolePolicy foi lançada.	9 de junho de 2025
Versão inicial do Guia do Usuário	O Guia do Usuário do Amazon Elastic VMware Service foi lançado. O Guia do usuário do Amazon EVS descreve todos os conceitos do Amazon EVS e fornece instruções sobre como usar os vários recursos com o console e a interface da linha de comando.	9 de junho de 2025

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.