Guía del usuario de

Amazon Elastic VMware Service

Amazon Elastic VMware Service: Guía del usuario de

Table of Contents

¿Qué es Amazon Elastic VMware Service?

Puede usar Amazon Elastic VMware Service (Amazon EVS) para implementar y ejecutar un entorno de VMware Cloud Foundation (VCF) directamente en EC2 instancias completas dentro de (Amazon Virtual Private Cloud VPC).

Temas

Características de Amazon EVS

Las siguientes son las principales características de Amazon EVS:

Simplifique y acelere su migración a AWS

Elimine las complicaciones de la migración y garantice la coherencia operativa con la portabilidad de las suscripciones y el despliegue automatizado de VMware Cloud Foundation (VCF) en la nube. Amplíe las redes locales y migre las cargas de trabajo sin tener que cambiar las direcciones IP, volver a capacitar al personal ni volver a escribir los manuales operativos.

Mantenga el control de su arquitectura en la nube VMware

Mantenga el control total de su VMware arquitectura y optimice un conjunto de virtualización que satisfaga las demandas únicas de sus aplicaciones, incluidos los complementos y las soluciones de terceros.

Administre usted mismo o aproveche a AWS los socios para disfrutar de una experiencia gestionada

Libere opciones y flexibilidad para autogestionarse o aproveche la experiencia de los AWS socios para gestionar y operar su entorno de VCF AWS a fin de cumplir sus objetivos empresariales en términos de talento, tiempo y costes.

Amplíe y proteja su empresa de las interrupciones

Mejore la escalabilidad en la nube más segura, escalable y resistente para migrar y operar sus VMware cargas de trabajo basadas en datos.

Aproveche AWS la innovación para transformar sus aplicaciones e infraestructura

Como servicio AWS nativo, Amazon EVS simplifica la ampliación y expansión de su VMware entorno con más de 200 servicios (incluidas bases de datos gestionadas, análisis, contenedores y sin servidor e IA generativa) para transformar su negocio.

Comience a utilizar Amazon EVS

Para crear su primer entorno Amazon EVS, consulteIntroducción. En general, empezar a utilizar Amazon EVS implica completar los siguientes pasos.

1. Completar los requisitos previos. Para obtener más información, consulte Configuración de Amazon Elastic VMware Service.
2. Cree un entorno Amazon EVS. Durante la creación del entorno, Amazon EVS crea las subredes de VLAN necesarias mediante los rangos de CIDR que especifique y añade hosts al entorno.
3. Personalice VCF. Configure su entorno en la interfaz de usuario de vSphere según sus necesidades. Esto puede incluir la configuración de inicios de sesión, políticas, supervisión y mucho más.
4. Conéctese y migre. Conecte su entorno a su centro de datos local y migre sus cargas de trabajo de VCF a Amazon EVS.

Acceso a Amazon EVS

Puede definir y configurar sus despliegues de Amazon EVS mediante las siguientes interfaces:

- Consola Amazon EVS: proporciona una interfaz web para crear entornos Amazon EVS.
- AWS CLI - Proporciona comandos para un amplio conjunto de sistemas Servicios de AWS y es compatible con Windows, macOS y Linux. Para obtener más información, consulte AWS Command Line Interface.
- AWS CloudFormation - Proporciona una especificación para cada tipo de recurso, por ejemplo`AWS::EVS::Environment`. Usted crea una plantilla utilizando la especificación del recurso y CloudFormation se encarga de aprovisionar y configurar los recursos por usted.

Conceptos y componentes de Amazon EVS

En esta sección se explican algunos conceptos y componentes clave de Amazon EVS.

Entorno de Amazon EVS

Un entorno Amazon EVS es un contenedor lógico para los recursos de VMware Cloud Foundation (VCF), como los hosts de vSphere, vSAN, NSX y SDDC Manager. Un entorno contiene un dominio de VCF consolidado con un clúster de vSphere que aloja los componentes para administrar, supervisar y crear una instancia de la pila de software de VCF. Cada entorno se asigna directamente a un dispositivo SDDC Manager. Para obtener más información, consulte the section called "Arquitectura".

Anfitrión de Amazon EVS

Un host Amazon EVS es un host VMware ESX que se ejecuta en instancias Amazon EC2 básicas. Los hosts de Amazon EVS utilizan volúmenes de almacenes de NVMe instancias locales para los almacenes de datos de vSAN, que almacenan las máquinas virtuales de administración y carga de trabajo.

> **Warning**
>
> Los volúmenes de los almacenes de instancias son efímeros. Los datos almacenados en estos volúmenes no se conservan si la instancia EC2 subyacente se detiene o finaliza. Detener o terminar Amazon EC2 las instancias utilizadas por Amazon EVS sin retirarlas dentro de VCF puede provocar la pérdida de datos.
> Para obtener más información sobre el mantenimiento del host, consulte. the section called "Mantenimiento del host"

Subred de acceso a servicios

La subred de acceso al servicio es una subred de VPC estándar que permite a Amazon EVS acceder a la implementación de VCF. Durante la creación del entorno de Amazon EVS, debe especificar la VPC y la subred que Amazon EVS utilizará para el acceso al servicio.

Al crear un entorno Amazon EVS, Amazon EVS aprovisiona interfaces de red elásticas en la subred de acceso al servicio para facilitar la conectividad de administración con los dispositivos VCF y los

hosts ESX. Esta conectividad es necesaria para que Amazon EVS pueda implementar, gestionar y supervisar la implementación de VCF.

Subred de VLAN de Amazon EVS

Una subred de VLAN de Amazon EVS es una subred de Amazon VPC gestionada por Amazon EVS. Las subredes de VLAN proporcionan conectividad de VPC para los hosts de Amazon EVS y los dispositivos VCF, como NSX, VMware VMware HCX y vCenter Server. VMware Cada subred de VLAN tiene una etiqueta de VLAN que permite segmentar de forma lógica el tráfico de la red de VLAN.

Amazon EVS crea todas las subredes de VLAN que el servicio utiliza cuando se crea el entorno de Amazon EVS. Usted proporciona las entradas del bloque CIDR que utilizan las subredes de VLAN. Debe asegurarse de que los bloques CIDR de la subred de la VLAN tengan el tamaño adecuado de acuerdo con la cantidad de hosts que se configurarán, teniendo en cuenta las necesidades de escalado futuras. Los bloques CIDR deben tener un tamaño mínimo de máscara de red /28 y un tamaño máximo de /24. Los bloques CIDR no deben superponerse con ningún bloque CIDR existente que esté asociado a la VPC.

Al crearlas, las subredes de VLAN se asocian implícitamente a la tabla de enrutamiento principal de la VPC. Tras la implementación, puede asociar de forma explícita las subredes de VLAN a una tabla de enrutamiento personalizada. Para obtener más información, consulte the section called “Consideraciones sobre las redes de Amazon EVS”.

> **Important**
>
> Las subredes VLAN de Amazon EVS solo se pueden crear durante la creación del entorno de Amazon EVS y no se pueden modificar una vez creado el entorno. Debe asegurarse de que los bloques CIDR de la subred de la VLAN tengan el tamaño adecuado antes de crear el entorno. No podrá agregar subredes de VLAN después de implementar el entorno.

> **Important**
>
> Las reglas de los grupos de seguridad de EC2 no se aplican en las interfaces de red elásticas de Amazon EVS que están conectadas a las subredes de VLAN. Para controlar el tráfico hacia y desde las subredes de VLAN, debe usar una lista de control de acceso a la red.

Subred VLAN de administración de hosts

La subred VLAN de administración de hosts separa el tráfico de administración del tráfico de usuarios y permite la administración remota de los hosts. La interfaz de red vmkernel de administración de hosts de EVS se conecta a esta subred.

Subred VLAN de VMotion

La subred VLAN de vMotion segmenta de forma lógica el tráfico de VMware vMotion y se utiliza durante un proceso de vMotion para mover máquinas virtuales entre hosts.

Subred de VLAN de vSAN

vSAN utiliza la subred VLAN de vSAN para separar el tráfico relacionado con las VMware operaciones de almacenamiento de vSAN del resto del tráfico de red.

Subred VLAN de VTEP

La subred VLAN de VTEP utiliza puntos de enlace de túnel virtual (VTEP) de VMware NSX para encapsular y desencapsular el tráfico de red superpuesto para los hosts ESX de Amazon EVS.

Subred VLAN VTEP de Edge

La subred VLAN VTEP de Edge es una subred VLAN VTEP especializada dedicada al tráfico superpuesto de los dispositivos NSX Edge. Esta VLAN se utiliza para la comunicación superpuesta entre NSX Edge y los hosts ESX.

Subred VLAN de VM de administración

La subred VLAN de máquinas virtuales de administración se utiliza para administrar dispositivos virtuales, incluidos NSX Manager, vCenter Server y SDDC Manager.

Subred VLAN de enlace ascendente HCX

La subred VLAN de enlace ascendente HCX se utiliza para la comunicación entre los dispositivos HCX Interconnect (HCX-IX) y HCX Network Extension (HCX-NE), y permite la creación del enlace ascendente en malla de servicios HCX.

Subred VLAN de enlace ascendente de NSX

La subred de VLAN de enlace superior de NSX se utiliza para conectar las redes superpuestas de NSX al resto de la VPC y a cualquier otra red externa que configure. La subred de VLAN de enlace superior de NSX está configurada en los enlaces superiores del nodo de NSX Edge.

Subred de VLAN de expansión

La subred VLAN de expansión se puede utilizar para habilitar funciones adicionales compatibles con VCF, como NSX Federation. Amazon EVS crea dos subredes de VLAN de expansión durante la creación del entorno.

VMware NSX

VMware NSX es una plataforma de redes definidas por software (SDN) que permite la virtualización de redes. Amazon EVS usa VMware NSX para crear y administrar la red superpuesta en la que se ejecutan los dispositivos y las cargas de trabajo de VMware Cloud Foundation (VCF). Amazon EVS implementa un par de nodos de Active/Standby NSX Edge, junto con una red superpuesta de NSX. Amazon EVS configura automáticamente todo el enrutamiento y los enlaces superiores de NSX en su nombre como parte de la implementación. Para obtener más información sobre los conceptos comunes de NSX, consulte los conceptos clave en la Guía de instalación de NSX. VMware

VMware Extensión de nube híbrida (HCX)

VMware Hybrid Cloud Extension (VMware HCX) es una plataforma de movilidad de aplicaciones diseñada para simplificar la migración de aplicaciones, reequilibrar las cargas de trabajo y optimizar la recuperación ante desastres en los centros de datos y las nubes. Puede usar HCX para migrar sus cargas de trabajo VMware basadas a Amazon EVS.

Puede configurar la conectividad para VMware HCX mediante Direct Connect una puerta de enlace de tránsito asociada o mediante una conexión AWS Site-to-Site VPN a una puerta de enlace de tránsito. Para obtener más información, consulte Migración.

Arquitectura de Amazon EVS

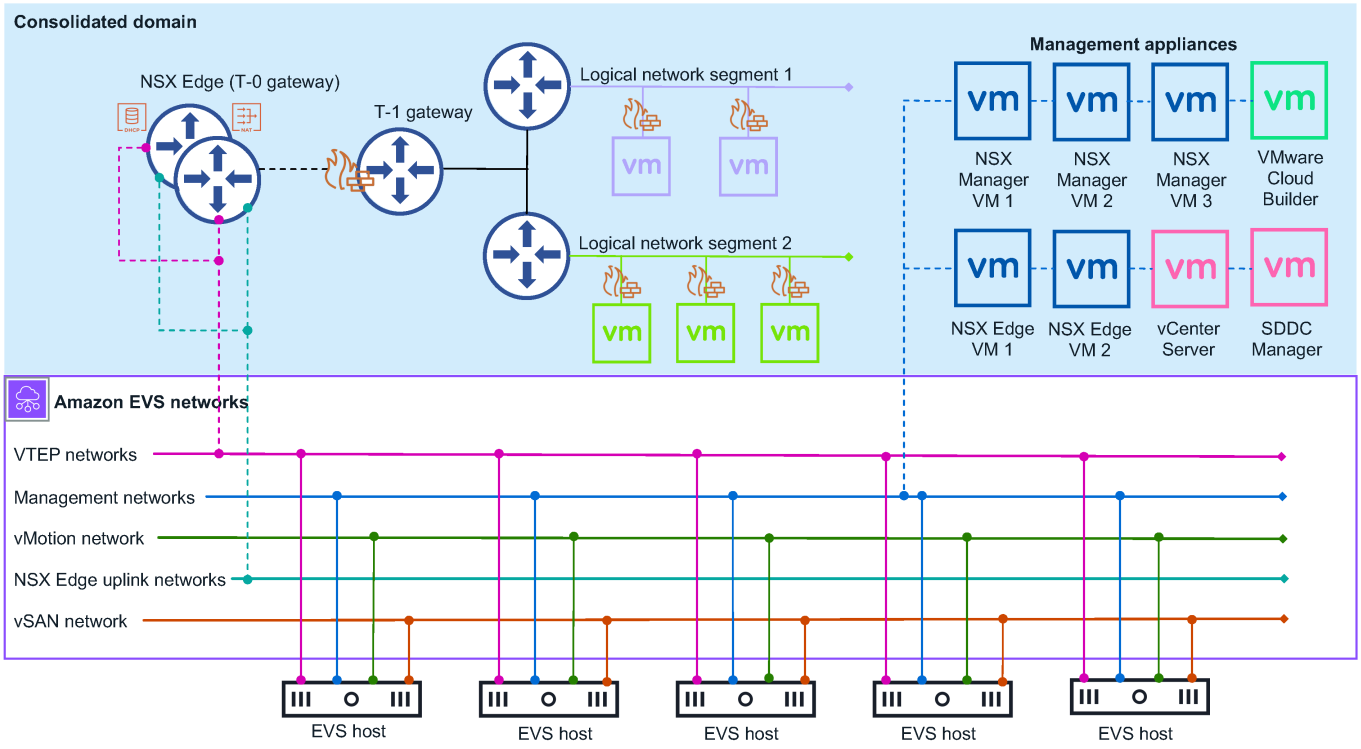
Amazon EVS implementa un modelo de arquitectura consolidada de VMware Cloud Foundation (VCF). En este modelo, los componentes de administración de VCF y las cargas de trabajo de los clientes se ejecutan juntos en un dominio consolidado. El entorno Amazon EVS se administra desde

un único vCenter Server con grupos de recursos de vSphere que proporcionan aislamiento entre las cargas de trabajo de administración y las de los clientes.

El dominio consolidado que implementa Amazon EVS contiene los siguientes componentes de administración de VCF:

- Hosts ESX
- Instancia de vCenter Server
- Administrador de SDDC
- Almacén de datos de vSAN
- Clúster de NSX Manager de tres nodos
- Clúster de vSphere
- Clúster de NSX Edge

El siguiente diagrama muestra un ejemplo de la arquitectura de Amazon EVS que se ha implementado en un entorno de Amazon EVS y muestra cómo están conectados los componentes del entorno. En el diagrama, el entorno de Amazon EVS con una arquitectura de dominio consolidada aparece sombreado en azul. La topología de la red Amazon EVS subyacente se ilustra dentro de la línea púrpura continua.



Topología de red

Un entorno Amazon EVS tiene dos capas de red de administración independientes:

Amazon VPC

Las subredes Amazon VPC y Amazon EVS VLAN que se crean en la VPC durante la creación del entorno forman la red subyacente para la implementación de VCF. Esta infraestructura proporciona conectividad para redes superpuestas de NSX, administración de hosts, vMotion y VSAN. El servidor de rutas Amazon VPC permite el enrutamiento dinámico entre la red subyacente y las redes superpuestas. Para obtener más información, consulte the section called “Conceptos y componentes”.

> **Note**
>
> Las subredes VLAN de Amazon EVS se utilizan únicamente para facilitar la comunicación subyacente de VCF. Las máquinas virtuales invitadas que ejecutan las cargas de trabajo de los clientes deben implementarse en las redes superpuestas de NSX. No se admite

el despliegue de máquinas virtuales invitadas en la red subyacente de subred VLAN de Amazon EVS.

VMware Red superpuesta de NSX

Amazon EVS configura una red superpuesta de NSX en su nombre como parte de la implementación. Puede configurar redes superpuestas de NSX adicionales para lograr el aislamiento de la red entre diferentes cargas de trabajo o aplicaciones dentro de su entorno de Amazon EVS. Para obtener más información, consulte Overlay Design for VMware Cloud Foundation en la documentación del VMware producto de Cloud Foundation.

> **Note**
>
> Amazon EVS solo admite una puerta de enlace de nivel 0 para un clúster de Active/Standby NSX Edge con dos nodos de NSX Edge. Esta puerta de enlace de nivel 0 se conecta a todas las redes superpuestas que configure para su uso con Amazon EVS y las anuncia.

Las dos capas de red están conectadas mediante un clúster de NSX Edge con dos nodos de Active/Standby NSX Edge. Los nodos de NSX Edge permiten la comunicación a través de la VPC entre las máquinas virtuales del mismo, así como VLANs la conectividad a Internet y la conectividad privada Direct Connect mediante AWS Site-to-Site una VPN con una puerta de enlace de tránsito.

Consideraciones sobre las redes de Amazon EVS

La red de administración requiere las siguientes configuraciones de recursos de red. Estas entradas se proporcionan durante la creación del entorno de Amazon EVS. Para obtener más información, consulte the section called “Conceptos y componentes”.

- Una Amazon VPC. Asegúrese de que el bloque IPv4 CIDR de VPC tenga el tamaño adecuado para adaptarse a la subred de VPC requerida y a las subredes de VLAN de Amazon EVS que Amazon EVS aprovisiona durante la creación del entorno. Para obtener más información, consulte the section called “Subred de VLAN de Amazon EVS”.

  > **Note**
  >
  > Amazon EVS no es compatible IPv6 en este momento.

- Una subred de acceso a servicios en su VPC. Amazon EVS utiliza esta subred para mantener una conexión persistente con el dispositivo SDDC Manager. Para obtener más información, consulte the section called “Subred de acceso a servicios”.

> **Note**
>
> Por el momento, Amazon EVS solo admite implementaciones Single-AZ. Todas las subredes de VPC que utiliza Amazon EVS deben estar en una única zona de disponibilidad en una región en la que el servicio esté disponible.

> **Note**
>
> Todas las subredes de VPC requieren tablas de enrutamiento asociadas que estén configuradas de acuerdo con los requisitos de red de la organización.

- Una dirección IP del servidor DNS principal y una dirección IP del servidor DNS secundario en el conjunto de opciones de DHCP de la VPC para resolver las direcciones IP del host. Amazon EVS también requiere que cree una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR para cada dispositivo de administración de VCF y host de Amazon EVS de su implementación. Para obtener más información, consulte the section called “Configure los servidores DNS”.
- El CIDR de la subred VLAN de Amazon EVS bloquea cada subred de VLAN que Amazon EVS le aprovisiona durante la creación del entorno. Los bloques CIDR deben tener un tamaño mínimo de máscara de red de /28 y un tamaño máximo de /24. Los bloques CIDR no deben superponerse.
- Una instancia de Amazon VPC Route Server con la propagación de Route Server habilitada.
- Dos puntos finales de Route Server en la subred de acceso al servicio.
- Dos pares de Route Server que unen los nodos de NSX Edge que Amazon EVS aprovisiona con los puntos de enlace de Route Server.

Puerta de enlace de nivel 0

La puerta de enlace de nivel 0 gestiona todo el tráfico norte-sur entre las redes lógicas y físicas y se crea en la red superpuesta de NSX. Esta puerta de enlace de nivel 0 se crea como parte de la implementación de Amazon EVS.

> **Note**
>
> Amazon EVS solo admite una puerta de enlace de nivel 0 para un clúster de Active/Standby NSX Edge con dos nodos de NSX Edge.

Puerta de enlace de nivel 1

La puerta de enlace de nivel 1 gestiona el tráfico de este a oeste entre los segmentos de red enrutados dentro de un entorno y se crea en la red superpuesta de NSX. La puerta de enlace de nivel 1 tiene conexiones de enlace descendente a los segmentos y conexiones de enlace de enlace ascendente a la puerta de enlace de nivel 0. Puede crear y configurar puertas de enlace de nivel 1 adicionales si las necesita.

Clúster de NSX Edge

Amazon EVS usa la interfaz de NSX Manager para implementar un clúster de NSX Edge con dos nodos de NSX Edge que se ejecutan en modo. Active/Standby Este clúster de NSX Edge proporciona la plataforma en la que se ejecutan las puertas de enlace de nivel 0 y nivel 1, junto con las conexiones VPN y su maquinaria de enrutamiento BGP. IPsec

Recursos de Amazon EVS

Amazon EVS aprovisiona los siguientes AWS recursos durante la creación del entorno. Estos recursos aparecen en la VPC a la que permite el acceso de Amazon EVS y están visibles en el momento de su creación Consola de administración de AWS y AWS CLI después de crearlos.

> **Important**
>
> La modificación de estos recursos fuera de la consola y la API de Amazon EVS podría afectar a la disponibilidad y estabilidad del entorno de Amazon EVS.

- Interfaces de red elásticas de Amazon EVS que permiten la conectividad con sus dispositivos y hosts VCF.
- Hosts ESX de Amazon EVS que se ejecutan en Amazon EC2 instancias básicas. Para obtener más información, consulte the section called “Anfitrión de Amazon EVS”.

> **Important**
>
> Su entorno Amazon EVS debe tener un mínimo de 4 hosts y no más de 16 hosts. Amazon EVS solo admite entornos con 4 a 16 hosts.

- Subredes VLAN de Amazon EVS que conectan la VPC a los dispositivos VCF. Para obtener más información, consulte the section called “Subred de VLAN de Amazon EVS”.

Configuración de Amazon Elastic VMware Service

Para usar Amazon EVS, necesitará configurar otros AWS servicios, así como configurar su entorno para cumplir con los requisitos de VMware Cloud Foundation (VCF). Para obtener una lista resumida de los requisitos previos de implementación, consulte. the section called “Lista de verificación de implementación”

Temas

Inscríbase en AWS

Si no tienes una Cuenta de AWS, sigue estos pasos para crearla.

1. Abre el https://portal.aws.amazon.com/billing/ registro.

2. Siga las instrucciones que se le indiquen.

Creación de un usuario de IAM

1. Inicie sesión en la consola de IAM como propietario de la cuenta; para ello, seleccione el usuario raíz e introduzca la dirección de correo electrónico de su AWS cuenta. En la siguiente página, escriba su contraseña.

   > **Note**
   >
   > Le recomendamos que siga la práctica recomendada de utilizar el usuario de IAM `Administrator` como se indica a continuación y guardar de forma segura las credenciales de usuario raíz. Inicie sesión como usuario raíz únicamente para realizar algunas tareas de administración de servicios y de cuentas.

2. En el panel de navegación, selecciona Usuarios y, a continuación, selecciona Crear usuario.
3. En Nombre de usuario, escriba `Administrator`.
4. Seleccione la casilla de verificación situada junto al acceso a AWS la consola de administración. A continuación, seleccione Custom password (Contraseña personalizada) y luego escriba la nueva contraseña en el cuadro de texto.
5. (Opcional) De forma predeterminada, AWS requiere que el nuevo usuario cree una contraseña nueva al iniciar sesión por primera vez. Puede quitar la marca de selección de la casilla de verificación situada junto a User must create a new password at next sign-in (El usuario debe crear una nueva contraseña en el siguiente inicio de sesión) para permitir al nuevo usuario restablecer su contraseña después de iniciar sesión.
6. Elija Next: Permissions.
7. En Set permissions (Establecer permisos), elija Add user to group (Añadir usuario a grupo).
8. Elija Create group (Crear grupo).
9. En el cuadro de diálogo Create group (Crear grupo), en Group name (Nombre del grupo) escriba `Administrators`.
10. Elija Filtrar políticas y, a continuación, seleccione la función AWS managed -job para filtrar el contenido de la tabla.
11. En la lista de políticas, active la casilla de verificación correspondiente AdministratorAccess. A continuación, elija Create group (Crear grupo).

> **Note**
>
> Debe activar el acceso de usuario y rol de IAM a Billing antes de poder usar `AdministratorAccess` los permisos para acceder a la consola de AWS Billing and Cost Management. Para ello, siga las instrucciones que se indican en el paso 1 del tutorial sobre cómo delegar el acceso a la consola de facturación.

12. Retroceda a la lista de grupos y active la casilla de verificación del nuevo grupo. Elija Refresh si es necesario para ver el grupo en la lista.
13. Elija Next: Tags (Siguiente: Etiquetas).
14. (Opcional) Añadir metadatos al rol asociando las etiquetas como pares de clave-valor. Para obtener más información sobre la utilización de etiquetas en IAM, consulte Etiquetado de entidades de IAM en la Guía del usuario de IAM.
15. Elija Next: Review (Siguiente: Revisión) para ver la lista de suscripciones a grupos que se van a añadir al nuevo usuario. Cuando esté listo para continuar, elija Create user (Crear usuario).

Puede utilizar este mismo proceso para crear más grupos y usuarios y dar a sus usuarios acceso a los recursos de su AWS cuenta. Para obtener información sobre el uso de políticas que restringen los permisos de los usuarios a AWS recursos específicos, consulte Administración de acceso y ejemplos de políticas.

Cree un rol de IAM para delegar el permiso de Amazon EVS a un usuario de IAM

Puede usar roles para delegar el acceso a sus recursos. AWS Con las funciones de IAM, puede establecer relaciones de confianza entre su cuenta de confianza y otras cuentas de AWS confianza. La cuenta de confianza es propietaria del recurso al que se va a acceder y la cuenta de confianza contiene los usuarios que necesitan acceder al recurso.

Tras crear la relación de confianza, un usuario de IAM o una aplicación de la cuenta de confianza pueden utilizar la operación de la `AssumeRole` API AWS Security Token Service (AWS STS). Esta operación proporciona credenciales de seguridad temporales que permiten el acceso a AWS los recursos de su cuenta. Para obtener más información, consulte Crear un rol para delegar permisos a un usuario de IAM en la Guía del AWS Identity and Access Management usuario.

Siga estos pasos para crear un rol de IAM con una política de permisos que permita el acceso a las operaciones de Amazon EVS.

> **Note**
>
> Amazon EVS no admite el uso de un perfil de instancia para transferir una función de IAM a una EC2 instancia.

Example

IAM console

1. Ve a la consola de IAM.
2. En el menú de la izquierda, selecciona Políticas.
3. Elija Crear política.
4. En el editor de políticas, cree una política de permisos que habilite las operaciones de Amazon EVS. Para ver una política de ejemplo, consulte the section called “Cree y gestione un entorno Amazon EVS”. Para ver todas las acciones, recursos y claves de condición de Amazon EVS disponibles, consulte Acciones en la referencia de autorización de servicio.
5. Elija Siguiente.
6. En Nombre de la política, introduzca un nombre de política significativo para identificar esta política.
7. Revise los permisos definidos en esta política.
8. (Opcional) Agregue etiquetas para ayudar a identificar, organizar o buscar este recurso.
9. Elija Crear política.
10. En el menú de la izquierda, selecciona Funciones.
11. Elija Crear rol.
12. En Tipo de entidad de confianza, elija Cuenta de AWS.
13. En An Cuenta de AWS , especifique la cuenta en la que desea realizar las acciones de Amazon EVS y seleccione Siguiente.
14. En la página Añadir permisos, seleccione la política de permisos que creó anteriormente y pulse Siguiente.
15. En Nombre del rol, introduzca un nombre significativo para identificar este rol.

16. Revise la política de confianza y asegúrese de que Cuenta de AWS la correcta aparezca como principal.
17. (Opcional) Agregue etiquetas para ayudar a identificar, organizar o buscar este recurso.
18. Elija Crear rol.

AWS CLI

1. Copie el siguiente contenido en un archivo JSON de política de confianza. Para el ARN principal, sustituya el ID y el nombre del ejemplo por su propio Cuenta de AWS Cuenta de AWS ID y `service-user` nombre de usuario de IAM.

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

2. Creación del rol. `evs-environment-role-trust-policy.json`Sustitúyalo por el nombre del archivo de la política de confianza.

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

3. Cree una política de permisos que permita las operaciones de Amazon EVS y asocie la política al rol. Reemplace `myAmazonEVSEnvironmentRole` por el nombre de su rol. Para ver una política de ejemplo, consulte the section called “Cree y gestione un entorno Amazon EVS”. Para ver todas las acciones, recursos y claves de condición de Amazon EVS disponibles, consulte Acciones en la referencia de autorización de servicio.

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

```
  --role-name myAmazonEVSEnvironmentRole
```

Inscríbase en un AWS plan Business, AWS Enterprise On-Ramp o AWS Enterprise Support

Amazon EVS requiere que los clientes estén inscritos en un plan AWS Business, AWS Enterprise On-Ramp o Enterprise AWS Support para recibir acceso continuo al soporte técnico y a la orientación arquitectónica. AWS Business Support es el nivel de AWS soporte mínimo que cumple con los requisitos de Amazon EVS. Si tiene cargas de trabajo críticas para la empresa, le recomendamos que se inscriba en los planes Enterprise On-Ramp o AWS AWS Enterprise Support. Para obtener más información, consulte Compare AWS Support Plans.

Important

Se produce un error en la creación del entorno de Amazon EVS si no se suscribe a un plan AWS Business, AWS Enterprise On-Ramp o Enterprise AWS Support.

Comprobación de las cuotas de

Para habilitar la creación del entorno Amazon EVS, asegúrese de que su cuenta tenga las cuotas mínimas requeridas a nivel de cuenta. Para obtener más información, consulte Cuotas de servicio.

Important

Se produce un error en la creación del entorno de Amazon EVS si el valor de la cuota de recuento de hosts por entorno de EVS no es de al menos 4.

Planifique los tamaños de CIDR de VPC

Al crear un entorno de Amazon EVS, debe especificar un bloque CIDR de VPC. El bloque CIDR de la VPC no se puede cambiar una vez creado el entorno y necesitará tener suficiente espacio reservado para alojar las subredes y los hosts de EVS necesarios que Amazon EVS cree durante la implementación del entorno. Como resultado, es fundamental planificar cuidadosamente el tamaño del bloque de CIDR, teniendo en cuenta los requisitos de Amazon EVS y sus futuras necesidades de

escalado antes de la implementación. Amazon EVS requiere un bloque CIDR de VPC con un tamaño mínimo de /22 de máscara de red para dejar espacio suficiente para las subredes y los hosts de EVS necesarios. Para obtener más información, consulte the section called “Consideraciones sobre las redes de Amazon EVS”.

> **Important**
>
> Asegúrese de tener suficiente espacio de direcciones IP para la subred de VPC y las subredes de VLAN que Amazon EVS crea para los dispositivos VCF. El bloque CIDR de la VPC debe tener un tamaño mínimo de /22 para permitir suficiente espacio para las subredes y los hosts de EVS necesarios.

> **Note**
>
> Amazon EVS no es compatible IPv6 en este momento.

Crear una VPC con subredes

Amazon EVS implementa su entorno en una VPC que usted proporciona. Esta VPC debe contener una subred para el acceso al servicio Amazon EVS (). the section called “Subred de acceso a servicios” Para ver los pasos para crear una VPC con subredes para Amazon EVS, consulte. the section called “Cree una VPC con subredes y tablas de enrutamiento”

Configurar la tabla de enrutamiento principal de la VPC

Las subredes VLAN de Amazon EVS están asociadas implícitamente a la tabla de enrutamiento principal de la VPC. Para habilitar la conectividad con los servicios dependientes, como el DNS o los sistemas locales, para una implementación correcta del entorno, debe configurar la tabla de enrutamiento principal para permitir el tráfico a estos sistemas. Para obtener más información, consulte the section called “Asocie de forma explícita las subredes VLAN de Amazon EVS a una tabla de enrutamiento de VPC”.

> **Important**
>
> Amazon EVS admite el uso de una tabla de enrutamiento personalizada solo después de crear el entorno de Amazon EVS. No se deben utilizar tablas de enrutamiento personalizadas

durante la creación del entorno de Amazon EVS, ya que esto puede provocar problemas de conectividad.

Requisitos de ruta de puerta de enlace

Configure las rutas para estos tipos de puerta de enlace en función de sus requisitos de conectividad:

- Puerta de enlace NAT (NGW)
  - Opcional para el acceso a Internet solo de salida.
  - Debe estar en una subred pública con acceso a una pasarela de Internet.
  - Agregue rutas desde subredes privadas y subredes VLAN de EVS a la puerta de enlace NAT.
  - Para obtener más información, consulte Trabajar con puertas de enlace NAT en la Guía del usuario de Amazon VPC.
- Pasarela de tránsito (TGW)
  - Necesario para la conectividad local a través de AWS Direct Connect y AWS Site-to-Site VPN.
  - Agregue rutas para los rangos de redes locales.
  - Configure la propagación de rutas si utiliza BGP.
  - Para obtener más información, consulte Pasarelas de tránsito en Amazon VPC Transit Gateways en la Guía del usuario de Amazon VPC.

Prácticas recomendadas

- Documente todas las configuraciones de la tabla de rutas.
- Utilice convenciones de nomenclatura coherentes.
- Audite periódicamente sus tablas de rutas.
- Pruebe la conectividad después de realizar cambios.
- Realice una copia de seguridad de las configuraciones de la tabla de rutas
- Supervise el estado y la propagación de las rutas.

Para obtener más información sobre cómo trabajar con tablas de enrutamiento, consulte Configurar tablas de enrutamiento en la Guía del usuario de Amazon VPC.

Configure el conjunto de opciones de DHCP de su VPC

Important

La implementación de su entorno falla si no cumple estos requisitos de Amazon EVS:

- Incluya una dirección IP del servidor DNS principal y una dirección IP del servidor DNS secundario en el conjunto de opciones de DHCP.
- Incluya una zona de búsqueda directa de DNS con registros A para cada dispositivo de administración de VCF y host de Amazon EVS de su implementación.
- Incluya una zona de búsqueda inversa de DNS con registros PTR para cada dispositivo de administración de VCF y host de Amazon EVS de su implementación.
- Configure la tabla de rutas principal de la VPC para garantizar que exista una ruta a sus servidores DNS.
- Asegúrese de que el registro del nombre de dominio sea válido y no haya caducado, y de que no existan nombres de host o direcciones IP duplicados.
- Configure sus grupos de seguridad y listas de control de acceso a la red (ACLs) para permitir que Amazon EVS se comunique con:
  - Servidores DNS a través TCP/UDP del puerto 53.
  - Subred VLAN de administración de hosts a través de HTTPS y SSH.
  - Subred de VLAN de administración a través de HTTPS y SSH.

Para obtener más información, consulte the section called “Configuración de los servidores DNS y NTP mediante el conjunto de opciones de DHCP de la VPC”.

Crear y configurar la infraestructura de VPC Route Server

Amazon EVS utiliza Amazon VPC Route Server para habilitar el enrutamiento dinámico basado en BGP a su red subyacente de VPC. Debe especificar un servidor de rutas que comparta rutas con al menos dos puntos finales del servidor de rutas en la subred de acceso al servicio. El ASN del par configurado en los pares del servidor de rutas debe coincidir y las direcciones IP del par deben ser únicas.

Important

La implementación de su entorno falla si no cumple estos requisitos de Amazon EVS para la configuración del servidor de rutas de VPC:

- Debe configurar al menos dos puntos finales del servidor de rutas en la subred de acceso al servicio.
- Al configurar el Border Gateway Protocol (BGP) para la puerta de enlace de nivel 0, el valor de ASN del mismo nivel del servidor de rutas de la VPC debe coincidir con el valor del ASN del mismo nivel de NSX Edge.
- Al crear los dos servidores de rutas homólogos, debe utilizar una dirección IP única de la VLAN de enlace superior de NSX para cada punto final. Estas dos direcciones IP se asignarán a los bordes de NSX durante la implementación del entorno Amazon EVS.
- Al habilitar la propagación del servidor de rutas, debe asegurarse de que todas las tablas de rutas que se propaguen tengan al menos una asociación de subred explícita. El anuncio de rutas BGP falla si las tablas de rutas propagadas no tienen una asociación de subred explícita.

Note

Para la detección de actividad entre pares de Route Server, Amazon EVS solo admite el mecanismo BGP keepalive predeterminado. Amazon EVS no admite la detección de reenvío bidireccional (BFD) de varios saltos.

Requisitos previos

Antes de comenzar, necesitará:

- Una subred de VPC para su servidor de rutas.
- Permisos de IAM para administrar los recursos del servidor de rutas de VPC.
- Un valor ASN de BGP para el servidor de rutas (ASN del lado de Amazon). El valor debe estar en el rango de 1 a 4294967295.

- Un ASN homólogo para emparejar el servidor de rutas con la puerta de enlace NSX de nivel 0. Los valores de ASN del mismo nivel introducidos en el servidor de rutas y en la puerta de enlace NSX de nivel 0 deben coincidir. El ASN predeterminado de un dispositivo NSX Edge es 65000.

Steps

Para ver los pasos para configurar el servidor de rutas de VPC, consulte el tutorial de introducción a Route Server.

> **Note**
>
> Si utiliza una puerta de enlace NAT o una puerta de enlace de tránsito, asegúrese de que el servidor de rutas esté configurado correctamente para propagar las rutas de NSX a las tablas de rutas de la VPC.

> **Note**
>
> Le recomendamos que habilite las rutas persistentes para la instancia del servidor de rutas con una duración de persistencia de entre 1 y 5 minutos. Si está habilitada, las rutas se conservarán en la base de datos de enrutamiento del servidor de rutas incluso si finalizan todas las sesiones de BGP.

> **Note**
>
> El estado de conectividad de BGP estará inactivo hasta que el entorno Amazon EVS esté implementado y operativo.

Cree una puerta de enlace de tránsito para la conectividad local

Puede configurar la conectividad de su centro de datos local Direct Connect con su AWS infraestructura mediante una puerta de enlace de tránsito asociada o mediante un accesorio de AWS Site-to-Site VPN a una puerta de enlace de tránsito. Para obtener más información, consulte the section called “Configurar la conectividad de red local (opcional)”.

Crear una reserva de EC2 capacidad en Amazon

Amazon EVS lanza instancias Amazon EC2 i4i.metal que representan los hosts ESX de su entorno Amazon EVS. Para asegurarse de que dispone de suficiente capacidad de instancias i4i.metal cuando la necesite, le recomendamos que solicite una reserva de capacidad de Amazon EC2 . Puede crear una reserva de capacidad en cualquier momento y decidir cuándo debe iniciarse. Puede solicitar una reserva de capacidad para su uso inmediato o puede solicitar una reserva de capacidad para una fecha futura. Para obtener más información, consulte Reserva de capacidad informática con reservas de capacidad EC2 bajo demanda en la Guía del usuario de Amazon Elastic Compute Cloud.

Configure el AWS CLI

AWS CLI Es una herramienta de línea de comandos con la que trabajar Servicios de AWS, incluida Amazon EVS. También se utiliza para autenticar a los usuarios o roles de IAM para acceder al entorno de virtualización de Amazon EVS y a otros AWS recursos desde su máquina local. Para aprovisionar AWS recursos desde la línea de comandos, debe obtener un identificador de clave de AWS acceso y una clave secreta para utilizarlos en la línea de comandos. A continuación, debe configurar estas credenciales en la AWS CLI. Para obtener más información, consulte Configuración AWS CLI en la Guía del AWS Command Line Interface usuario de la versión 2.

Crear un Amazon EC2 key pair

Amazon EVS utiliza un Amazon EC2 key pair que usted proporciona durante la creación del entorno para conectarse a sus hosts. Para crear un par de claves, sigue los pasos que se indican en Crear un par de claves para tu Amazon EC2 instancia en la Guía del Amazon Elastic Compute Cloud usuario.

Prepara tu entorno para VMware Cloud Foundation (VCF)

Antes de implementar su entorno Amazon EVS, este debe cumplir con los requisitos de infraestructura de VMware Cloud Foundation (VCF). Para ver los requisitos previos detallados del VCF, consulte el libro de trabajo de planificación y preparación en la documentación del VMware producto de Cloud Foundation.

También debes familiarizarte con los requisitos de VCF 5.2.x. Consulte las notas de la versión 5.2.x de VCF para obtener información relevante sobre la versión.

> **Note**
>
> Para obtener información sobre las versiones de VCF proporcionadas por Amazon EVS, consulte. the section called “Versiones e instancias de VCF EC2 ”

Adquisición de las claves de licencia de VCF

Para utilizar Amazon EVS, debe proporcionar una clave de solución de VCF y una clave de licencia de vSAN. La clave de la solución VCF debe tener al menos 256 núcleos. La clave de licencia de vSAN debe tener al menos 110 TiB de capacidad de vSAN. Para obtener más información sobre las licencias de VCF, consulte Administrar las claves de licencia en VMware Cloud Foundation en la Guía de administración de VMware Cloud Foundation.

> **Important**
>
> Utilice la interfaz de usuario de SDDC Manager para gestionar la solución VCF y las claves de licencia de vSAN. Amazon EVS requiere que mantenga claves de licencia de vSAN y de solución VCF válidas en SDDC Manager para que el servicio funcione correctamente.

> **Note**
>
> Su licencia VCF estará disponible para Amazon EVS en todas AWS las regiones para garantizar el cumplimiento de la licencia. Amazon EVS no valida las claves de licencia. Para validar las claves de licencia, visite el soporte de Broadcom.

VMware Requisitos previos de HCX

Puede usar VMware HCX para migrar sus cargas de trabajo VMware basadas existentes a Amazon EVS. Antes de usar VMware HCX con Amazon EVS, asegúrese de haber completado las siguientes tareas previas.

> **Note**
>
> VMware HCX no está instalado en el entorno EVS de forma predeterminada.

- Antes de poder utilizar VMware HCX con Amazon EVS, se deben cumplir los requisitos mínimos de base de red. Para obtener más información, consulte los requisitos mínimos de red subyacente en la Guía del VMware usuario de HCX.
- Confirme que VMware NSX esté instalado y configurado en el entorno. Para obtener más información, consulte la Guía de instalación de VMware NSX.
- Asegúrese de que el VMware HCX esté activado e instalado en el entorno. Para obtener más información sobre la activación e instalación de VMware HCX, consulte Introducción a VMware HCX en la Guía de introducción a HCX. VMware
- Si necesita conectividad a Internet con el HCX, debe completar los siguientes requisitos previos:
  - Asegúrese de que su cuota de IPAM para la longitud de la máscara de red de bloques IPv4 CIDR públicos contiguos proporcionada por Amazon sea de /28 o superior.

    > **Important**
    >
    > Para la conectividad a Internet HCX, Amazon EVS requiere el uso del bloque IPv4 CIDR de un grupo de IPAM público con una longitud de máscara de red igual o superior a /28. El uso de cualquier bloque CIDR con una longitud de máscara de red inferior a /28 provocará problemas de conectividad del HCX. Para obtener más información sobre cómo aumentar las cuotas de IPAM, consulte Cuotas de su IPAM.

  - Cree un IPAM y un grupo de IPv4 IPAM público con un CIDR que tenga una longitud mínima de máscara de red de /28.
  - Asigne al menos dos direcciones IP elásticas (EIPs) del grupo de IPAM para los dispositivos HCX Manager y HCX Interconnect (HCX-IX). Asigne una dirección IP elástica adicional para cada dispositivo de red HCX que necesite implementar.
  - Añada el bloque IPv4 CIDR público como CIDR adicional a su VPC.

Para obtener más información sobre la configuración de HCX, consulte y. the section called “Elija su opción de conectividad HCX” the section called “Opciones de conectividad HCX”

Lista de verificación de requisitos previos para el despliegue de Amazon EVS

Esta sección contiene una lista de requisitos previos que deben cumplirse para permitir una implementación correcta del entorno Amazon EVS.

Información clave de licencia de VCF

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
ID del sitio	ID de sitio proporcionado por Broadcom para acceder al portal de soporte de Broadcom.	Debe proporcionar un identificador de sitio de Broadcom en la solicitud de creación del entorno EVS.	01234567
Clave de solución de VCF	Una clave de licencia de VCF única que desbloquea las funciones de todo el paquete de VCF, incluidas vSphere, NSX, SDDC Manager y vCenter Server.	Debe proporcionar una clave de solución VCF activa y válida en la solicitud de creación del entorno EVS. La clave no puede estar ya en uso en un entorno EVS existente.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ
Clave de licencia de vSAN	Una clave de licencia de vSAN le permite activar y utilizar el software vSAN en un entorno VCF.	Debe proporcionar una clave de licencia de vSAN activa y válida en la solicitud de creación del entorno EVS. La clave no puede estar ya en uso en un entorno de EVS existente.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

AWS información sobre la cuenta y la región

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de valores
AWS número de ID de cuenta	La AWS cuenta le permite crear y	Debe tener acceso a una AWS cuenta.	139.9999

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de valores
	administrar AWS recursos y acceder a AWS los servicios.		
AWS Región	Un área geográfica física donde se AWS mantienen varios centros de datos aislados denominados zonas de disponibilidad.	Debe especificar una AWS región en la que se vaya a realizar el despliegue de Amazon EVS. Para obtener una lista de las regiones en las que Amazon EVS está disponible actualmente, consulte los puntos de enlace y las cuotas de Amazon Elastic VMware Service en la Guía de referencia AWS general.	Oeste de EE. UU. (Oregón)

AWS Transit Gateway para conectividad de centros de datos locales

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
ID de puerta de enlace de tránsito	Una puerta de enlace de tránsito actúa como un enrutador virtual regional para el tráfico que fluye entre la VPC y las redes locales.	Debe usar una pasarela de tránsito para conectar un entorno de Amazon EVS a sus redes locales.	Ejemplo del TGW-0262A0E521

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
Método de conexión	Para conectar sus redes locales a un entorno de Amazon EVS, debe utilizar una puerta de enlace de tránsito con Direct AWS Connect o AWS Site-to-Site VPN.	Determine si usará AWS Direct Connect, AWS Site-to-Site VPN o una combinación de ambas. Para obtener más información sobre el uso de Site-to-Site una VPN con Direct Connect, consulte AWS Site-to-Site VPN con IP privada con AWS Direct Connect.	AWS Site-to-Site VPN con AWS Direct Connect

VPC para el entorno Amazon EVS

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor
ID de VPC	Una VPC es una red virtual que se parece mucho a una red tradicional que operaría en su propio centro de datos.	Se puede usar cualquier Amazon VPC para la implementación del entorno.	vpc-0abcdef1234567890
Bloque CIDR de VPC	En Amazon VPC, un bloque CIDR define el rango de direcciones IP disponibles en la VPC.	Un bloque CIDR según la norma RFC 1918 con un tamaño mínimo de /22 de máscara de red. El bloque CIDR de la VPC debe tener el tamaño adecuado	10.1.0.0/20

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor
		para adaptarse a todas las subredes y hosts de EVS que se van a implementar en la VPC. Este bloque CIDR debe ser único en todos sus entornos.	

Subredes de VPC para entorno EVS

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
ID de subred de acceso al servicio	Una subred de acceso a servicios es una subred de VPC estándar que permite el acceso a los servicios de Amazon EVS. Para obtener más información, consulte the section called “Subred de acceso a servicios”.	Se puede usar cualquier subred de VPC, siempre que la subred tenga el tamaño adecuado dentro de la VPC. Sugerimos especificar un bloque CIDR de subred de VPC con una máscara de red de /24.	subnet-abcdef1234567890e
subred de acceso al servicio (CIDR)	un bloque CIDR de subred de VPC es un rango de direcciones IP, definido mediante la notación CIDR, que se asigna a una	La subred de acceso al servicio debe tener el tamaño adecuado para dar cabida también a las demás subredes y hosts de EVS que se van	10.1.0.0/24

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
	subred específica dentro de una VPC.	a implementar en la VPC. Sugerimos especificar un bloque CIDR de subred de VPC con una máscara de red de /24.	
AWS ID de zona de disponibilidad dentro de la región	Una ubicación distinta dentro de una AWS región, diseñada para aislarse de los fallos en otras AZs, y que consta de uno o más centros de datos.	Puede especificar la zona de disponibilidad en la que se implementan las subredes de VPC durante la creación de la subred. Para obtener más información, consulte Crear una subred en la Guía del usuario de Amazon VPC.	us-west-2a

Subredes VLAN de EVS para el entorno de EVS

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor
VLAN CIDR de administración de hosts	El bloque CIDR para la subred de VLAN de administración del host. Para obtener más información, consulte the section called “Subred VLAN	Debe tener un tamaño mínimo de máscara de red de /28 y un tamaño máximo de /24. No debe superponerse con ningún bloque CIDR	10.1.1.0/24

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor
	de administración de hosts".	existente que esté asociado a la VPC.	
CIDR de VLAN de vMotion	El bloque CIDR de la subred VLAN de vMotion. Para obtener más información, consulte the section called "Subred VLAN de VMotion".	Debe tener el mismo tamaño que la VLAN de administración del host.	10.1.2.0/24
CIDR de VLAN de vSAN	El bloque CIDR de la subred de VLAN de vSAN. Para obtener más información, consulte the section called "Subred de VLAN de vSAN".	Debe tener el mismo tamaño que la VLAN de administración del host.	10.1.3.0/24
VTEP VLAN CIDR	El bloque CIDR para la subred VLAN de VTEP. Para obtener más información, consulte the section called "Subred VLAN de VTEP".	Debe tener el mismo tamaño que la VLAN de administración del host.	10.1.4.0/24

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor
VLAN VTEP de Edge (CIDR)	El bloque CIDR para la subred VLAN VTEP perimetral. Para obtener más información, consulte the section called “Subred VLAN VTEP de Edge”.	Debe tener un tamaño mínimo de máscara de red de /28 y un tamaño máximo de /24. No debe superponerse con ningún bloque CIDR existente que esté asociado a la VPC.	10.1.5.0/24
VM de administración, VLAN, CIDR	El bloque CIDR para la subred VLAN de la máquina virtual de administración. Para obtener más información, consulte the section called “Subred VLAN de VM de administración”.	Debe tener un tamaño mínimo de máscara de red de /28 y un tamaño máximo de /24. No debe superponerse con ningún bloque CIDR existente que esté asociado a la VPC.	10.1.6.0/24
CIDR de VLAN de enlace ascendente HCX	El bloque CIDR de la subred VLAN de enlace ascendente HCX. Para obtener más información, consulte the section called “Subred VLAN de enlace ascendente HCX”.	Debe tener un tamaño mínimo de máscara de red de /28 y un tamaño máximo de /24. No debe superponerse con ningún bloque CIDR existente que esté asociado a la VPC.	10.1.7.0/24

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor
CIDR de VLAN de enlace superior de NSX	El bloque CIDR de la subred de VLAN de enlace superior de NSX. Para obtener más información, consulte the section called “Subred VLAN de enlace ascendente de NSX”.	Debe tener un tamaño mínimo de máscara de red de /28 y un tamaño máximo de /24. No debe superponerse con ningún bloque CIDR existente que esté asociado a la VPC.	10.1.8.0/24
Expansión VLAN 1 CIDR	Bloque CIDR para la subred de la VLAN de expansión . Para obtener más información, consulte the section called “Subred de VLAN de expansión”.	Debe tener un tamaño mínimo de máscara de red de /28 y un tamaño máximo de /24. No debe superponerse con ningún bloque CIDR existente que esté asociado a la VPC.	10.1.9.0/24
Expansión VLAN 2 CIDR	Bloque CIDR para la subred de la VLAN de expansión . Para obtener más información, consulte the section called “Subred de VLAN de expansión”.	Debe tener un tamaño mínimo de máscara de red de /28 y un tamaño máximo de /24. No debe superponerse con ningún bloque CIDR existente que esté asociado a la VPC.	10.1.10.0/24

Infraestructura DNS y NTP

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
Dirección IP del servidor DNS principal	El servidor principal del sistema de nombres de dominio (DNS) utilizado como fuente de veracidad para todos los registros DNS del dominio.	Puede usar cualquier IPv4 dirección válida y no utilizada dentro del rango de hosts utilizable.	10.1.1.10
Dirección IP del servidor DNS secundario	Un servidor DNS de respaldo para los registros DNS del dominio.	Puede usar cualquier IPv4 dirección válida y no utilizada dentro del rango de hosts utilizable.	10.1.5.25
Dirección IP del servidor NTP	Un servidor de protocolo de tiempo de red (NTP) es un dispositivo o aplicación que sincroniza los relojes de una red mediante el estándar NTP.	Puedes usar el Amazon Time Sync Service predeterminado con la dirección `169.254.169.123` IP local o con otra dirección IP del servidor NTP.	169.254.169.123 (Servicio Amazon Time Sync)
FQDN para la implementación de VCF	Un nombre de dominio completo (FQDN) es el nombre absoluto de un dispositivo de una red. Un FQDN consta de un nombre de host y un nombre de dominio.	Un FQDN solo puede contener caracteres alfanuméricos, el signo menos (-) y puntos que se utilizan como delimitadores entre etiquetas. Debe ser un FQDN único	frente a local

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
		que sea válido y no haya caducado.	

Conjunto de opciones de DHCP para VPC

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
ID del conjunto de opciones de DHCP	Un conjunto de opciones de DHCP es un grupo de configuraciones de red que utilizan los recursos de la VPC, EC2 como las instancias, para comunicarse a través de la red virtual.	Debe contener un mínimo de 2 servidores DNS. Puede usar Route 53 o servidores DNS personalizados. También debe contener su nombre de dominio DNS y un servidor NTP.	dopt-0a1b2c3d

EC2 key pair

Componente	Description (Descripción)	Requisitos mínimos	Valor (s) de ejemplo
EC2 nombre del par de claves	Un EC2 key pair es un conjunto de credenciales de seguridad que se utilizan para conectarse de forma segura a una EC2 instancia de Amazon.	El nombre del par de claves debe ser único.	`my-ec2-key-pair`

Tablas de enrutamiento de la VPC

Componente	Description (Descripción)	Requisitos mínimos	Valor (s) de ejemplo
ID de la tabla de rutas principal	En Amazon VPC, la tabla de enrutamiento principal es la tabla de enrutamiento predeterminada que se crea automáticamente con la VPC y regula el tráfico de cualquier subred de VPC que no esté asociada explícitamente a una tabla de enrutamiento diferente. Las subredes VLAN de EVS se asocian implícitamente a la tabla de enrutamiento principal de la VPC cuando Amazon EVS las crea.	Debe configurarse para permitir la conectividad con los servicios dependientes, como el DNS o los sistemas locales, para que la implementación del entorno se realice correctamente.	rtb-0123456789abcdef0

Lista de control de acceso (ACL) de red

Componente	Description (Descripción)	Requisitos mínimos	Valor (s) de ejemplo
ID de ACL de red	Una lista de control de acceso a la red (ACL) permite o deniega el tráfico entrante o	Debe permitir que Amazon EVS se comunique con:	acl-0f62c640e793a38a3

Componente	Description (Descripción)	Requisitos mínimos	Valor (s) de ejemplo
	saliente a nivel de subred.	• Servidores DNS a través TCP/UDP del puerto 53. • Subred VLAN de administración de hosts a través de HTTPS y SSH. • Administración de la subred VLAN de VM a través de HTTPS y SSH.	

Registros DNS para componentes de VCF

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de dirección IP	Ejemplo de nombre de host
Host ESX 1	Dirección IP y nombre de host definidos en el registro A y el registro PTR del host ESX 1.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada host ESX en cada implementación de EVS.	10.1.0.10	esxi01

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de dirección IP	Ejemplo de nombre de host
Host ESX 2	Dirección IP y nombre de host definidos en el registro A y el registro PTR del host ESX 2.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada host ESX en cada implementación de EVS.	10.1.0.11	esxi02
Host ESX 3	Dirección IP y nombre de host definidos en el registro A y el registro PTR del host ESX 3.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada host ESX en cada implementación de EVS.	10.1.0.12	esxi03

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de dirección IP	Ejemplo de nombre de host
Host ESX 4	Dirección IP y nombre de host definidos en el registro A y el registro PTR del host ESX 4.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada host ESX en cada implementación de EVS.	10.1.0.13	esxi04
Dispositivo vCenter Server	La dirección IP y el nombre de host se definen en los registros A y PTR de vCenter Server Appliance.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.10	vc01

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de dirección IP	Ejemplo de nombre de host
Clúster de NSX Manager	La dirección IP y el nombre de host se definen en los registros A y PTR del clúster de NSX Manager.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.11	nsx
Dispositivo SDDC Manager	La dirección IP y el nombre de host se definen en los registros A y PTR del dispositivo SDDC Manager.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.12	sddcm01

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de dirección IP	Ejemplo de nombre de host
Dispositivo Cloud Builder	La dirección IP y el nombre de host se definen en los registros A y PTR del dispositivo Cloud Builder.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.13	cb01
Dispositivo NSX Edge 1	La dirección IP y el nombre de host se definen en los registros A y PTR del dispositivo NSX Edge 1.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.14	edge01

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de dirección IP	Ejemplo de nombre de host
Dispositivo NSX Edge 2	La dirección IP y el nombre de host se definen en los registros A y PTR del dispositivo NSX Edge 2.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.15	edge02
Dispositivo NSX Manager 1	La dirección IP y el nombre de host se definen en los registros A y PTR del dispositivo NSX Manager 1.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.16	nsx01

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo de dirección IP	Ejemplo de nombre de host
Dispositivo NSX Manager 2	La dirección IP y el nombre de host se definen en los registros A y PTR del dispositivo NSX Manager 2.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.17	nsx02
Dispositivo NSX Manager 3	La dirección IP y el nombre de host se definen en los registros A y PTR del dispositivo NSX Manager 3.	Amazon EVS requiere una zona de búsqueda directa de DNS con registros A y una zona de búsqueda inversa con registros PTR creados para cada dispositivo de administración de VCF en cada implementación de EVS.	10.1.5.18	nsx03

Infraestructura de VPC Route Server

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
ID del servidor de rutas	Amazon EVS utiliza Amazon VPC Route Server para habilitar el enrutamiento dinámico basado en BGP a su red subyacente de VPC.	Debe especificar un servidor de rutas que comparta rutas con al menos dos puntos finales del servidor de rutas de la subred de acceso al servicio. El ASN del mismo nivel configurado en el servidor de rutas y el del mismo nivel de NSX Edge deben coincidir, y las direcciones IP del mismo nivel deben ser únicas.	rs-0a1b2c3d4e5f67890
asociación de servidores de rutas	La conexión entre un servidor de rutas y una VPC.	El servidor de rutas debe estar asociado a la VPC.	`{ "RouteServerAssociation": { "RouteServerId": "rs-0a1b2c3d4e5f67890", "VpcId": "vpc-1", "State": "associating" } }`
ASN BGP del lado del servidor de rutas de	El ASN del lado de Amazon represent	Este valor debe ser único y estar	65001

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
VPC (ASN del lado de Amazon)	a el AWS lado de la sesión de BGP entre el servidor de rutas de VPC y el par de NSX Edge. Debe especificar este ASN BGP al crear el servidor de rutas. Para obtener más información, consulte Crear un servidor de rutas en la Guía del usuario de Amazon VPC.	comprendido entre 1 y 4294967295. AWS recomienda utilizar un ASN privado en el rango 64512—65534 (ASN de 16 bits) o 4200000000—4294967294 (ASN de 32 bits).	
ID de punto final 1 del servidor de rutas	Un punto final del servidor de rutas es un componente AWS administrado dentro de una subred que facilita las conexiones BGP (Border Gateway Protocol) entre su servidor de rutas y sus pares de BGP.	Debe implementar el punto final del servidor de rutas en la subred de acceso al servicio.	rse-0123456789abcdef0
ID de par 1 del servidor de rutas	El par del servidor de rutas es una sesión de interconexión BGP entre un punto final del servidor de rutas y el dispositivo en el que está desplegado AWS (NSX Edge).	El valor de ASN del mismo nivel especificado en el par del servidor de rutas debe coincidir con el valor de ASN del mismo nivel utilizado para la puerta de enlace de nivel 0 de NSX Edge.	rsp-0123456789abcdef0

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
servidor de enrutamiento por 1 dirección IP (EVS NSX Edge de 1 cara)	La dirección IP del servidor de rutas peer ()`PeerAddress` .	Debe usar una dirección IP única no utilizada de la VLAN de enlace superior de NSX. Amazon EVS aplicará esta dirección IP a NSX Edge 1 como parte de la implementación y se sincronizará con el punto final del servidor de rutas.	10.1.7.10
dirección ENI del punto final del servidor de rutas igual a 1	La dirección IP ENI del punto final del servidor de rutas peer (`EndpointEniAddress`).	Generada automáticamente por el servidor de rutas al crear el par.	10.1.7.11
ID del punto final 2 del servidor de rutas	Un punto final del servidor de rutas es un componente AWS administrado dentro de una subred que facilita las conexiones BGP (Border Gateway Protocol) entre su servidor de rutas y sus pares de BGP.	Debe implementar el punto final del servidor de rutas en la subred de acceso al servicio.	rse-fedcba9876543210f

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)
ID de servidor de enrutamiento par 2 (EVS NSX Edge 2 side)	El par del servidor de rutas es una sesión de emparejamiento BGP entre un punto final del servidor de rutas y el dispositivo en el que está desplegado AWS (NSX Edge).	El valor de ASN del mismo nivel especificado en el par del servidor de rutas debe coincidir con el valor de ASN del mismo nivel utilizado para la puerta de enlace de nivel 0 de NSX Edge.	rsp-fedcba9876543210f
dirección IP par 2 del servidor de rutas	La dirección IP del servidor de rutas peer (`PeerAddress`).	Debe usar una dirección IP única de la VLAN de enlace superior de NSX. Amazon EVS aplicará esta dirección IP a NSX Edge 2 como parte de la implementación y se sincronizará con el punto final del servidor de rutas.	10.1.7.200
dirección ENI del punto final del servidor de rutas par 2	La dirección IP ENI del punto final del servidor de rutas peer (`EndpointEniAddress`).	Generada automáticamente por el servidor de rutas al crear el par.	10.1.7.201

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor (s)

propagación del servidor de rutas	La propagación del servidor de rutas instala las rutas de la FIB en la tabla de rutas que especificó.	Debe especificar la tabla de rutas asociada a la subred de acceso al servicio. Amazon EVS solo admite IPv4 redes en este momento.	<pre>{
			"RouteServerEndpoint": {
			"RouteServerId": "rs-1",
			"RouteServerEndpointId": "rse-1",
			"VpcId": "vpc-1",
			"SubnetId": "subnet-1",
			"State": "pending"
			}
			}</pre>

BGP ASN del lado homólogo de NSX	BGP ASN para el lado NSX de la conexión.	Se sugiere usar el ASN 65000 predeterminado de NSX	65000

Recursos de acceso a Internet de HCX (opcional)

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor
ID DE SPAM	El administrador de direcciones IP (IPAM) de Amazon VPC se utiliza para administrar las direcciones IP para el acceso a Internet mediante HCX.	Debe configurarse para proporcionar direcciones públicas. IPv4 Necesario solo para la configuración de acceso a Internet de HCX.	ipam-0123456789abcdef0

Componente	Description (Descripción)	Requisitos mínimos	Ejemplo (s) de valor
ID del grupo de IPAM	Un grupo de IPv4 IPAM público propiedad de Amazon que proporciona direcciones para los componentes de HCX.	Debe configurarse como un grupo público. IPv4 Necesario solo para la configuración de acceso a Internet de HCX.	ipam-pool-0123456789abcdef0
Bloque CIDR de VLAN pública HCX	Un bloque IPv4 CIDR público secundario asignado desde el grupo de IPAM para la subred de VLAN pública de HCX.	Debe tener una máscara de red /28 y asignarse desde el grupo público de IPAM propiedad de Amazon. Necesario solo para la configuración de acceso a Internet de HCX.	18.97.137.0/28
Direcciones IP elásticas	Direcciones IP elásticas secuenciales asignadas desde el grupo de IPAM para los componentes de HCX.	Mínimo de 3 EIPs del mismo grupo de IPAM para HCX Manager, HCX Interconnect Appliance (HCX-IX) y HCX Network Extension (HCX-NE). Necesario únicamente para la configuración de acceso a Internet de HCX.	eipalloc-0123456789abcdef0, eipalloc-0123456789abcdef1, eipalloc-0123456789abcdef2

Introducción a Amazon Elastic VMware Service

Utilice esta guía para empezar a utilizar Amazon Elastic VMware Service (Amazon EVS). Aprenderá a crear un entorno de Amazon EVS con hosts dentro de su propia Amazon Virtual Private Cloud (VPC).

Cuando haya terminado, dispondrá de un entorno de Amazon EVS que podrá utilizar para migrar sus cargas de trabajo VMware basadas en vSphere a. Nube de AWS

Important

Para empezar de la forma más sencilla y rápida posible, en este tema se incluyen los pasos para crear una VPC y se especifican los requisitos mínimos para la configuración del servidor DNS y la creación del entorno Amazon EVS. Antes de crear estos recursos, le recomendamos que planifique el espacio de direcciones IP y la configuración de los registros DNS de forma que cumpla sus requisitos. También debería familiarizarse con los requisitos de VCF 5.2.x. Consulte las notas de la versión 5.2.x de VCF para obtener información relevante sobre la versión.

Important

Para obtener información sobre las versiones de VCF proporcionadas por Amazon EVS, consulte. the section called “Versiones e instancias de VCF EC2 ”

Temas

Requisitos previos

Antes de empezar, debe completar las tareas previas de Amazon EVS. Para obtener más información, consulte Configuración de Amazon Elastic VMware Service.

Cree una VPC con subredes y tablas de enrutamiento

> **Note**
>
> La VPC, las subredes y el entorno de Amazon EVS deben crearse en la misma cuenta. Amazon EVS no admite el uso compartido entre cuentas de subredes de VPC o entornos de Amazon EVS.

Example

Amazon VPC console

1. Abra la consola de Amazon VPC.
2. En el panel de VPC, elija Create VPC (Crear VPC).
3. En Recursos para crear, elija VPC y más.
4. Mantenga seleccionada la opción Generación automática de etiquetas de nombre para crear etiquetas de nombre para los recursos de la VPC, o desactívela para proporcionar sus propias etiquetas de nombre para los recursos de la VPC.
5. Para el bloque IPv4 CIDR, introduzca un bloque CIDR. IPv4 Una VPC debe tener un bloque IPv4 CIDR. Asegúrese de crear una VPC con el tamaño adecuado para alojar las subredes de Amazon EVS. Para obtener más información, consulte the section called “Consideraciones sobre las redes de Amazon EVS”.

> **Note**
>
> Amazon EVS no es compatible IPv6 en este momento.

6. Mantenga Tenancy como. `Default` Con esta opción seleccionada, EC2 las instancias que se lancen en esta VPC utilizarán el atributo de tenencia especificado cuando se lancen las instancias. Amazon EVS lanza EC2 instancias completas en su nombre.
7. En Número de zonas de disponibilidad (AZs), elija 1.

> **Note**
>
> Por el momento, Amazon EVS solo admite implementaciones Single-AZ.

8. Amplíe Personalizar AZs y elija la zona de disponibilidad para sus subredes.

> **Note**
>
> Debe realizar la implementación en una AWS región en la que Amazon EVS sea compatible. Para obtener más información sobre la disponibilidad regional de Amazon EVS, consulte los puntos de enlace y las cuotas de Amazon Elastic VMware Service en la Guía de referencia AWS general.

9. (Opcional) Si necesita conectividad a Internet, en Número de subredes públicas, elija 1.
10. En Número de subredes privadas, elija 1. Esta subred privada se utilizará como subred de acceso al servicio que proporcionó a Amazon EVS durante el paso de creación del entorno. Para obtener más información, consulte the section called “Subred de acceso a servicios”.
11. Para elegir los rangos de direcciones IP para las subredes, expanda Personalizar bloques CIDR de subredes.

> **Note**
>
> Las subredes VLAN de Amazon EVS también deberán crearse a partir de este espacio CIDR de VPC. Asegúrese de dejar suficiente espacio en el bloque CIDR de la VPC para las subredes de VLAN que requiere el servicio. Para obtener más información, consulte the section called “Consideraciones sobre las redes de Amazon EVS”

12. (Opcional) Para conceder acceso a Internet IPv4 a los recursos, en el caso de las puertas de enlace NAT, selecciona In 1 AZ. Tenga en cuenta que existe un costo asociado a las puertas de enlace NAT. Para obtener más información, consulte los precios de las pasarelas NAT.

> **Note**
>
> Amazon EVS requiere el uso de una puerta de enlace NAT para habilitar la conectividad a Internet saliente.

13. Para VPC endpoints (Puntos de conexión de la VPC), elija None (Ninguno).

> **Note**
>
> Amazon S3 Por el momento, Amazon EVS no admite puntos de enlace de VPC. Para habilitar la Amazon S3 conectividad, debe configurar un punto final de VPC de interfaz que utilice AWS PrivateLink for. Amazon S3Para obtener más información, consulte AWS PrivateLink la Guía del usuario de Amazon Simple Storage Service. Amazon S3

14. Para las opciones de DNS, mantenga los valores predeterminados seleccionados. Amazon EVS requiere que su VPC tenga capacidad de resolución de DNS para todos los componentes de VCF.

15. (Opcional) Para agregar una etiqueta a su VPC, expanda Etiquetas adicionales, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.

16. Seleccione Creación de VPC.

> **Note**
>
> Durante la creación de la VPC, crea Amazon VPC automáticamente una tabla de enrutamiento principal y le asocia subredes de forma implícita de forma predeterminada.

AWS CLI

1. Abra una sesión de terminal.
2. Cree una VPC con una subred privada y una subred pública opcional en una única zona de disponibilidad.

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

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

3. Habilite los nombres de host DNS y la compatibilidad con 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. Cree una subred privada en la 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. Guarde el ID de subred privada para usarlo en los siguientes comandos.

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

6. (Opcional) Cree una subred pública si necesita conectividad 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) Guarde el ID de subred pública para usarlo en comandos posteriores.

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

8. (Opcional) Cree y adjunte una puerta de enlace a Internet si se crea la subred pública.

```
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) Cree una puerta de enlace NAT si necesita conectividad 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. Cree y configure las tablas de enrutamiento necesarias.

```
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. Agregue las rutas necesarias a las tablas de rutas.

```
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. Asocie las tablas de rutas a sus subredes.

```
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 la creación de la VPC, crea Amazon VPC automáticamente una tabla de enrutamiento principal y le asocia subredes de forma implícita de forma predeterminada.

Elija su opción de conectividad HCX

Seleccione una opción de conectividad para su entorno Amazon EVS:

- Conectividad privada: proporciona vías de red de alto rendimiento para HCX, lo que optimiza la fiabilidad y la coherencia. Requiere el uso de AWS Direct Connect o Site-to-Site VPN para la conectividad de red externa.
- Conectividad a Internet: utiliza la Internet pública para establecer una ruta de migración flexible y rápida de configurar. Requiere el uso del administrador de direcciones IP (IPAM) de VPC y direcciones IP elásticas.

Para obtener un análisis detallado, consulte. the section called “Opciones de conectividad HCX”

Elija su opción:

- Opción A: Solo conectividad privada → Continuarthe section called “Configurar la tabla de enrutamiento principal de la VPC”.
- Opción B: Conectividad a Internet → Continuarthe section called “Configuración de conectividad a Internet del HCX”.

Configuración de conectividad a Internet del HCX

> **Note**
>
> Omita esta sección si ha elegido la conectividad privada HCX y continúe. the section called “Configurar la tabla de enrutamiento principal de la VPC”

Para habilitar la conectividad a Internet HCX para Amazon EVS, debe:

- Asegúrese de que la cuota del administrador de direcciones IP (IPAM) de VPC para la longitud de la máscara de red de bloques IPv4 CIDR públicos contiguos proporcionada por Amazon sea de /28 o superior.

  > **Important**
  >
  > El uso de cualquier bloque IPv4 CIDR público contiguo proporcionado por Amazon con una longitud de máscara de red inferior a /28 provocará problemas de conectividad de HCX. Para obtener más información sobre cómo aumentar las cuotas de IPAM, consulta Cuotas de tu IPAM.

- Cree un IPAM y un grupo de IPv4 IPAM público con un CIDR que tenga una longitud mínima de máscara de red de /28.
- Asigne al menos dos direcciones IP elásticas (EIPs) del grupo de IPAM para los dispositivos HCX Manager y HCX Interconnect (HCX-IX). Asigne una dirección IP elástica adicional para cada dispositivo de red HCX que necesite implementar.
- Añada el bloque IPv4 CIDR público como CIDR adicional a su VPC.

Para obtener más información sobre la administración de la conectividad a Internet del HCX tras la creación del entorno, consulte. the section called “Conectividad pública HCX”

Cree un IPAM

Siga estos pasos para crear un IPAM.

> **Note**
>
> Puede usar la capa gratuita de IPAM para crear recursos de IPAM para usarlos con Amazon EVS. Si bien el IPAM en sí mismo es gratuito con la capa gratuita, usted es responsable de los costos de otros AWS servicios utilizados junto con la IPAM, como las pasarelas NAT y cualquier IPv4 dirección pública que utilice y que supere el límite de la capa gratuita. Para obtener más información sobre los precios de IPAM, consulta la página de precios.Amazon VPC

> **Note**
>
> Amazon EVS no admite direcciones de unidifusión IPv6 global (GUA) privadas CIDRs en este momento.

Cree un grupo de IPAM público IPv4

Siga estos pasos para crear un IPv4 grupo público.

IPAM console

1. Abra la consola de IPAM.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el alcance público. Para obtener más información sobre los ámbitos, consulte Cómo funciona la IPAM.
4. Elija Create pool (Crear grupo).
5. (Opcional) Agregue una Name tag (Etiqueta de nombre) y una Description (Descripción) para el grupo.
6. En Familia de direcciones, elija. IPv4
7. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance.
8. En Locale (Configuración regional), elija la configuración regional para el grupo. La configuración regional es la AWS región en la que desea que este grupo de IPAM esté disponible para las asignaciones. La configuración regional que elija debe coincidir con la AWS región en la que está implementada la VPC.
9. En Servicio, elija EC2 (EIP/VPC). Esto anunciará las CIDRs asignaciones de este grupo para el EC2 servicio de Amazon (para direcciones IP elásticas).
10. En Fuente de IP pública, seleccione Propiedad de Amazon.
11. En CIDRs Para aprovisionar, selecciona Añadir CIDR público propiedad de Amazon.
12. En Máscara de red, elija una longitud de máscara de red CIDR. /28 es la longitud mínima de máscara de red requerida.
13. Elija Create pool (Crear grupo).

AWS CLI

1. Abra una sesión de terminal.
2. Obtenga el ID de ámbito público de su IPAM.

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

3. Cree un grupo de IPAM en el ámbito 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. Guarde el ID del grupo para usarlo en comandos posteriores.

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

5. Aprovisione un bloque CIDR del grupo con una longitud mínima de máscara de red de /28.

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

Asigne direcciones IP elásticas del grupo de IPAM

Siga estos pasos para asignar direcciones IP elásticas (EIPs) del grupo de IPAM para los dispositivos HCX Service Mesh.

Amazon VPC console

1. Abra la Consola de Amazon VPC.
2. En el panel de navegación, elija Elastic. IPs
3. Elija Asignar dirección IP elástica.
4. Seleccione Asignar mediante un grupo de IPv4 IPAM.
5. Seleccione el IPv4 grupo público propiedad de Amazon que configuró anteriormente.
6. En Asignar el método de IPAM, elija Introducir manualmente la dirección dentro del grupo de IPAM.

> **Important**
>
> No puede asociar las dos primeras EIPs ni las últimas EIP del bloque CIDR de IPAM público a la subred de la VLAN. EIPs Están reservadas como direcciones de red, puerta de enlace predeterminada y direcciones de transmisión. Amazon EVS arroja un error de validación si intenta EIPs asociarlos a la subred de VLAN.

> **Important**
>
> Introduzca manualmente las direcciones dentro del grupo de IPAM para garantizar que no se EIPs asignen las reservas de Amazon EVS. Si permite que IPAM elija el EIP, IPAM puede asignar un EIP que Amazon EVS reserve, lo que provocará un error durante la asociación del EIP a la subred de la VLAN.

7. Especifique el EIP que se va a asignar del grupo de IPAM.
8. Elija Asignar.
9. Repita este proceso para asignar el resto EIPs que necesite. Debe asignar al menos dos EIPs del grupo de IPAM para los dispositivos HCX Manager y HCX Interconnect (HCX-IX). Asigne un EIP adicional para cada dispositivo de red HCX que necesite implementar.

AWS CLI

1. Abra una sesión de terminal.
2. Obtenga el ID del grupo de IPAM que creó anteriormente.

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

3. Asigne direcciones IP elásticas del grupo de IPAM. Debe asignar al menos dos EIPs del grupo de IPAM para los dispositivos HCX Manager y HCX Interconnect (HCX-IX). Asigne un EIP adicional para cada dispositivo de red HCX que necesite implementar.

> **Important**
>
> No puede asociar las dos primeras EIPs ni las últimas EIP del bloque CIDR de IPAM público a una subred de VLAN. EIPs Están reservadas como direcciones de red, puerta de enlace predeterminada y direcciones de transmisión. Amazon EVS arroja un error de validación si intenta EIPs asociarlos a la subred de VLAN.

> **Important**
>
> Introduzca manualmente las direcciones dentro del grupo de IPAM para garantizar que no se EIPs asignen las reservas de Amazon EVS. Si permite que IPAM elija el EIP, IPAM puede asignar un EIP que Amazon EVS reserve, lo que provocará un error durante la asociación del EIP a la subred de la 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
```

Agregue el bloque IPv4 CIDR público del grupo de IPAM a la VPC para la conectividad a Internet HCX

Para habilitar la conectividad a Internet de HCX, debe agregar el bloque IPv4 CIDR público del grupo de IPAM a su VPC como CIDR adicional. Amazon EVS utiliza este bloque CIDR para conectar VMware HCX a la red. Siga estos pasos para añadir el bloque CIDR a su VPC.

> **Important**
>
> Debe introducir manualmente el bloque IPv4 CIDR que añada a la VPC. Amazon EVS no admite el uso de un bloque CIDR asignado a IPAM en este momento. El uso de un bloque CIDR asignado al IPAM puede provocar un error en la asociación del EIP.

Amazon VPC console

1. Abra la Consola de Amazon VPC.
2. En el panel de navegación, elija Su. VPCs
3. Seleccione la VPC que creó anteriormente y elija Acciones, Editar. CIDRs
4. Elija Añadir un nuevo IPV4 CIDR.
5. Seleccione la entrada manual IPV4 del CIDR.
6. Especifique el bloque CIDR del grupo de IPAM público que creó anteriormente.

AWS CLI

1. Abra una sesión de terminal.
2. Obtenga el ID del grupo de IPAM y el bloque CIDR aprovisionado.

```
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. Añada el bloque CIDR a su VPC.

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

Configurar la tabla de enrutamiento principal de la VPC

Las subredes VLAN de Amazon EVS están asociadas implícitamente a la tabla de enrutamiento principal de la VPC. Para habilitar la conectividad con los servicios dependientes, como el DNS o los sistemas locales, para una implementación correcta del entorno, debe configurar la tabla de enrutamiento principal para permitir el tráfico a estos sistemas. La tabla de rutas principal debe incluir una ruta para el CIDR de la VPC. El uso de la tabla de rutas principal solo es necesario para la implementación inicial del entorno Amazon EVS. Tras la implementación del entorno, puede configurarlo para que utilice una tabla de rutas personalizada. Para obtener más información, consulte the section called “Configure una tabla de enrutamiento personalizada”.

Tras la implementación del entorno, debe asociar de forma explícita cada una de las subredes de VLAN de Amazon EVS a una tabla de enrutamiento de la VPC. La conectividad de NSX falla si las subredes de VLAN no están asociadas explícitamente a una tabla de enrutamiento de VPC. Le recomendamos encarecidamente que asocie las subredes de forma explícita a una tabla de enrutamiento personalizada después de la implementación del entorno. Para obtener más información, consulte the section called “Configurar la tabla de enrutamiento principal de la VPC”.

> **Important**
>
> Amazon EVS admite el uso de una tabla de enrutamiento personalizada solo después de crear el entorno de Amazon EVS. No se deben utilizar tablas de enrutamiento personalizadas durante la creación del entorno de Amazon EVS, ya que esto puede provocar problemas de conectividad.

Configuración de los servidores DNS y NTP mediante el conjunto de opciones de DHCP de la VPC

Important

La implementación de su entorno falla si no cumple estos requisitos de Amazon EVS:

- Incluya una dirección IP del servidor DNS principal y una dirección IP del servidor DNS secundario en el conjunto de opciones de DHCP.
- Incluya una zona de búsqueda directa de DNS con registros A para cada dispositivo de administración de VCF y host de Amazon EVS de su implementación.
- Incluya una zona de búsqueda inversa de DNS con registros PTR para cada dispositivo de administración de VCF y host de Amazon EVS de su implementación.
- Configure la tabla de rutas principal de la VPC para garantizar que exista una ruta a sus servidores DNS.
- Asegúrese de que el registro del nombre de dominio sea válido y no haya caducado, y de que no existan nombres de host o direcciones IP duplicados.
- Configure sus grupos de seguridad y listas de control de acceso a la red (ACLs) para permitir que Amazon EVS se comunique con:
  - Servidores DNS a través TCP/UDP del puerto 53.
  - Subred VLAN de administración de hosts a través de HTTPS y SSH.
  - Subred de VLAN de administración a través de HTTPS y SSH.

Amazon EVS utiliza el conjunto de opciones de DHCP de la VPC para recuperar lo siguiente:

- Servidores del sistema de nombres de dominio (DNS) para la resolución de direcciones IP del host.
- Nombres de dominio para la resolución de DNS.
- Servidores de protocolo de tiempo de red (NTP) para la sincronización horaria.

Puede crear un conjunto de opciones de DHCP mediante la Amazon VPC consola o. AWS CLI Para obtener más información, consulte Crear un conjunto de opciones de DHCP en la Guía del Amazon VPC usuario.

Configure los servidores DNS

La configuración de DNS permite la resolución de nombres de host en su entorno Amazon EVS. Para implementar correctamente un entorno Amazon EVS, el conjunto de opciones de DHCP de su VPC debe tener la siguiente configuración de DNS:

- Una dirección IP del servidor DNS principal y una dirección IP del servidor DNS secundario en el conjunto de opciones de DHCP.
- Una zona de búsqueda directa de DNS con registros A para cada dispositivo de administración de VCF y host de Amazon EVS de la implementación.
- Una zona de búsqueda inversa con registros PTR para cada dispositivo de administración de VCF y host de Amazon EVS de la implementación. Para la configuración de NTP, puede utilizar la dirección `169.254.169.123` Amazon NTP predeterminada u otra IPv4 dirección que prefiera.

Para obtener más información sobre la configuración de los servidores DNS en un conjunto de opciones de DHCP, consulte Crear un conjunto de opciones de DHCP.

Configure el DNS para la conectividad local

Para la conectividad local, recomendamos el uso de zonas alojadas privadas de Route 53 con resolutores entrantes. Esta configuración permite la resolución de DNS híbrida, en la que puede usar Route 53 para el DNS interno de su VPC e integrarlo con su infraestructura de DNS local existente. Esto permite que los recursos de la VPC resuelvan los nombres de dominio alojados en la red local y viceversa, sin necesidad de configuraciones complejas. Si es necesario, también puede usar su propio servidor DNS con los resolutores de salida de Route 53. Para ver los pasos de configuración, consulte Creación de una zona alojada privada y Reenvío de consultas de DNS entrantes a la VPC en la Guía para desarrolladores de Amazon Route 53.

> **Note**
>
> El uso de Route 53 y un servidor de sistema de nombres de dominio (DNS) personalizado en el conjunto de opciones de DHCP puede provocar un comportamiento inesperado.

> **Note**
>
> Si utilizas nombres de dominio DNS personalizados definidos en una zona alojada privada o utilizas un DNS privado con puntos de enlace de VPC de interfaz (AWS PrivateLink),

debes establecer `enableDnsHostnames` tanto `enableDnsSupport` los atributos como en. Route 53`true` Para obtener más información, consulte Atributos de DNS para su VPC.

Solucione los problemas de accesibilidad del DNS

Amazon EVS requiere una conexión persistente con el administrador del SDDC y los servidores DNS del conjunto de opciones de DHCP de la VPC para acceder a los registros de DNS. Si la conexión persistente con SDDC Manager deja de estar disponible, Amazon EVS ya no podrá validar el estado del entorno y es posible que pierda el acceso al entorno. Para obtener información sobre los pasos para solucionar este problema, consulte. the section called “Falló la comprobación de accesibilidad”

Configure los servidores NTP

Los servidores NTP proporcionan el tiempo a la red. Una referencia de tiempo coherente y precisa en su EC2 instancia de Amazon es crucial para muchas tareas y procesos del entorno VCF. La sincronización horaria es esencial para:

- Registro y auditoría del sistema
- Operaciones de seguridad
- Administración de sistemas distribuidos
- Resolución de problemas

Puede introducir las IPv4 direcciones de hasta cuatro servidores NTP en el conjunto de opciones de DHCP de su VPC. Puedes especificar la IPv4 dirección de Amazon Time Sync Service`169.254.169.123`. De forma predeterminada, las EC2 instancias de Amazon que despliega Amazon EVS utilizan el Amazon Time Sync Service en IPv4 la dirección. `169.254.169.123`

Para obtener más información sobre los servidores NTP, consulte la RFC 2123. Para obtener más información sobre Amazon Time Sync Service, consulte Sincronización precisa del reloj y la hora en su EC2 instancia y Configurar NTP en los hosts de VMware Cloud Foundation en la documentación de VMware Cloud Foundation.

Para configurar los ajustes de NTP

1. Elija su fuente de NTP:
   - Amazon Time Sync Service (recomendado)

- Servidores NTP personalizados

2. Agregue servidores NTP a su conjunto de opciones de DHCP. Para obtener más información, consulte Crear un conjunto de opciones de DHCP en la Guía del usuario de Amazon VPC.
3. Verifique la sincronización horaria. Para obtener más información sobre la configuración del conjunto de opciones de DHCP, consultethe section called “Configure el conjunto de opciones de DHCP de su VPC”.

Configurar la conectividad de red local (opcional)

Puede configurar la conectividad de su centro de datos local Direct Connect con su AWS infraestructura mediante una puerta de enlace de tránsito asociada o mediante un adjunto de AWS Site-to-Site VPN a una puerta de enlace de tránsito.

Para habilitar la conectividad con los sistemas locales para una implementación correcta en el entorno, debe configurar la tabla de rutas principal de la VPC para permitir el tráfico a estos sistemas. Para obtener más información, consulte the section called “Configurar la tabla de enrutamiento principal de la VPC”.

Una vez creado el entorno de Amazon EVS, debe actualizar las tablas de rutas de Transit Gateway con la CIDRs VPC creada en el entorno de Amazon EVS. Para obtener más información, consulte the section called “Configure las tablas de rutas de las pasarelas de tránsito y los prefijos de Direct Connect para la conectividad local (opcional)”.

Para obtener más información sobre cómo configurar una Direct Connect conexión, consulte Direct Connect pasarelas y asociaciones de pasarelas de tránsito. Para obtener más información sobre el uso de la AWS Site-to-Site VPN con AWS Transit Gateway, consulte los adjuntos de AWS Site-to-Site VPN en Amazon VPC Transit Gateways en la Guía del usuario de Amazon VPC Transit Gateway.

> **Note**
>
> Amazon EVS no admite la conectividad a través de una interfaz virtual privada (VIF) de AWS Direct Connect ni a través de una conexión AWS Site-to-Site VPN que termine directamente en la VPC subyacente.

Configure una instancia de VPC Route Server con puntos finales y pares

Amazon EVS utiliza Amazon VPC Route Server para habilitar el enrutamiento dinámico basado en BGP a su red subyacente de VPC. Debe especificar un servidor de rutas que comparta rutas con al menos dos puntos finales del servidor de rutas en la subred de acceso al servicio. El ASN del par configurado en los pares del servidor de rutas debe coincidir y las direcciones IP del par deben ser únicas.

Si está configurando Route Server para la conectividad a Internet de HCX, debe configurar las propagaciones de Route Server tanto para la subred de acceso al servicio como para la subred pública que creó en el primer paso de este procedimiento.

Important

La implementación de su entorno falla si no cumple estos requisitos de Amazon EVS para la configuración del servidor de rutas de VPC:

- Debe configurar al menos dos puntos finales del servidor de rutas en la subred de acceso al servicio.
- Al configurar el Border Gateway Protocol (BGP) para la puerta de enlace de nivel 0, el valor de ASN del mismo nivel del servidor de rutas de la VPC debe coincidir con el valor del ASN del mismo nivel de NSX Edge.
- Al crear los dos servidores de rutas homólogos, debe utilizar una dirección IP única de la VLAN de enlace superior de NSX para cada punto final. Estas dos direcciones IP se asignarán a los bordes de NSX durante la implementación del entorno Amazon EVS.
- Al habilitar la propagación del servidor de rutas, debe asegurarse de que todas las tablas de rutas que se propaguen tengan al menos una asociación de subred explícita. El anuncio de rutas BGP falla si las tablas de rutas propagadas no tienen una asociación de subred explícita.

Para obtener más información sobre la configuración del servidor de rutas de VPC, consulte el tutorial de introducción a Route Server.

Important

Al habilitar la propagación del servidor de rutas, asegúrese de que todas las tablas de rutas que se están propagando tengan al menos una asociación de subred explícita. El anuncio de rutas BGP falla si la tabla de enrutamiento tiene una asociación de subred explícita.

Note

Para la detección de actividad entre pares de Route Server, Amazon EVS solo admite el mecanismo BGP keepalive predeterminado. Amazon EVS no admite la detección de reenvío bidireccional (BFD) de varios saltos.

Note

Le recomendamos que habilite las rutas persistentes para la instancia del servidor de rutas con una duración de persistencia de entre 1 y 5 minutos. Si está habilitada, las rutas se conservarán en la base de datos de enrutamiento del servidor de rutas incluso si finalizan todas las sesiones de BGP. Para obtener más información, consulte Crear un servidor de rutas en la Guía del Amazon VPC usuario.

Note

Si utiliza una puerta de enlace NAT o una puerta de enlace de tránsito, asegúrese de que el servidor de rutas esté configurado correctamente para propagar las rutas de NSX a las tablas de rutas de la VPC.

Resolución de problemas

Si tiene problemas:

- Compruebe que cada tabla de enrutamiento tenga una asociación de subred explícita.
- Compruebe que los valores de ASN homólogos introducidos para el servidor de rutas y la puerta de enlace de nivel 0 de NSX coincidan.

- Confirme que las direcciones IP de los puntos finales de Route Server sean únicas.
- Revise el estado de propagación de la ruta en sus tablas de rutas.
- Utilice el registro de pares de VPC Route Server para supervisar el estado de la sesión de BGP y solucionar problemas de conexión. Para obtener más información, consulte el registro entre pares del servidor de rutas en la Guía del usuario de Amazon VPC.

Cree una ACL de red para controlar el tráfico de subred de VLAN de Amazon EVS

Amazon EVS utiliza una lista de control de acceso a la red (ACL) para controlar el tráfico hacia y desde las subredes VLAN de Amazon EVS. Puede usar la ACL de red predeterminada para su VPC o puede crear una ACL de red personalizada para su VPC con reglas similares a las reglas de sus grupos de seguridad para agregar una capa de seguridad a su VPC. Para obtener más información, consulte Crear una ACL de red para su VPC en la Guía del usuario de Amazon VPC.

Si planea configurar la conectividad a Internet de HCX, asegúrese de que las reglas de ACL de red que configure permitan las conexiones entrantes y salientes necesarias para los componentes de HCX. Para obtener más información sobre los requisitos de los puertos HCX, consulte la Guía del usuario de HCX. VMware

Important

Si se conecta a través de Internet, la asociación de una dirección IP elástica a una VLAN proporciona acceso directo a Internet a todos los recursos de esa subred de la VLAN. Asegúrese de tener las listas de control de acceso a la red adecuadas configuradas para restringir el acceso según sea necesario según sus requisitos de seguridad.

Important

EC2 los grupos de seguridad no funcionan en las interfaces de red elásticas que están conectadas a las subredes de VLAN de Amazon EVS. Para controlar el tráfico hacia y desde las subredes VLAN de Amazon EVS, debe usar una lista de control de acceso a la red.

Cree un entorno Amazon EVS

> **Important**
>
> Para empezar de la forma más sencilla y rápida posible, en este tema se incluyen los pasos para crear un entorno de Amazon EVS con la configuración predeterminada. Antes de crear un entorno, le recomendamos que se familiarice con todos los ajustes e implemente un entorno con los ajustes que se ajusten a sus requisitos. Los entornos solo se pueden configurar durante la creación inicial del entorno. Los entornos no se pueden modificar después de haberlos creado. Para obtener una descripción general de todas las posibles configuraciones del entorno de Amazon EVS, consulte la Guía de referencia de la API de Amazon EVS.

> **Note**
>
> Su ID de entorno estará disponible para Amazon EVS en todas AWS las regiones para satisfacer las necesidades de conformidad con las licencias VCF.

> **Note**
>
> Los entornos de Amazon EVS se deben implementar en la misma región y zona de disponibilidad que las subredes de VPC y VPC.

Complete este paso para crear un entorno Amazon EVS con hosts y subredes de VLAN.

Example

Amazon EVS console

1. Ve a la consola Amazon EVS.

   > **Note**
   >
   > Asegúrese de que la AWS región que se muestra en la parte superior derecha de la consola es la AWS región en la que desea crear el entorno. Si no es así, selecciona el

menú desplegable situado junto al nombre de la AWS región y elige la AWS región que quieras usar.

2. En el panel de navegación, elija Entornos.
3. Seleccione Creación de entorno.
4. En la página de requisitos de Validate Amazon EVS, comprueba que se cumplen los requisitos de servicio. Para obtener más información, consulte Configuración de Amazon Elastic VMware Service.
   a. (Opcional) En Nombre, introduzca un nombre de entorno.
   b. Para la versión de entorno, elija su versión de VCF. Para obtener información sobre las versiones de VCF proporcionadas por Amazon EVS, consulte. the section called “Versiones e instancias de VCF EC2 ”
   c. Para el ID del sitio, introduzca el ID del sitio de Broadcom.
   d. Para la clave de solución VCF, introduzca una clave de solución VCF (vSphere 8 Enterprise Plus for VMware VCF). Un entorno existente no puede utilizar esta clave de licencia.

> **Note**
>
> La clave de la solución VCF debe tener al menos 256 núcleos.

> **Note**
>
> Su licencia VCF estará disponible para Amazon EVS en todas AWS las regiones para garantizar el cumplimiento de la licencia. Amazon EVS no valida las claves de licencia. Para validar las claves de licencia, visite el soporte de Broadcom.

> **Note**
>
> Amazon EVS requiere que mantenga una clave de solución VCF válida en SDDC Manager para que el servicio funcione correctamente. Si administra la clave de la solución VCF mediante vSphere Client después de la implementación, debe asegurarse de que las claves también aparezcan en la pantalla de licencias de la interfaz de usuario de SDDC Manager.

e. Para la clave de licencia de vSAN, introduzca una clave de licencia de vSAN. Un entorno existente no puede utilizar esta clave de licencia.

> **Note**
>
> La clave de licencia de vSAN debe tener al menos 110 TiB de capacidad de vSAN.

> **Note**
>
> Su licencia VCF estará disponible para Amazon EVS en todas AWS las regiones para garantizar el cumplimiento de la licencia. Amazon EVS no valida las claves de licencia. Para validar las claves de licencia, visite el soporte de Broadcom.

> **Note**
>
> Amazon EVS requiere que mantenga una clave de licencia de vSAN válida en SDDC Manager para que elija el servicio para que funcione correctamente. Si administra la clave de licencia de vSAN mediante vSphere Client después de la implementación, debe asegurarse de que las claves también aparezcan en la pantalla de licencias de la interfaz de usuario de SDDC Manager.

f. Para conocer los términos de licencia de VCF, marque la casilla para confirmar que ha adquirido y seguirá manteniendo el número necesario de licencias de software de VCF para cubrir todos los núcleos de procesador físicos del entorno Amazon EVS. La información sobre el software VCF en Amazon EVS se compartirá con Broadcom para verificar el cumplimiento de la licencia.

g. Elija Siguiente.

5. En la página Especifique los detalles del host, complete los siguientes pasos cuatro veces para añadir cuatro hosts al entorno. Los entornos de Amazon EVS requieren cuatro hosts para la implementación inicial.

   a. Seleccione Añadir detalles del host.

   b. Para el nombre de host DNS, introduzca el nombre de host del host.

   c. Para el tipo de instancia, elija el tipo de EC2 instancia.

d. Para la versión de host ESX, durante la creación del entorno se utilizará una versión de ESX predeterminada para la versión de VCF elegida. Para obtener más información, consulte the section called “Versiones e instancias de VCF EC2 ”.

> **Important**
>
> No detenga ni cancele EC2 las instancias que despliega Amazon EVS. Esta acción provoca la pérdida de datos.

> **Note**
>
> Amazon EVS solo admite EC2 instancias i4i.metal en este momento.

e. Para el par de claves SSH, elija un par de claves SSH para el acceso SSH al host.

f. Elija Agregar host.

6. En la página Configurar redes y conectividad, haga lo siguiente.

a. Para conocer los requisitos de conectividad del HCX, seleccione si desea utilizar el HCX con conectividad privada o a través de Internet.

b. Para la VPC, elija la VPC que creó anteriormente.

c. (Solo para la conectividad a Internet HCX) Para la ACL de red HCX, elija la ACL de red a la que se asociará su VLAN HCX.

> **Important**
>
> Le recomendamos encarecidamente que cree una ACL de red personalizada dedicada a la VLAN HCX. Para obtener más información, consulte the section called “Configure la ACL de red”.

d. En Subred de acceso al servicio, elija la subred privada que se creó al crear la VPC.

e. Para el grupo de seguridad (opcional), puede elegir hasta dos grupos de seguridad que controlen la comunicación entre el plano de control de Amazon EVS y la VPC. Amazon EVS utiliza el grupo de seguridad predeterminado si no se elige ningún grupo de seguridad.

> **Note**
>
> Asegúrese de que los grupos de seguridad que elija proporcionen conectividad a sus servidores DNS y a las subredes VLAN de Amazon EVS.

f. En Conectividad de administración, introduzca los bloques CIDR que se van a utilizar para las subredes de VLAN de Amazon EVS. Para el bloque CIDR de VLAN de enlace ascendente HCX, si configura una VLAN HCX pública, debe especificar un bloque CIDR con una longitud de máscara de red exacta de /28. Amazon EVS genera un error de validación si se especifica cualquier otro tamaño de bloque de CIDR para la VLAN HCX pública. Para una VLAN HCX privada y todos los demás bloques VLANs CIDR, la longitud mínima de la máscara de red que puede utilizar es /28 y la máxima es /24.

> **Important**
>
> Las subredes VLAN de Amazon EVS solo se pueden crear durante la creación del entorno de Amazon EVS y no se pueden modificar una vez creado el entorno. Debe asegurarse de que los bloques CIDR de la subred de la VLAN tengan el tamaño adecuado antes de crear el entorno. No podrá agregar subredes de VLAN después de implementar el entorno. Para obtener más información, consulte the section called “Consideraciones sobre las redes de Amazon EVS”.

g. En Expansión VLANs, introduzca los bloques CIDR para las subredes VLAN de Amazon EVS adicionales que se puedan utilizar para ampliar las capacidades de VCF en Amazon EVS, por ejemplo, para habilitar NSX Federation.

h. En Conectividad de carga de trabajo/VCF, introduzca el bloque CIDR para la VLAN de enlace superior de NSX y elija dos servidores de rutas de VPC homólogos IDs que se conecten a los puntos finales del servidor de rutas a través del enlace superior de NSX.

> **Note**
>
> Amazon EVS requiere una instancia de servidor de rutas de VPC que esté asociada a dos puntos de enlace del servidor de rutas y dos pares de servidores de rutas antes de la implementación del EVS. Esta configuración permite el enrutamiento dinámico basado en BGP a través del enlace superior de NSX. Para obtener más

información, consulte the section called “Configure una instancia de VPC Route Server con puntos finales y pares”.

i. Elija Siguiente.

7. En la página Especificar los nombres de host DNS de administración, haga lo siguiente.

   a. En los nombres de host DNS de los dispositivos de administración, introduzca los nombres de host DNS de las máquinas virtuales que alojarán los dispositivos de administración de VCF. Si utiliza Route 53 como proveedor de DNS, elija también la zona alojada que contiene sus registros de DNS.

   b. En Credenciales, elige si quieres usar la clave de KMS AWS administrada para Secrets Manager o una clave de KMS administrada por el cliente que proporciones. Esta clave se usa para cifrar las credenciales de VCF que se requieren para usar los dispositivos SDDC Manager, NSX Manager y vCenter.

   > **Note**
   >
   > Las claves KMS administradas por el cliente conllevan costes de uso. Para obtener más información, consulte la página de precios de AWS KMS.

   c. Elija Siguiente.

8. (Opcional) En la página Añadir etiquetas, añada las etiquetas que desee asignar a este entorno y seleccione Siguiente.

   > **Note**
   >
   > Los anfitriones creados como parte de este entorno recibirán la siguiente etiqueta:`DoNotDelete-EVS-<environmentid>-<hostname>`.

   > **Note**
   >
   > Las etiquetas asociadas al entorno de Amazon EVS no se propagan a AWS los recursos subyacentes, como EC2 las instancias. Puede crear etiquetas en AWS los recursos subyacentes mediante la consola de servicio correspondiente o la. AWS CLI

9. En la página Revisar y crear, revise la configuración y elija Crear entorno.

> **Important**
>
> Durante la implementación del entorno, Amazon EVS crea las subredes de VLAN de EVS y las asocia implícitamente a la tabla de enrutamiento principal. Una vez completada la implementación, debe asociar explícitamente las subredes de VLAN de Amazon EVS a una tabla de enrutamiento para fines de conectividad de NSX. Para obtener más información, consulte the section called “Asocie de forma explícita las subredes VLAN de Amazon EVS a una tabla de enrutamiento de VPC”.

> **Note**
>
> Amazon EVS implementa una versión empaquetada reciente de VMware Cloud Foundation que puede no incluir actualizaciones de productos individuales, conocidas como parches asíncronos. Una vez finalizada esta implementación, le recomendamos encarecidamente que revise y actualice los productos individuales mediante la herramienta de parches asíncronos (herramienta AP) de Broadcom o la automatización LCM integrada en el producto con SDDC Manager. Las actualizaciones de NSX deben realizarse fuera del SDDC Manager.

> **Note**
>
> La creación del entorno puede tardar varias horas.

AWS CLI

1. Abra una sesión de terminal.
2. Cree un entorno Amazon EVS. A continuación se muestra un ejemplo de `aws evs create-environment` solicitud.

> **Important**
>
> Antes de ejecutar el `aws evs create-environment` comando, compruebe que se cumplen todos los requisitos previos de Amazon EVS. La implementación del entorno

falla si no se cumplen los requisitos previos. Para obtener más información, consulte Configuración de Amazon Elastic VMware Service.

Important

Durante la implementación del entorno, Amazon EVS crea las subredes de VLAN de EVS y las asocia implícitamente a la tabla de enrutamiento principal. Una vez completada la implementación, debe asociar explícitamente las subredes de VLAN de Amazon EVS a una tabla de enrutamiento para fines de conectividad de NSX. Para obtener más información, consulte the section called “Asocie de forma explícita las subredes VLAN de Amazon EVS a una tabla de enrutamiento de VPC”.

Note

Amazon EVS implementa una versión empaquetada reciente de VMware Cloud Foundation que puede no incluir actualizaciones de productos individuales, conocidas como parches asíncronos. Una vez finalizada esta implementación, le recomendamos encarecidamente que revise y actualice los productos individuales mediante la herramienta de parches asíncronos (herramienta AP) de Broadcom o la automatización LCM integrada en el producto con SDDC Manager. Las actualizaciones de NSX deben realizarse fuera del SDDC Manager.

Note

La implementación del entorno puede tardar varias horas.

- Para `--vpc-id`, especifique la VPC que creó anteriormente con un rango de IPv4 CIDR mínimo de /22.
- Para `--service-access-subnet-id`, especifique el ID único de la subred privada que se creó al crear la VPC.
- Para `--vcf-version`, consulte las the section called “Versiones e instancias de VCF EC2 ” versiones de VCF proporcionadas por Amazon EVS,

- Con`--terms-accepted`, usted confirma que ha adquirido y seguirá manteniendo el número necesario de licencias de software VCF para cubrir todos los núcleos de procesadores físicos del entorno Amazon EVS. La información sobre el software VCF en Amazon EVS se compartirá con Broadcom para verificar el cumplimiento de la licencia.
- Para ello`--license-info`, introduzca la clave de solución de VCF (VMware vSphere 8 Enterprise Plus for VCF) y la clave de licencia de vSAN.

> **Note**
>
> La clave de la solución VCF debe tener al menos 256 núcleos. La clave de licencia de vSAN debe tener al menos 110 TiB de capacidad de vSAN.

> **Note**
>
> Amazon EVS requiere que mantenga una clave de solución de VCF y una clave de licencia de vSAN válidas en SDDC Manager para que el servicio funcione correctamente. Si administra estas claves de licencia mediante vSphere Client después de la implementación, debe asegurarse de que también aparezcan en la pantalla de licencias de la interfaz de usuario de SDDC Manager.

> **Note**
>
> La clave de solución de VCF y la clave de licencia de vSAN no se pueden utilizar en un entorno Amazon EVS existente.

- Para `--initial-vlans` especificar los rangos de CIDR para las subredes VLAN de Amazon EVS que Amazon EVS crea en su nombre. Se VLANs utilizan para implementar dispositivos de administración de VCF. Si configura una VLAN HCX pública, debe especificar un bloque CIDR con una longitud de máscara de red exacta de /28. Amazon EVS genera un error de validación si se especifica cualquier otro tamaño de bloque de CIDR para la VLAN HCX pública. Para una VLAN HCX privada y todos los demás bloques VLANs CIDR, la longitud mínima de la máscara de red que puede utilizar es /28 y la máxima es /24.
- `hcxNetworkAclId`se utiliza para configurar la conectividad a Internet del HCX. Especifique una ACL de red personalizada para la VLAN HCX pública.

> **Important**
>
> Le recomendamos encarecidamente que cree una ACL de red personalizada dedicada a la VLAN HCX. Para obtener más información, consulte the section called "Configure la ACL de red".

> **Important**
>
> Las subredes VLAN de Amazon EVS solo se pueden crear durante la creación del entorno de Amazon EVS y no se pueden modificar una vez creado el entorno. Debe asegurarse de que los bloques CIDR de la subred de la VLAN tengan el tamaño adecuado antes de crear el entorno. No podrá agregar subredes de VLAN después de implementar el entorno. Para obtener más información, consulte the section called "Consideraciones sobre las redes de Amazon EVS".

- Para `--hosts`, especifique los detalles de los hosts que Amazon EVS requiere para la implementación del entorno. Incluya el nombre de host DNS, el nombre de la clave EC2 SSH y el tipo de EC2 instancia para cada host. El ID de host dedicado es opcional.

> **Important**
>
> No detenga ni cancele EC2 las instancias que despliega Amazon EVS. Esta acción provoca la pérdida de datos.

> **Note**
>
> Amazon EVS solo admite EC2 instancias i4i.metal en este momento.

- Para `--connectivity-info`, especifique el par de 2 servidores de rutas de VPC IDs que creó en el paso anterior.

> **Note**
>
> Amazon EVS requiere una instancia de servidor de rutas de VPC que esté asociada a dos puntos de enlace del servidor de rutas y dos pares de servidores de rutas

antes de la implementación del EVS. Esta configuración permite el enrutamiento dinámico basado en BGP a través del enlace superior de NSX. Para obtener más información, consulte the section called “Configure una instancia de VPC Route Server con puntos finales y pares”.

- Para ello`--vcf-hostnames`, introduzca los nombres de host DNS de las máquinas virtuales que alojarán los dispositivos de administración VCF.
- Para`--site-id`, introduzca el ID único de su sitio de Broadcom. Este ID permite el acceso al portal de Broadcom y Broadcom se lo proporciona al cerrar el contrato de software o al renovar el contrato.
- (Opcional) Para`--region`, introduzca la región en la que se implementará su entorno. Si no se especifica la región, se utiliza la región predeterminada.

```
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
```

A continuación, se muestra una respuesta de ejemplo.

```
{
    "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"
        }
    }
}
```

Verificar la creación del entorno Amazon EVS

Example

Amazon EVS console

1. Ve a la consola Amazon EVS.
2. En el panel de navegación, elija Entornos.
3. Seleccione el entorno.
4. Seleccione la pestaña Detalles.
5. Compruebe que el estado del entorno esté aprobado y que el estado del entorno esté creado. Esto le permite saber que el entorno está listo para usarse.

> **Note**
>
> La creación del entorno puede tardar varias horas. Si el estado del entorno sigue siendo Creando, actualice la página.

AWS CLI

1. Abra una sesión de terminal.
2. Ejecute el siguiente comando, utilizando el ID de entorno de su entorno y el nombre de la región que contiene sus recursos. El entorno estará listo para usarse cuando lo `environmentState` esté`CREATED`.

> **Note**
>
> La creación del entorno puede tardar varias horas. Si `environmentState` sigue apareciendo`CREATING`, ejecute el comando de nuevo para actualizar el resultado.

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

A continuación, se muestra una respuesta de ejemplo.

```
{
    "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": []
    }
}
```

Asocie de forma explícita las subredes VLAN de Amazon EVS a una tabla de enrutamiento de VPC

Asocie de forma explícita cada una de las subredes de VLAN de Amazon EVS a una tabla de enrutamiento de la VPC. Esta tabla de enrutamiento se utiliza para permitir que AWS los recursos se comuniquen con máquinas virtuales en los segmentos de red de NSX que se ejecutan con Amazon EVS. Si ha creado una VLAN HCX pública, asegúrese de asociar explícitamente la subred HCX VLAN pública a una tabla de enrutamiento pública en su VPC que enrute a una puerta de enlace de Internet.

Example

Amazon VPC console

1. Ve a la consola de VPC.
2. En el panel de navegación, elija Tablas de enrutamiento.
3. Elija la tabla de enrutamiento que desee asociar a las subredes de VLAN de Amazon EVS.
4. Seleccione la pestaña Asociaciones de subredes.
5. En Asociaciones de subredes explícitas, seleccione Editar asociaciones de subredes.

6. Seleccione todas las subredes VLAN de Amazon EVS.
7. Seleccione Save associations (Guardar asociaciones).

AWS CLI

1. Abra una sesión de terminal.
2. Identifique la subred VLAN de Amazon EVS. IDs

```
aws ec2 describe-subnets
```

3. Asocie las subredes de VLAN de Amazon EVS a una tabla de enrutamiento en su VPC.

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

Asóciese EIPs a la subred de VLAN pública de HCX (para conectividad a Internet de HCX)

Siga estos pasos para asociar la dirección IP elástica (EIPs) del grupo de IPAM a la VLAN pública de HCX para la conectividad a Internet de HCX. Debe asociar al menos dos EIPs dispositivos para los dispositivos HCX Manager y HCX Interconnect (HCX-IX). Asocie un EIP adicional a cada dispositivo de red HCX que necesite implementar. Puede tener hasta 13 EIPs del grupo de IPAM asociado a la VLAN pública de HCX.

Important

La conectividad a Internet pública de HCX falla si no se asocian al menos dos EIPs del grupo de IPAM a una subred de VLAN pública de HCX.

Note

Amazon EVS solo admite la asociación EIPs con la VLAN HCX en este momento.

> **Note**
>
> No puede asociar las dos primeras EIPs ni las últimas EIP del bloque CIDR de IPAM público a la subred de la VLAN. EIPs Están reservadas como direcciones de red, puerta de enlace predeterminada y direcciones de transmisión. Amazon EVS arroja un error de validación si intenta EIPs asociarlos a la subred de VLAN.

Amazon EVS console

1. Ve a la consola Amazon EVS.
2. En el menú de navegación, selecciona Entornos.
3. Seleccione el entorno.
4. En la pestaña Redes y conectividad, seleccione la VLAN pública HCX.
5. Elija Asociar el EIP a la VLAN.
6. Seleccione las direcciones IP elásticas que desee asociar a la VLAN pública de HCX.
7. Elija Asociar EIPs.
8. Compruebe las asociaciones de EIP para confirmar que se EIPs han asociado a la VLAN pública de HCX.

AWS CLI

1. Para asociar una dirección IP elástica a una VLAN, utilice el comando example. `associate-eip-to-vlan`
   - `environment-id`- El ID de su entorno de Amazon EVS.
   - `vlan-name`- El nombre de la VLAN que se va a asociar a la dirección IP elástica.
   - `allocation-id`- El ID de asignación de la dirección IP elástica.

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

   El comando devuelve detalles sobre la VLAN, incluida la nueva asociación 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"
    }
}
```


La `eipAssociations` matriz muestra la nueva asociación, que incluye:

- `associationId`- El identificador único de esta asociación de EIP, que se utiliza para la disociación.
- `allocationId`- El ID de asignación de la dirección IP elástica asociada.
- `ipAddress`- La dirección IP asignada a la VLAN.

2. Repita el paso para asociar más. EIPs

Configure las tablas de rutas de las pasarelas de tránsito y los prefijos de Direct Connect para la conectividad local (opcional)

Si está configurando la conectividad de red local mediante Direct Connect una AWS Site-to-Site VPN con una puerta de enlace de tránsito, debe actualizar las tablas de rutas de la puerta de enlace de tránsito con la CIDRs VPC creada en el entorno de Amazon EVS. Para obtener más información, consulte las tablas de rutas de Transit Gateways en Amazon VPC Transit Gateways.

Si utiliza AWS Direct Connect, es posible que también deba actualizar los prefijos de Direct Connect para enviar y recibir rutas actualizadas desde la VPC. Para obtener más información, consulte Permite interacciones de prefijos para las puertas de enlace AWS Direct Connect.

Recupere las credenciales de VCF y acceda a los dispositivos de administración de VCF

Amazon EVS usa AWS Secrets Manager para crear, cifrar y almacenar los secretos gestionados en su cuenta. Estos secretos contienen las credenciales de VCF necesarias para instalar y acceder a los dispositivos de administración de VCF, como vCenter Server, NSX y SDDC Manager, así como la contraseña raíz de ESX. Para obtener más información sobre cómo recuperar secretos, consulte Obtener AWS secretos de Secrets Manager en la Guía del usuario de AWS Secrets Manager.

> **Note**
>
> Amazon EVS no ofrece una rotación administrada de los secretos. Recomendamos que se roten los secretos con regularidad en una ventana de rotación establecida para asegurar que los secretos no duren mucho.

Una vez que haya recuperado sus credenciales de VCF de AWS Secrets Manager, podrá utilizarlas para iniciar sesión en sus dispositivos de administración de VCF. Para obtener más información, consulte Iniciar sesión en la interfaz de usuario de SDDC Manager y Cómo usar y configurar vSphere Client en la documentación del producto. VMware

Configure la consola en EC2 serie (opcional)

De forma predeterminada, Amazon EVS habilita el ESX Shell en los hosts Amazon EVS recién implementados. Esta configuración permite el acceso al puerto serie de la EC2 instancia de Amazon a través de la consola EC2 serie, que puede utilizar para solucionar problemas de arranque, configuración de red y otros problemas. La consola serie no requiere que la instancia tenga ninguna capacidad de red. Con la consola en serie, puede introducir comandos en una EC2 instancia en ejecución como si el teclado y el monitor estuvieran conectados directamente al puerto serie de la instancia.

Se puede acceder a la consola EC2 serie mediante la EC2 consola o el AWS CLI. Para obtener más información, consulta EC2 Serial Console para instancias en la Guía del EC2 usuario de Amazon.

> **Note**
>
> La consola EC2 serie es el único mecanismo compatible con Amazon EVS para acceder a la interfaz de usuario de consola directa (DCUI) e interactuar con un host ESX de forma local.

> **Note**
>
> Amazon EVS desactiva el SSH remoto de forma predeterminada. Para obtener más información sobre cómo habilitar SSH para acceder al ESX Shell remoto, consulte Acceso remoto al ESX Shell con SSH en la documentación del producto VMware vSphere.

Conéctese a la consola EC2 serie

Para conectarse a la consola EC2 en serie y utilizar la herramienta que elija para la solución de problemas, debe completar algunas tareas previas. Para obtener más información, consulte Requisitos previos para la consola EC2 serie y Connect to the EC2 Serial Console en la Guía del EC2 usuario de Amazon.

> **Note**
>
> Para conectarse a la consola EC2 en serie, el estado de la EC2 instancia debe ser`running`. No puedes conectarte a la consola en serie si la instancia está en el `terminated` estado `pending` `stopping``stopped`,`shutting-down`,, o. Para obtener más información sobre los cambios de estado de las instancias, consulta los cambios de estado de las EC2 instancias de Amazon en la Guía del EC2 usuario de Amazon.

Configure el acceso a la consola EC2 serie

Para configurar el acceso a la consola EC2 en serie, usted o su administrador deben conceder el acceso a la consola en serie a nivel de cuenta y, a continuación, configurar las políticas de IAM para conceder el acceso a sus usuarios. En el caso de las instancias de Linux, también debe configurar un usuario basado en una contraseña en cada instancia para que los usuarios puedan utilizar la consola en serie para solucionar problemas. Para obtener más información, consulte Configurar el acceso a la consola EC2 serie en la Guía del EC2 usuario de Amazon.

Limpieza

Siga estos pasos para eliminar los AWS recursos que se crearon.

Eliminar los hosts y el entorno de Amazon EVS

Siga estos pasos para eliminar los hosts y el entorno de Amazon EVS. Esta acción elimina la instalación de VMware VCF que se ejecuta en su entorno Amazon EVS.

> **Note**
>
> Para eliminar un entorno de Amazon EVS, primero debe eliminar todos los hosts del entorno. No se puede eliminar un entorno si hay hosts asociados al entorno.

Example

Amazon EVS console

1. Ve a la consola Amazon EVS.
2. En el panel de navegación, elija Entorno.
3. Seleccione el entorno que contiene los hosts que desee eliminar.
4. Seleccione la pestaña Hosts.
5. Seleccione el anfitrión y elija Eliminar en la pestaña Hosts. Repita este paso para cada host del entorno.
6. En la parte superior de la página Entornos, elija Eliminar y, a continuación, Eliminar entorno.

   > **Note**
   >
   > La eliminación del entorno también elimina las subredes de VLAN de Amazon EVS y los secretos de Secrets Manager AWS que creó Amazon EVS. AWS los recursos que cree no se eliminan. Es posible que estos recursos sigan incurriendo en costes.

7. Si tienes reservas EC2 de Amazon Capacity que ya no necesitas, asegúrate de cancelarlas. Para obtener más información, consulta Cancelar una reserva de capacidad en la Guía del EC2 usuario de Amazon.

AWS CLI

1. Abra una sesión de terminal.
2. Identifique el entorno que contiene el host que desea eliminar.

```
aws evs list-environments
```

A continuación, se muestra una respuesta de ejemplo.

```
{
    "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. Elimine los hosts del entorno. A continuación se muestra un ejemplo de `aws evs delete-environment-host` solicitud.

> **Note**
>
> Para poder eliminar un entorno, primero debe eliminar todos los hosts contenidos en el entorno.

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

4. Repita los pasos anteriores para eliminar los hosts restantes del entorno.
5. Elimine el entorno.

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

> **Note**
>
> La eliminación del entorno también elimina las subredes de VLAN de Amazon EVS y los secretos de Secrets Manager AWS que creó Amazon EVS. AWS Los demás recursos que cree no se eliminan. Es posible que estos recursos sigan incurriendo en costes.

6. Si tienes reservas EC2 de Amazon Capacity que ya no necesitas, asegúrate de cancelarlas. Para obtener más información, consulta Cancelar una reserva de capacidad en la Guía del EC2 usuario de Amazon.

Elimine los recursos de IPAM (para la conectividad a Internet HCX)

Si ha configurado la conectividad a Internet de HCX, siga estos pasos para eliminar sus recursos de IPAM.

1. Libera las asignaciones de EIP del grupo público de IPAM. Para obtener más información, consulte Publicar una asignación en la Guía del usuario del administrador de direcciones IP de VPC.
2. Desaprovisione el IPv4 CIDR público del grupo de IPAM. Para obtener más información, consulte Desaprovisionar CIDRs de un grupo en la Guía del usuario del administrador de direcciones IP de VPC.
3. Elimine el grupo de IPAM público. Para obtener más información, consulte Eliminar un grupo en la Guía del usuario del administrador de direcciones IP de VPC.
4. Elimine el IPAM. Para obtener más información, consulte Eliminar un IPAM en la Guía del usuario del administrador de direcciones IP de VPC.

Eliminar los componentes del servidor de rutas de VPC

Para conocer los pasos para eliminar los componentes del servidor de rutas de Amazon VPC que ha creado, consulte la limpieza del servidor de rutas en la Guía del usuario de Amazon VPC.

Elimine la lista de control de acceso a la red (ACL)

Para ver los pasos para eliminar una lista de control de acceso a la red, consulte Eliminar una ACL de red para su VPC en la Guía del usuario de Amazon VPC.

Desasocie y elimine las tablas de enrutamiento de subred

Para ver los pasos para desasociar y eliminar las tablas de enrutamiento de subred, consulte las tablas de enrutamiento de subred en la Guía del usuario de Amazon VPC.

Elimine las subredes

Elimine las subredes de VPC, incluida la subred de acceso al servicio. Para ver los pasos para eliminar subredes de VPC, consulte Eliminar una subred en la Guía del usuario de Amazon VPC.

> **Note**
>
> Si usa Route 53 para DNS, elimine los puntos finales entrantes antes de intentar eliminar la subred de acceso al servicio. De lo contrario, no podrá eliminar la subred de acceso al servicio.

> **Note**
>
> Amazon EVS elimina las subredes de VLAN en su nombre cuando se elimina el entorno. Las subredes VLAN de Amazon EVS solo se pueden eliminar cuando se elimina el entorno.

Elimine la VPC

Para ver los pasos para eliminar la VPC, consulte Eliminar la VPC en la Guía del usuario de Amazon VPC.

Siguientes pasos

Migre sus cargas de trabajo a Amazon EVS mediante VMware Hybrid Cloud Extension (VMware HCX). Para obtener más información, consulte Migración.

Migre las cargas de trabajo a Amazon EVS mediante HCX VMware

Después de implementar Amazon EVS, puede implementar VMware HCX con conectividad a Internet pública o privada para facilitar la migración de las cargas de trabajo a Amazon EVS. Para obtener más información, consulte Introducción a VMware HCX en la Guía del usuario de HCX. VMware

Important

Por lo general, no se recomienda la migración de HCX basada en Internet para:

- Aplicaciones sensibles a las fluctuaciones o la latencia de la red.
- Operaciones de vMotion en las que el tiempo es crítico.
- Migraciones a gran escala con requisitos de rendimiento estrictos.

Para estos escenarios, recomendamos utilizar la conectividad privada HCX. Una conexión privada dedicada ofrece un rendimiento más fiable en comparación con las conexiones basadas en Internet.

Opciones de conectividad HCX

Puede migrar las cargas de trabajo a Amazon EVS mediante conectividad privada con AWS Direct Connect o conexión Site-to-Site VPN, o mediante conectividad pública.

Según su situación y sus opciones de conectividad, es posible que prefiera utilizar la conectividad pública o privada con HCX. Por ejemplo, algunos sitios pueden tener conectividad privada con una mayor uniformidad de rendimiento, pero un rendimiento inferior debido al cifrado de la VPN o a las velocidades de enlace limitadas. Del mismo modo, es posible que tengas una conectividad a Internet pública de alto rendimiento que tenga una mayor variación en el rendimiento. Con Amazon EVS, puede elegir la opción de conectividad que mejor se adapte a sus necesidades.

En la siguiente tabla se comparan las diferencias entre la conectividad pública y privada de HCX.

Conectividad privada	Conectividad pública
Información general	Información general
Utiliza solo conexiones privadas dentro de la VPC. Opcionalmente, puede usar AWS Direct Connect o Site-to-Site VPN con una puerta de enlace de tránsito para la conectividad de red externa.	Utiliza conectividad pública a Internet con direcciones IP elásticas, lo que permite las migraciones sin una conexión privada dedicada.
Ideal para	El más adecuado para
• Operaciones de vMotion urgentes. • Migraciones a gran escala. • Aplicaciones sensibles a la latencia o a la fluctuación. • Transferencias de datos de gran volumen. • Organizaciones con AWS Direct AWS Site-to-Site Connect/VPN existentes.	• Ubicaciones sin conexión AWS AWS Site-to-Site directa/VPN. • Proyectos sensibles a los costos.
Ventajas principales	Ventajas principales
• Conectividad uniforme de baja latencia. • Asignación de ancho de banda dedicado. • Rendimiento de red más fiable. • El cifrado HCX predeterminado se puede desactivar en los entornos privados para optimizar el rendimiento. • No se requiere una administración de IP pública.	• Configuración más rápida que la conectividad privada. • Rentable para migraciones más pequeñas.
Consideraciones clave	Consideraciones clave
• Configuración inicial más compleja. • Costes de infraestructura iniciales más altos. • Plazo de implementación más prolongado.	• Rendimiento de red más variable. • Es posible que haya limitaciones de ancho de banda.

Conectividad privada	Conectividad pública
• No hay conectividad directa a Internet para ningún componente del HCX.	• Mayor latencia que la conectividad privada. • Cada componente requiere una dirección IP elástica dedicada asignada desde el grupo de IPAM público. • Las asociaciones EIP permiten la conectividad directa a Internet para cada componente del HCX.

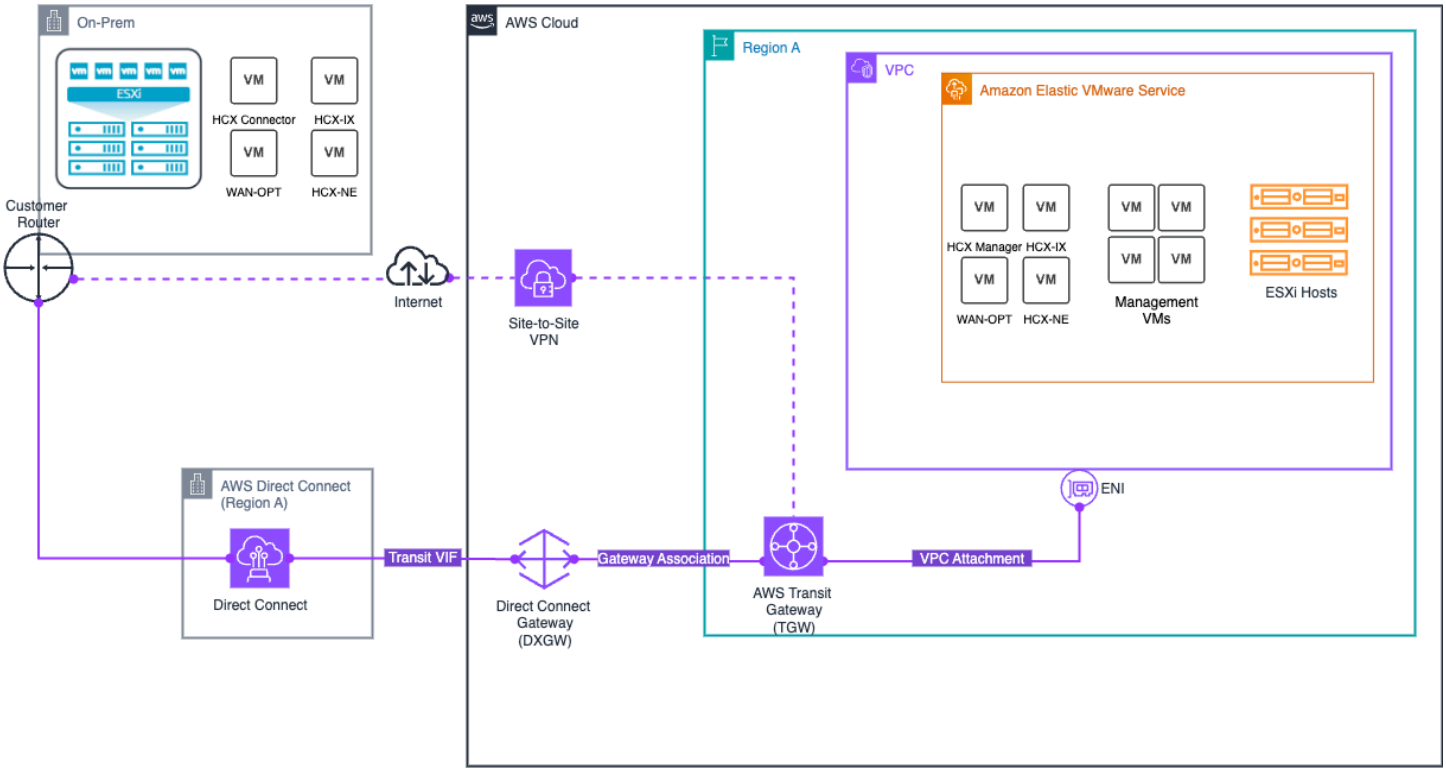
Arquitectura de conectividad privada HCX

La solución de conectividad privada HCX integra varios componentes:

- Componentes de red Amazon EVS
  - Utiliza únicamente subredes de VLAN privadas para una comunicación segura, incluida una VLAN HCX privada.
  - Soporta redes ACLs para el control del tráfico.
  - Admite la propagación dinámica de rutas BGP a través de un servidor de rutas de VPC privado.
- AWS opciones de tránsito de red gestionadas para la conectividad local
  - AWS Direct Connect + AWS Transit Gateway le permite conectar su red local a Amazon EVS a través de una conexión privada dedicada. Para obtener más información, consulte AWS Direct Connect + AWS Transit Gateway.
  - AWS Site-to-Site VPN + AWS Transit Gateway ofrece la opción de crear una conexión IPsec VPN entre su red remota y la pasarela de tránsito a través de Internet. Para obtener más información, consulte AWS Transit Gateway + AWS Site-to-Site VPN.

> **Note**
>
> Amazon EVS no admite la conectividad a través de una interfaz virtual privada (VIF) de AWS Direct Connect ni a través de una conexión AWS Site-to-Site VPN que termine directamente en la VPC subyacente.

El siguiente diagrama ilustra la arquitectura de conectividad privada de HCX y muestra cómo puede usar AWS Direct Connect y Site-to-Site VPN con la puerta de enlace de tránsito para permitir la migración segura de la carga de trabajo a través de una conexión privada dedicada.



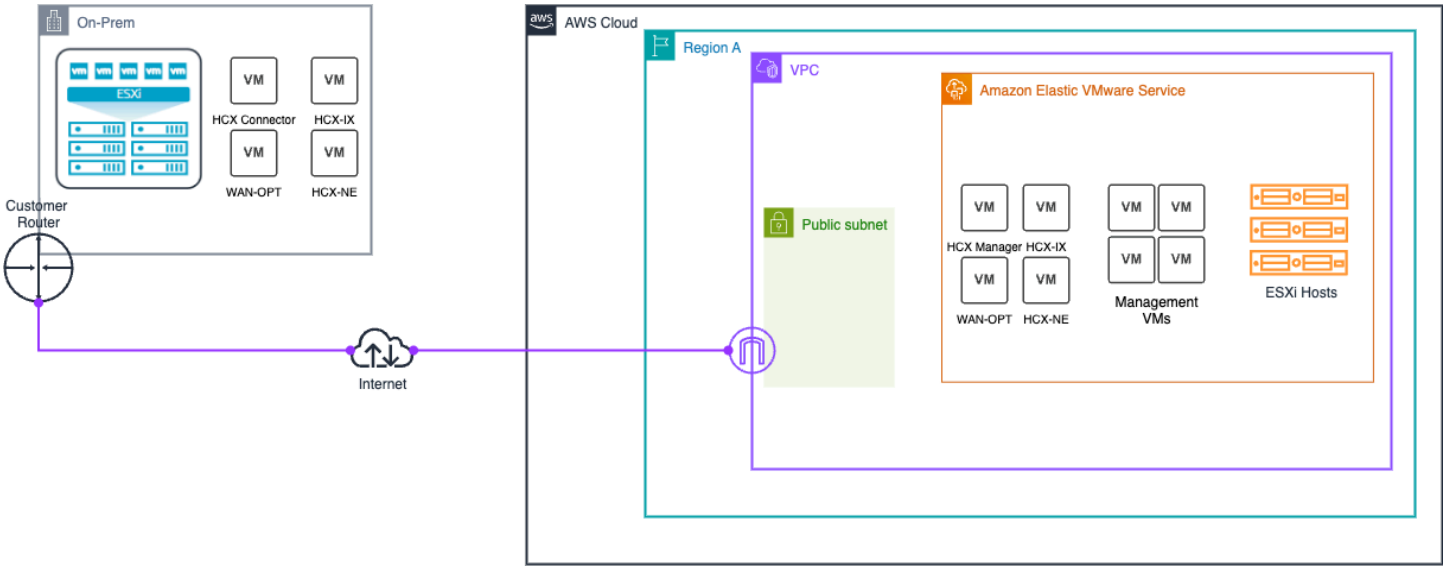
Arquitectura de conectividad a Internet HCX

La solución de conectividad a Internet de HCX consta de varios componentes que funcionan juntos:

- Componentes de red Amazon EVS
  - Utiliza una subred HCX VLAN pública aislada para permitir la conectividad a Internet entre Amazon EVS y sus dispositivos HCX locales.
  - ACLs Admite la red para el control del tráfico.
  - Admite la propagación dinámica de rutas BGP a través de un servidor de rutas de VPC público.
- Administración de IPAM e IP pública
  - El administrador de direcciones IP (IPAM) de Amazon VPC administra la asignación de IPv4 direcciones públicas desde el grupo de IPAM públicas propiedad de Amazon.
  - El bloque CIDR de VPC secundario (/28) se asigna desde el grupo de IPAM, lo que crea una subred pública aislada separada del CIDR de VPC principal.

Para obtener más información, consulte the section called “Conectividad pública HCX”.

El siguiente diagrama ilustra la arquitectura de conectividad a Internet de HCX.



Configuración de migración a HCX

En este tutorial se describe cómo configurar VMware HCX para migrar sus cargas de trabajo a Amazon EVS.

Requisitos previos

Antes de usar VMware HCX con Amazon EVS, asegúrese de que se cumplen los requisitos previos de HCX. Para obtener más información, consulte the section called “VMware Requisitos previos de HCX”.

> **Important**
>
> Amazon EVS tiene requisitos exclusivos para la conectividad a Internet pública de HCX. Si necesita conectividad pública HCX, debe cumplir los siguientes requisitos:
>
> - Cree un IPAM y un grupo de IPv4 IPAM público con un CIDR que tenga una longitud mínima de máscara de red de /28.
> - Asigne al menos dos direcciones IP elásticas (EIPs) del grupo de IPAM para los dispositivos HCX Manager y HCX Interconnect (HCX-IX). Asigne una dirección IP elástica adicional para cada dispositivo de red HCX que necesite implementar.
> - Añada el bloque IPv4 CIDR público como CIDR adicional a su VPC.

Para obtener más información, consulte the section called “Configuración de conectividad a Internet del HCX”.

Compruebe el estado de la subred VLAN HCX

Se crea una VLAN para HCX como parte de la implementación estándar de Amazon EVS. Siga estos pasos para comprobar que la subred VLAN de HCX esté configurada correctamente.

Example

Amazon EVS console

1. Ve a la consola Amazon EVS.
2. En el panel de navegación, elija Entornos.
3. Seleccione el entorno Amazon EVS.
4. Seleccione la pestaña Redes y conectividad.
5. En VLANs, identifique la VLAN HCX y compruebe que el estado es creado y el de público es verdadero.

AWS CLI

1. Ejecute el siguiente comando, utilizando el ID de entorno de su entorno y el nombre de la región que contiene sus recursos.

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

2. En el resultado de la respuesta, identifique la VLAN con un `functionName` de `hcx` y compruebe que `vlanState` es `CREATED` y `isPublic` está configurada en. `true` A continuación, se muestra una respuesta de ejemplo.

```
{
    "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
        }
    ]
}
```


Compruebe que la subred VLAN HCX esté asociada a una ACL de red

Siga estos pasos para comprobar que la subred VLAN HCX esté asociada a una ACL de red. Para obtener más información sobre la asociación de ACL de red, consulte. the section called “Cree una ACL de red para controlar el tráfico de subred de VLAN de Amazon EVS”

> **Important**
>
> Si se conecta a través de Internet, la asociación de una dirección IP elástica a una VLAN proporciona acceso directo a Internet a todos los recursos de esa VLAN. Asegúrese de tener las listas de control de acceso a la red adecuadas configuradas para restringir el acceso según sea necesario según sus requisitos de seguridad.

> **Important**
>
> EC2 los grupos de seguridad no funcionan en las interfaces de red elásticas que están conectadas a las subredes de VLAN de Amazon EVS. Para controlar el tráfico hacia y desde las subredes VLAN de Amazon EVS, debe utilizar una lista de control de acceso a la red (ACL).

Example

Amazon VPC console

1. Vaya a la consola. Amazon VPC
2. En el panel de navegación, selecciona Red ACLs.
3. Seleccione la ACL de red a la que están asociadas las subredes de la VLAN.
4. Seleccione la pestaña Asociaciones de subredes.
5. Compruebe que la subred VLAN HCX aparezca entre las subredes asociadas.

AWS CLI

1. Ejecute el siguiente comando utilizando el ID de subred VLAN HCX del filtro. `Values`

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

2. Compruebe que en la respuesta se devuelva la ACL de red correcta.

Compruebe que las subredes VLAN de EVS estén asociadas explícitamente a una tabla de enrutamiento

Amazon EVS requiere que todas las subredes de VLAN de EVS estén asociadas de forma explícita a una tabla de enrutamiento de la VPC. Para la conectividad a Internet de HCX, su subred de VLAN pública de HCX debe estar asociada explícitamente a una tabla de enrutamiento pública en su VPC que se enrute a una puerta de enlace de Internet. Siga estos pasos para comprobar la asociación explícita de la tabla de enrutamiento.

Example

Amazon VPC console

1. Ve a la consola de VPC.
2. En el panel de navegación, elija Tablas de enrutamiento.
3. Elija la tabla de enrutamiento a la que deben asociarse explícitamente las subredes de VLAN de EVS.
4. Seleccione la pestaña Asociaciones de subredes.
5. En Asociaciones de subredes explícitas, compruebe que aparezcan todas las subredes de VLAN de EVS. Si una subred de VLAN no aparece aquí, la subred de VLAN está asociada implícitamente a la tabla de rutas principal. Para que Amazon EVS funcione correctamente, debe asociar de forma explícita todas las subredes de VLAN a una tabla de enrutamiento. Para la subred de VLAN pública de HCX, debe tener una tabla de enrutamiento pública asociada con una puerta de enlace a Internet como destino. Para solucionar este problema, elija Editar asociaciones de subredes y añada las subredes de VLAN que faltan.

AWS CLI

1. Abra una sesión de terminal.
2. Ejecute el siguiente comando de ejemplo para recuperar detalles sobre todas las subredes de VLAN de EVS, incluida la asociación de la tabla de rutas. Si una subred de VLAN no aparece aquí, la subred de VLAN está asociada implícitamente a la tabla de enrutamiento principal. Para que Amazon EVS funcione correctamente, debe asociar de forma explícita todas las subredes de VLAN a una tabla de enrutamiento. Para la subred de VLAN pública de HCX, debe tener una tabla de enrutamiento pública asociada con una puerta de enlace a Internet como destino.

```
aws ec2 describe-subnets
```

3. Asocie de forma explícita las subredes de VLAN de EVS a una tabla de enrutamiento en su VPC. A continuación, se muestra un comando de ejemplo.

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

(Para la conectividad a Internet del HCX) Compruebe que EIPs estén asociados a la subred VLAN del HCX

Para cada dispositivo de red HCX que implemente, debe tener una EIP del grupo de IPAM asociada a una subred de VLAN pública de HCX. Debe asociar al menos dos EIPs a la subred de VLAN pública de HCX para los dispositivos HCX Manager y HCX Interconnect (HCX-IX). Siga estos pasos para comprobar que existen las asociaciones de EIP necesarias.

Important

La conectividad a Internet pública de HCX falla si no se asocian al menos dos EIPs del grupo de IPAM a una subred de VLAN pública de HCX.

Note

No puede asociar las dos primeras EIPs ni las últimas EIP del bloque CIDR de IPAM público a una subred de VLAN. EIPs Están reservadas como direcciones de red, puerta de enlace predeterminada y direcciones de transmisión. Amazon EVS arroja un error de validación si intenta EIPs asociarlos a una subred de VLAN.

Example

Amazon EVS console

1. Ve a la consola Amazon EVS.
2. En el menú de navegación, selecciona Entornos.

3. Seleccione el entorno.
4. En la pestaña Redes y conectividad, seleccione la VLAN pública HCX.
5. Consulte la pestaña de asociaciones de EIP para confirmar que se EIPs han asociado a la VLAN pública de HCX.

AWS CLI

1. Para comprobar cuáles EIPs están asociadas a la subred de la VLAN HCX, utilice el comando. `list-environment-vlans` Para ello`environment-id`, utilice el identificador único del entorno EVS que contiene la VLAN HCX.

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

El comando devuelve detalles sobre sus asociaciones de EIP VLANs, incluidas las siguientes:

```
{
  "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"
    },
    ...
  ]
}
```

La `eipAssociations` matriz muestra la asociación EIP, que incluye:

- `associationId`- El identificador único de esta asociación de EIP.
- `allocationId`- El ID de asignación de la dirección IP elástica asociada.
- `ipAddress`- La dirección IP asignada a la VLAN.

Cree un grupo de puertos distribuidos con el ID de VLAN de enlace ascendente público de HCX

Vaya a la interfaz de vSphere Client y siga los pasos que se indican en Agregar un grupo de puertos distribuidos para agregar un grupo de puertos distribuidos a un conmutador distribuido de vSphere.

Al configurar la conmutación por recuperación en la interfaz de vSphere Client, asegúrese de que uplink1 sea un enlace superior activo y uplink2 sea un enlace superior en espera para habilitar la conmutación por error. Active/Standby Para la configuración de VLAN en la interfaz de vSphere Client, introduzca el ID de VLAN de HCX que identificó anteriormente.

(Opcional) Configure la optimización WAN de HCX

> **Note**
>
> La función de optimización de WAN ya no está disponible en HCX 4.11.3. Para obtener más información, consulte las notas de la versión HCX 4.11.3.

El servicio de optimización de WAN de HCX (HCX-WO) mejora las características de rendimiento de las líneas privadas o las rutas de Internet mediante la aplicación de técnicas de optimización de

la WAN, como la reducción de datos y el acondicionamiento de las rutas de la WAN. El servicio de optimización WAN de HCX se recomienda en las implementaciones que no pueden dedicar rutas de 10 Gb a las migraciones. En las implementaciones de 10 Gb y baja latencia, es posible que el uso de la optimización de WAN no produzca un mejor rendimiento de migración. Para obtener más información, consulte Consideraciones y prácticas recomendadas sobre la implementación de VMware HCX.

El servicio de optimización de WAN de HCX se implementa junto con el dispositivo de servicio de interconexión WAN de HCX (HCX-IX). HCX-IX es responsable de la replicación de datos entre el entorno empresarial y el entorno Amazon EVS.

Para utilizar el servicio de optimización WAN de HCX con Amazon EVS, debe utilizar un grupo de puertos distribuidos en la subred de VLAN de HCX. Utilice el grupo de puertos distribuidos que se creó en el paso anterior.

(Opcional) Habilite la red optimizada para HCX Mobility

La red optimizada para movilidad (MON) de HCX es una función del servicio de extensión de red HCX. Las extensiones de red habilitadas para MON mejoran los flujos de tráfico de las máquinas virtuales migradas al permitir el enrutamiento selectivo dentro de su entorno Amazon EVS. MON le permite configurar la ruta óptima para migrar el tráfico de carga de trabajo a Amazon EVS al ampliar las redes de capa 2, lo que evita una ruta de red larga de ida y vuelta a través de la puerta de enlace de origen. Esta función está disponible para todas las implementaciones de Amazon EVS. Para obtener más información, consulte Configuración de redes optimizadas para movilidad en la Guía del usuario de VMware HCX.

> **Important**
>
> Antes de activar HCX MON, lea las siguientes limitaciones y configuraciones no compatibles con la extensión de red HCX.
> Restricciones y limitaciones de la extensión de red
> Restricciones y limitaciones de las topologías de redes optimizadas para la movilidad

> **Important**
>
> Antes de habilitar HCX MON, asegúrese de haber configurado la redistribución de rutas para el CIDR de la red de destino en la interfaz NSX. Para obtener más información, consulte Configurar el BGP y la redistribución de rutas en la documentación de NSX. VMware

Compruebe la conectividad de HCX

VMware El HCX incluye herramientas de diagnóstico integradas que se pueden utilizar para probar la conectividad. Para obtener más información, consulte Solución de problemas del VMware HCX en la Guía del usuario del VMware HCX.

Configurar la conectividad a Internet pública de HCX

Puede configurar el acceso público a Internet para su VLAN pública HCX asociando direcciones IP elásticas a su VLAN. Esto permite la conectividad directa a Internet para los dispositivos VMware HCX y las cargas de trabajo que requieren acceso a Internet para las operaciones de migración.

Temas relacionados

Este tema trata sobre la administración del acceso a Internet para la VLAN pública HCX. Para una implementación completa:

1. Complete los requisitos previos enConfiguración de Amazon Elastic VMware Service.
2. Configure la configuración inicial enIntroducción.
3. Configurar el acceso a Internet (este tema).

Acerca del acceso a Internet mediante VLAN HCX

Puede configurar el acceso a Internet para los dispositivos VMware HCX, lo que le permitirá realizar la migración HCX de sus cargas de trabajo a Amazon EVS a través de Internet.

Este enfoque:

- Permite migraciones de máquinas virtuales sin necesidad de conectividad privada dedicada.

- Proporciona una solución flexible y rentable para la migración.

> **Important**
>
> Por lo general, no se recomienda la migración a HCX basada en Internet para:
>
> - Aplicaciones sensibles a las fluctuaciones o la latencia de la red.
> - Operaciones de vMotion en las que el tiempo es crítico.
> - Migraciones a gran escala con requisitos de rendimiento estrictos.
>
> Para estos escenarios, recomendamos utilizar la conectividad privada HCX. Una conexión privada dedicada ofrece un rendimiento más fiable en comparación con las conexiones basadas en Internet.

Descripción general de la conectividad a Internet

Revise las siguientes consideraciones.

Requisitos de red HCX y DNAT

HCX tiene restricciones de red específicas que afectan a la forma de configurar el acceso público a Internet.

HCX no admite la traducción de direcciones de red de destino (DNAT). En su lugar, HCX requiere que la red de enlace ascendente sea enrutable con una dirección IP de puerta de enlace predeterminada.

Las subredes VLAN de Amazon EVS incluyen una dirección IP de puerta de enlace predeterminada, al igual que otras subredes de VPC. Sin embargo, estas subredes son siempre subredes privadas, incluso cuando se utilizan bloques CIDR fuera del rango de direcciones. RFC1918

Habilitar la conectividad a Internet HCX

Para habilitar la conectividad a Internet sin DNAT, Amazon EVS utiliza un enfoque de configuración CIDR específico:

- Requisito de CIDR enrutable por Internet: Amazon EVS requiere un CIDR enrutable por Internet que coincida con el CIDR de la subred de VLAN HCX.

- Asignación de IPAM: Amazon EVS utiliza un CIDR público asignado a IPAM con una longitud mínima de máscara de red de /28 como CIDR enrutable por Internet.
- Configuración de VPC: debe agregar manualmente el CIDR público asignado a IPAM a su VPC como CIDR de VPC secundario.
- Implementación de subredes de VLAN: una vez configuradas la IPAM y la VPC, puede utilizar el CIDR público asignado a IPAM en la subred de VLAN de HCX durante la implementación de Amazon EVS.
- Configuración de IP elástica: Amazon EVS requiere la siguiente configuración:
  - Asignar Elastic IPs: se asigna Elastic IPs desde el CIDR asignado por el IPAM. Debe asignar al menos dos direcciones IP elásticas (EIPs) del grupo de IPAM para los dispositivos HCX Manager y HCX Interconnect (HCX-IX). Asigne una dirección IP elástica adicional para cada dispositivo de red HCX que necesite implementar.
  - Asociar con la VLAN: asocie cada IP elástica que desee utilizar con un dispositivo HCX a la subred de la VLAN HCX. Utilice la consola Amazon EVS o AWS CLI para esta asociación.
  - Configure la dirección de la puerta de enlace: la primera dirección utilizable del CIDR se convierte en la dirección de la puerta de enlace que configure en el dispositivo HCX.
  - Enrutamiento del tráfico: el tráfico de cada Elastic IP asociada se enruta directamente al dispositivo HCX de destino con la misma dirección IP, sin DNAT.

Para conocer los pasos para configurar HCX con conectividad a Internet para la implementación del entorno Amazon EVS, consulte Configuración de Amazon Elastic VMware Service y. Introducción

Consideraciones de operación

- El bloque CIDR de la VLAN pública HCX debe tener una longitud de máscara de red de /28.
- EIPs pueden asociarse o disociarse de la VLAN pública de HCX después de la implementación mediante la consola Amazon EVS o AWS CLI, pero deben ser del mismo grupo de IPAM.
- Cada asociación de EIP tiene su propio ID de asociación único.
- Puede tener hasta 13 EIPs de un grupo de IPAM público asociado a la VLAN pública /28 HCX. No puede asociar las dos primeras EIPs ni las últimas EIP del bloque CIDR público asignado al IPAM a la subred de VLAN pública de HCX. EIPs Están reservadas como direcciones de red, puerta de enlace predeterminada y direcciones de transmisión. Amazon EVS arroja un error de validación si intenta EIPs asociarlos a la VLAN.

Consideraciones de seguridad

- Las listas de control de acceso a la red (ACLs) siguen aplicándose al tráfico que fluye a través de la subred de VLAN pública de HCX.
- Las reglas de los grupos de seguridad no se aplican al tráfico en las subredes de VLAN públicas de HCX. Utilice la red ACLs para controlar el tráfico.

> **Important**
>
> Si se conecta a través de Internet, la asociación de una dirección IP elástica a una VLAN proporciona acceso directo a Internet a todos los recursos de esa VLAN. Asegúrese de tener las listas de control de acceso a la red adecuadas configuradas para restringir el acceso según sea necesario según sus requisitos de seguridad.

Administrar direcciones IP elásticas para VLANs

Puede asociar y desasociar direcciones IP elásticas a una VLAN pública de HCX mediante la consola Amazon EVS o. AWS CLI

> **Note**
>
> Por el momento, Amazon EVS solo admite la asociación y desasociación de direcciones IP elásticas con una VLAN pública de HCX.

Asocie una dirección IP elástica a una VLAN

Requisitos previos

Asegúrese de tener lo siguiente:

- La dirección IP elástica se asigna desde el grupo de IPAM público propiedad de Amazon.
- El entorno Amazon EVS ya está creado.

Example

Amazon EVS console

1. Ve a la consola Amazon EVS.
2. En el menú de navegación, selecciona Entornos.
3. Seleccione el entorno.
4. En la pestaña Redes y conectividad, seleccione la VLAN pública HCX.

> **Note**
>
> Amazon EVS solo admite la asociación EIPs con la VLAN HCX en este momento.

5. Elija Asociar el EIP a la VLAN.
6. Seleccione las direcciones IP elásticas que desee asociar a la VLAN pública de HCX.
7. Elija Asociar EIPs. Puede tener hasta 13 EIPs asociadas a la VLAN pública de HCX.

> **Note**
>
> No puede asociar las dos primeras del bloque CIDR EIPs de IPAM público a la subred de la VLAN. EIPs Están reservadas como direcciones de red y de puerta de enlace predeterminadas.

8. Compruebe las asociaciones de EIP para confirmar que se EIPs han asociado a la VLAN pública de HCX.

AWS CLI

1. Para asociar una dirección IP elástica a una VLAN, utilice el comando example. `associate-eip-to-vlan`
   - `environment-id`- El ID de su entorno de Amazon EVS.
   - `vlan-name`- Debe serlo. `hcx` Por el momento, Amazon EVS solo admite la asociación de EIP con la VLAN HCX.
   - `allocation-id`- El ID de asignación de la dirección IP elástica.

```
aws evs associate-eip-to-vlan \
  --environment-id "env-605uove256" \
```

```
  --vlan-name "hcx" \
  --allocation-id "eipalloc-0429268f30c4a34f7"
```

El comando devuelve detalles sobre la VLAN, incluida la nueva asociación 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"
    }
}
```


La `eipAssociations` matriz muestra la nueva asociación, que incluye:

- `associationId`- El identificador único de esta asociación de EIP, que se utiliza para la disociación.
- `allocationId`- El ID de asignación de la dirección IP elástica asociada.
- `ipAddress`- La dirección IP asignada a la VLAN.

2. Repita el paso para asociar más. EIPs Puede tener hasta 13 EIPs asociadas a la VLAN pública HCX.

Desasocie una dirección IP elástica de una VLAN

Requisitos previos

Asegúrese de tener lo siguiente:

- El entorno Amazon EVS ya está creado.
- La EIP está asociada al entorno Amazon EVS.

Example

Amazon EVS console

1. Ve a la consola Amazon EVS.
2. En el menú de navegación, selecciona Entornos.
3. Seleccione el entorno.
4. En la pestaña Redes y conectividad, seleccione la VLAN pública HCX.
5. Elija Desasociar el EIP de la VLAN.
6. Seleccione las direcciones IP elásticas que desee desasociar de la VLAN pública de HCX.

> **Important**
>
> La disociación EIPs puede provocar una pérdida de conectividad a Internet en los dispositivos que utilizan subredes de VLAN públicas.

7. Elija Desasociar EIPs.
8. Compruebe las asociaciones de EIP para confirmar que se EIPs han disociado de la VLAN pública de HCX.

AWS CLI

Para desasociar una dirección IP elástica de una VLAN, utilice el comando example. `disassociate-eip-from-vlan`

- `environment-id`- El ID de su entorno de Amazon EVS.
- `vlan-name`- Debe serlo. `hcx` Por el momento, Amazon EVS solo admite la asociación de EIP con la VLAN HCX.

- `association-id`- El ID de asociación de la asociación EIP que se va a eliminar.

> **Important**
>
> La disociación EIPs puede provocar una pérdida de conectividad a Internet en los dispositivos que utilizan subredes de VLAN públicas.

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

El comando devuelve detalles sobre la VLAN sin la asociación de 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": "2025-08-23T13:48:49.846000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

La `eipAssociations` matriz vacía confirma que la dirección IP elástica se ha disociado correctamente de la VLAN.

Acerca de la optimización WAN de HCX para migraciones basadas en Internet

> **Note**
>
> La función de optimización de WAN ya no está disponible en HCX 4.11.3. Para obtener más información, consulte las notas de la versión HCX 4.11.3.

Al realizar migraciones a través de Internet, la optimización WAN de HCX (HCX-WO) puede mejorar el rendimiento de la migración. El servicio funciona junto con el dispositivo de interconexión HCX (HCX-IX) para:

- Aplique técnicas de reducción de datos para minimizar el uso del ancho de banda.
- Implemente el acondicionamiento de rutas WAN para optimizar el rendimiento de la red.
- Mejore las velocidades de migración a través de conexiones a Internet de alta latencia.
- Mejore la confiabilidad de las migraciones basadas en Internet.

La optimización WAN de HCX es particularmente útil para las migraciones basadas en Internet en las que:

- La latencia de la red puede ser superior a la de las opciones de conectividad privada.
- El ancho de banda disponible puede ser limitado o variable.
- Las condiciones de la red pueden fluctuar debido a los patrones de tráfico de Internet.

Para obtener instrucciones detalladas sobre cómo configurar la optimización WAN de HCX después de configurar la conectividad a Internet, consulte. the section called “(Opcional) Configure la optimización WAN de HCX”

> **Note**
>
> Si bien la optimización de la WAN puede mejorar considerablemente el rendimiento de la migración basada en Internet, es posible que no ofrezca beneficios adicionales en entornos con conexiones dedicadas de 10 Gb y baja latencia. Tenga en cuenta las características de su red a la hora de decidir si habilitar esta función.

Administración de entornos de Amazon EVS

En este capítulo se incluyen los siguientes temas para ayudarle a gestionar su entorno.

- the section called “Suscripciones a VCF”- Describe cómo funcionan las suscripciones de VCF con Amazon EVS y las responsabilidades del cliente en cuanto a la gestión de las suscripciones de VCF.
- the section called “Versiones e instancias de VCF EC2 ”- Describe las versiones de VCF y ESX compatibles y cómo comprobar la disponibilidad de las versiones en Amazon EVS.
- the section called “Administración del ciclo de vida”- Describe las responsabilidades de administración del ciclo de vida dentro de un entorno Amazon EVS, incluida la administración de la infraestructura subyacente, la administración de actualizaciones de VCF y la administración del ciclo de vida del host ESX.
- the section called “Mantenimiento del entorno”- Describe cómo realizar tareas de mantenimiento habituales para su entorno Amazon EVS, incluida la configuración de la red, el mantenimiento del host ESX, la comprobación del estado del entorno y la gestión de los programas de rotación secretos para sus credenciales de VCF.
- the section called “Cree un anfitrión”- Describe cómo crear un host de Amazon EVS después de la implementación del entorno y cómo añadir el host al clúster.
- the section called “Eliminar un host”- Describe cómo eliminar un host de Amazon EVS y eliminarlo del clúster.

Suscripciones a VCF

> **Note**
>
> Amazon EVS no admite licencias perpetuas de vSphere. Debe tener una suscripción a VMware Cloud Foundation válida y activa para utilizar Amazon EVS.

Amazon EVS utiliza suscripciones a VMware Cloud Foundation (VCF) con los derechos de portabilidad de licencias que usted aporta a (BYOS). AWS Para implementar correctamente un entorno Amazon EVS, debe proporcionar una clave de solución VCF válida y una clave de licencia de vSAN en la solicitud de creación del entorno. La clave de licencia de vSphere sirve como clave de solución para VCF. Cada clave de licencia de VCF solo se puede utilizar para un entorno de Amazon

EVS. Se produce un error en la creación del entorno si intenta utilizar una clave de licencia de VCF que ya está en uso en otro entorno.

La clave de la solución VCF debe tener al menos 256 núcleos para proporcionar una capacidad de núcleo adecuada para los cuatro EC2 hosts i4i.metal iniciales que Amazon EVS despliega al crear el entorno. Cada host i4i.metal requiere 64 núcleos. La clave de licencia de vSAN debe tener al menos 110 TiB de capacidad de vSAN. Se produce un error en la creación del entorno si se intenta utilizar claves de licencia de tamaño insuficiente.

> **Note**
>
> Su suscripción a VCF estará disponible para Amazon EVS en todas AWS las regiones para garantizar el cumplimiento de las licencias. Amazon EVS no valida las claves de licencia. Para validar las claves de licencia, visite el soporte de Broadcom.

> **Note**
>
> La información sobre el software VCF en Amazon EVS se compartirá con Broadcom para verificar el cumplimiento de la licencia.

Administración de suscripciones

Usted es responsable de administrar sus suscripciones a VCF. Sus suscripciones a VCF deben administrarse en SDDC Manager. Eliminar las claves de licencia de SDDC Manager o sustituirlas por una clave de licencia en uso provocará un error en la comprobación del estado del entorno, lo que le impedirá añadir hosts a su entorno de Amazon EVS. Para obtener más información sobre las comprobaciones del estado del entorno, y. the section called “Supervise el estado del entorno” the section called “Solucione problemas con las comprobaciones de estado del entorno que no” Para obtener más información sobre las claves de licencia de VCF, consulte Administrar las claves de licencia en VMware Cloud Foundation en la documentación de VMware Cloud Foundation.

> **Important**
>
> Utilice la interfaz de usuario de SDDC Manager para gestionar la solución VCF y las claves de licencia de vSAN. Amazon EVS requiere que mantenga claves de licencia de vSAN y de solución VCF válidas en SDDC Manager para que el servicio funcione correctamente. Si bien

las claves se deben asignar a los hosts y al clúster de vSAN mediante vSphere Client, debe asegurarse de que esas claves también aparezcan en la pantalla de licencias de la interfaz de usuario del SDDC Manager.

Añadir claves de licencia de VCF

En el portal de soporte de Broadcom, puede comprar claves de licencia VCF adicionales, claves de licencia divididas si ya tiene claves grandes o combinar varias claves de licencia. Esto le permite licenciar los hosts que haya agregado a su entorno después de la implementación inicial o licenciar entornos adicionales. Asegúrese de añadir las claves de licencia adquiridas al inventario de vCenter Server y SDDC Manager. Si va a añadir hosts, asegúrese de que las licencias estén asignadas a los hosts correctos en vSphere y de que tengan los núcleos y la capacidad de almacenamiento de vSAN adecuados. Amazon EVS no admite hosts sin licencia. Para obtener más información, consulte Configuración de los ajustes de licencia para los activos en vSphere Client en la VMware documentación.

Las nuevas claves de licencia que no hayan caducado deben asignarse a vCenter Server antes de que venza el período de evaluación de la clave de licencia para que permanezcan activas. Se requieren claves de licencia activas para configurar correctamente un entorno Amazon EVS. El entorno no se podrá implementar si se proporciona una clave de licencia caducada. Para obtener más información sobre la creación de claves de licencia de VCF, consulte Crear una nueva licencia en la VMware documentación. Si tiene problemas con las claves de licencia agregadas, consultethe section called “No se pudo comprobar la cobertura de las claves”.

Eliminar las claves de licencia de VCF

Puede eliminar las claves de licencia de VCF del inventario de SDDC Manager para reducir la capacidad principal y de vSAN después de eliminar los hosts de su entorno. Para cumplir con los modelos de licencia de los productos que utiliza con vSphere, debe eliminar del inventario todas las claves de licencia no asignadas. Si ha dividido, fusionado o actualizado las claves de licencia en el portal de soporte de Broadcom, debe eliminar las claves de licencia antiguas. Para obtener más información, consulte Eliminar una licencia en la VMware documentación.

Versiones de VCF y tipos de EC2 instancias proporcionados por Amazon EVS

Amazon EVS ofrece varias versiones de VMware Cloud Foundation (VCF), ESX y tipos de EC2 instancias que puede seleccionar al crear un entorno y crear un host.

Comprobar las versiones de VCF, las versiones de ESX y los tipos de instancias proporcionados EC2

La AWS consola muestra la lista de versiones de VCF proporcionada por Amazon EVS en el asistente de creación de entornos. Las versiones de ESX disponibles están visibles al seleccionar un tipo de instancia al añadir un host a un entorno existente. También puede ver las versiones de VCF, las versiones de ESX y los tipos de EC2 instancias mediante la CLI.

Example

Amazon EVS console

1. Ve a la consola Amazon EVS.
2. En el menú de navegación, selecciona Entornos.
3. Realice una de las siguientes acciones:

   Para comprobar las versiones de VCF:

   a. Seleccione Crear entorno.
   b. En los requisitos de Validate Amazon EVS, elige tu versión de VCF para comprobar si el estado está disponible o restringido para ti.

   Para comprobar las versiones de ESX:

   a. Seleccione un entorno existente.
   b. Elija Create host (Crear alojamiento).
   c. Seleccione un tipo de instancia para ver las versiones de ESX disponibles.

AWS CLI

Ejecute el siguiente comando para recuperar información sobre las versiones de VCF y ESX:

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

Ejemplo de respuesta:

```
{
   "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**
>
> Si aparece `RESTRICTED` la versión que necesita y tiene una necesidad específica, consulte the section called “Solicitud de acceso a versiones restringidas de VCF” para obtener más información sobre cómo acceder a esa versión.

Versiones actuales de VCF en Amazon EVS

Amazon EVS ofrece actualmente las siguientes versiones de VCF para la creación de entornos:

Versión de VCF	Versión de ESX predeterminada	Status	EC2 tipos de instancias
VCF-5.2.2	ESXi-8.0u3G-24859861	DISPONIBLE	i4i.metal
VCF-5.2.1	ESXi-8.0u3B-24280767	RESTRINGIDO	i4i.metal

> **Note**
>
> Al crear un nuevo entorno de Amazon EVS, debe especificar una versión de VCF.

Consideraciones sobre la versión de ESX

Cada versión de VCF tiene una versión de ESX predeterminada basada en la lista de materiales (BOM) de Broadcom VCF. Al crear un entorno nuevo, no puede elegir una versión de ESX específica. La versión de ESX predeterminada para la versión de VCF seleccionada se aplica automáticamente.

Sin embargo, al agregar un host a su entorno, puede seleccionar una versión de ESX disponible para el tipo de instancia que elija. Si no especifica ninguna, Amazon EVS utiliza la versión ESX predeterminada asociada a la versión VCF de su entorno.

Una vez agregado un host, su versión de ESX solo se puede actualizar mediante vCenter Lifecycle Manager.

> **Note**
>
> Amazon EVS no proporciona todas las versiones de VCF y ESX publicadas por Broadcom. Para obtener información sobre la interoperabilidad del software, consulte la matriz de interoperabilidad de Broadcom. Para obtener información sobre la compatibilidad total del hardware con AWS EC2 las instancias, consulte la Guía de compatibilidad de Broadcom.

Solicitud de acceso a versiones restringidas de VCF

Si necesita acceder a una versión de VCF con un `RESTRICTED` estado, [póngase en contacto con AWS Support](#) con la siguiente información:

- El ID de su AWS cuenta
- La AWS región
- La versión específica de VCF que necesita
- Su caso de uso y su justificación empresarial (por ejemplosecurity/compliance, compatibility/dependency, y otros)

AWS Support revisará su solicitud y aprobará o solicitará información adicional. Tras la aprobación, el estado de la versión cambiará al de `AVAILABLE` la respuesta de la AWS consola o de la `get-versions` API.

Gestión del ciclo de vida del entorno Amazon EVS

En esta página se describen sus responsabilidades de gestión del ciclo de vida en un entorno de Amazon EVS.

Una ventaja clave de Amazon EVS es que tiene un control total sobre su VMware arquitectura en la nube. Puede optimizar el paquete de software de VMware Cloud Foundation (VCF) para satisfacer las demandas únicas de sus aplicaciones. Dado que Amazon EVS es un servicio autogestionado, usted es responsable de la administración y el mantenimiento del ciclo de vida del VMware software utilizado en el entorno de Amazon EVS, como ESX, vSphere, vSAN, NSX y SDDC Manager. También es responsable del mantenimiento de las integraciones de terceros, como las soluciones de protección de datos que integre en sus hosts de Amazon EVS.

Usted es responsable de la configuración de los componentes de AWS red subyacentes que utiliza Amazon EVS, incluidas las tablas de enrutamiento de VPC, las reglas de grupos de seguridad y listas de control de acceso a la red (ACL), la configuración del servidor de rutas de VPC, las puertas de enlace de Internet, las puertas de enlace NAT y las puertas de enlace de tránsito (para la conectividad local).

AWS es responsable de implementar el entorno Amazon EVS con las configuraciones de red que usted proporcione. La implementación del entorno incluye lo siguiente:

- Arrancar la configuración de red de su entorno Amazon EVS.

- Habilitar el enrutamiento norte-sur con la instancia de servidor de rutas de VPC que proporcione.
- Implementación de las subredes VLAN de EVS necesarias, las interfaces de red elásticas y los cuatro hosts ESX iniciales necesarios.
- Configuración de una red superpuesta de NSX con una puerta de enlace de nivel 0 y una puerta de enlace de nivel 1.
- Implementación de un clúster de NSX Edge con dos nodos de NSX Edge en modo. Active/Standby
- Crear y configurar el clúster de vSAN inicial y montar el almacén de datos.

Usted es responsable de la configuración de VMware NSX, incluidos los segmentos de red, las reglas de firewall distribuidas y los equilibradores de carga. También es responsable de la configuración de cualquier solución integrada que implemente con Amazon EVS después de la implementación del entorno EVS, incluida la configuración de VMware HCX y las puertas de enlace NSX de nivel 1 adicionales.

Para obtener más información sobre las responsabilidades del cliente AWS y las responsabilidades del cliente, consulte el modelo de responsabilidad compartida.AWS

> **Note**
>
> Se crean y configuran una puerta de enlace de nivel 0 y una puerta de enlace de nivel 1 como parte de la implementación del entorno Amazon EVS. Amazon EVS solo admite una única puerta de enlace de nivel 0 en este momento. Cualquier modificación en estos enrutadores lógicos o en el nodo NSX Edge VMs podría afectar a la conectividad y debe evitarse.

VMware actualizaciones de software

> **Warning**
>
> Si ha actualizado su versión de ESX después de la implementación del entorno Amazon EVS, es posible que el administrador del SDDC no funcione durante la validación del host de VCF en la etapa de comisionar los anfitriones. Para ver los pasos para solucionar este problema, consulte. the section called “El administrador del SDDC no pasa la validación del host VCF durante la puesta en servicio del host”

Para obtener información sobre las versiones de VCF proporcionadas por Amazon EVS, consulte. the section called “Versiones e instancias de VCF EC2 ” Según el modelo de responsabilidad AWS compartida, usted es responsable de aplicar cualquier parche, actualización o mejora al software VCF, incluidas ESX, vCenter Server, vSAN, NSX, SDDC Manager y otras soluciones integradas, en su entorno de EVS. Tras la implementación, le recomendamos que revise la versión del software VCF implementada por Amazon EVS y la actualice según sea necesario. Puede obtener las actualizaciones de VCF a través del portal de soporte de Broadcom. También le recomendamos que establezca y respete un programa de mantenimiento regular para las actualizaciones y los parches.

> **Note**
>
> Amazon EVS no es compatible con VMware Cloud Foundation 9 en este momento.

> **Note**
>
> Amazon EVS no proporciona todas las versiones de VCF y ESX publicadas por Broadcom. Para obtener información sobre la interoperabilidad del software, consulte la matriz de interoperabilidad de Broadcom. Para obtener información sobre la compatibilidad total del hardware con AWS EC2 las instancias, consulte la Guía de compatibilidad de Broadcom.

Determinados parches, actualizaciones o mejoras pueden afectar a las cargas de trabajo que se ejecutan en su entorno. Antes de aplicar parches o actualizar su software de VCF, le recomendamos que consulte la Guía de administración del ciclo de vida de VCF para comprender cómo afectarán estos cambios a su entorno. También le recomendamos que pruebe los cambios en un entorno provisional antes de implementarlos en producción. Puede consultar las notas de la versión 5.2.x de VCF para conocer las actualizaciones más recientes de VCF 5.2.x.

Mantenimiento y ciclo de vida del host ESX

Usted es responsable de la administración y el mantenimiento del ciclo de vida del host ESX en el entorno Amazon EVS, incluida la supervisión del estado del host y la solución de los problemas del host. Para obtener más información, consulte the section called “Mantenimiento del entorno”.

AWS realiza el mantenimiento programado de las EC2 instancias i4i.metal subyacentes para garantizar la confiabilidad, la disponibilidad y el rendimiento de la infraestructura. Para obtener más

información, consulte the section called “Acerca del mantenimiento AWS programado de las EC2 instancias”.

Realizar el mantenimiento de su entorno

En esta sección se describe cómo realizar tareas de mantenimiento comunes para su entorno de Amazon EVS.

Temas

- Supervise el estado y los recursos de su entorno
- Mantenimiento de AMI
- Mantenimiento del host Amazon EVS
- Configurar una tabla de enrutamiento personalizada para las subredes de Amazon EVS
- Configurar una lista de control de acceso a la red para controlar el tráfico de subred de VLAN de Amazon EVS
- Ciclo de vida de administración secreta

Supervise el estado y los recursos de su entorno

Puede supervisar varios aspectos del entorno de Amazon EVS y AWS los recursos subyacentes mediante la consola Amazon EVS o. AWS CLI

> **Note**
>
> VMware Los componentes de Cloud Foundation (VCF) se supervisan en SDDC Manager. No puede monitorizar los componentes del VCF mediante la consola Amazon EVS o. AWS CLI Para obtener información sobre el uso de SDDC Manager para monitorear los componentes de VMware Cloud Foundation (VCF), consulte Introducción a SDDC Manager.

Vea el estado y los recursos del entorno

El estado del entorno le ayuda a determinar si su entorno tiene problemas que requieren atención. Siga este procedimiento para comprobar el estado del entorno y ver los recursos subyacentes.

Example

Amazon EVS console

1. Abra la consola Amazon EVS.
2. En el panel de navegación, elija Entornos.
3. Elija su ID de entorno para abrir la página de detalles del entorno.
4. En Detalles, consulte el estado del entorno.

   Si su entorno está en buen estado, el estado aparece como Aprobado. Si hay problemas, el estado aparece como Fallido. Si el estado es Fallido, puede ver una ventana emergente que muestra los resultados de cuatro comprobaciones del estado del entorno:

   - Reutilización de claves: muestra la clave aprobada o no válida para indicar si la clave de licencia de VCF es válida.
   - Recuento de hosts: muestra Desconocido, Aprobado o Fallo para indicar el estado de la conectividad del host.
   - Cobertura clave: muestra la clave aprobada o no para indicar si la clave de licencia de VCF cubre todos los hosts.
   - Accesibilidad: muestra si se ha aprobado o no se ha podido acceder al SDDC Manager.

     Para obtener información sobre la resolución de errores en la comprobación del estado del entorno, consulte. Resolución de problemas

     Para ver los recursos de su entorno

     Elija una de las siguientes pestañas:

   - Anfitriones: muestra los hosts de su entorno.
   - Redes y conectividad: muestra la VPC, las subredes de EVS y los recursos del servidor de rutas de VPC asociados a su entorno.
   - Dispositivos de administración: muestra los dispositivos de administración de VCF de su entorno con sus nombres de host DNS y las credenciales relacionadas.
   - Etiquetas: muestra las etiquetas asociadas a su entorno.

AWS CLI

Puede utilizarlas AWS CLI para comprobar el estado y los recursos de su entorno.

Para enumerar todos los entornos y su estado

```
aws evs list-environments
```

> **Tip**
>
> Utilice el `--query` parámetro para filtrar la salida. Por ejemplo:

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

Para enumerar los hosts del entorno

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

Para enumerar el entorno VLANs

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

Para obtener más información sobre las operaciones de la API, consulte lo siguiente en la Guía de referencia de la API de Amazon EVS:

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

Mantenimiento de AMI

Amazon EVS implementa hosts ESX con una Amazon Machine Image (AMI) de EVS personalizada. La AMI contiene un complemento de proveedor personalizado que contiene los paquetes necesarios para ejecutar ESX en Amazon EC2.

Solucione el problema de un error al añadir el host debido a una imagen de clúster incompatible

Cuando agrega un host a su entorno, el host tiene la última versión disponible del complemento personalizado del proveedor de EVS. Si su entorno utiliza hosts con una versión complementaria anterior, se produce un error al agregar nuevos hosts y se produce un error que indica que el nuevo host no es compatible con la imagen de clúster. Para ver los pasos detallados para solucionar este problema, consultethe section called “Error al agregar el host debido a una imagen de clúster incompatible”.

Mantenimiento del host Amazon EVS

Como Amazon EVS es un servicio autogestionado, usted es responsable del mantenimiento del software VMware Cloud Foundation (VCF) que se ejecuta en el host, de supervisar su estado y de solucionar los problemas del host, incluida la sustitución del host en caso de que se produzca un fallo en el host. Para obtener más información sobre la administración de los hosts de ESX en VMware Cloud Foundation (VCF), consulte la documentación sobre la administración de hosts en Cloud Foundation. VMware

Comprobar el estado de la instancia subyacente EC2

Amazon EC2 realiza comprobaciones automatizadas en cada EC2 instancia en ejecución para identificar problemas de hardware y software. Puede ver los resultados de estas comprobaciones de estado en la EC2 consola o AWS CLI para identificar problemas específicos y detectables. Para obtener más información, consulta Ver comprobaciones de estado de una EC2 instancia de Amazon en la Guía del EC2 usuario de Amazon y describe-instance-statusen la Referencia de la línea de AWS CLI comandos.

Puedes crear una CloudWatch alarma que te avise si las comprobaciones de estado fallan en una instancia específica. Para obtener más información, consulta Crear CloudWatch alarmas para EC2 instancias de Amazon que no pasen las comprobaciones de estado en la Guía del EC2 usuario de Amazon.

Acerca del mantenimiento AWS programado de las EC2 instancias

AWS realiza el mantenimiento programado de las EC2 instancias subyacentes para garantizar la confiabilidad, la disponibilidad y el rendimiento. EC2 Las instancias completas están sujetas a los mismos tipos de eventos programados que las demás EC2 instancias. AWS puede programar eventos para reiniciar, detener y retirar las instancias debido a problemas subyacentes de hardware

o a un mantenimiento programado. Estos eventos no ocurren con frecuencia. Para obtener más información, consulta Tipos de eventos programados en la Guía del EC2 usuario de Amazon.

> **Note**
>
> Debe colocar los hosts en modo de mantenimiento en vSphere Client antes de cualquier evento de reinicio programado.

Si una de sus instancias se verá afectada por un evento programado, se lo AWS notificará con antelación por correo electrónico a la dirección de correo electrónico asociada al suyo. Cuenta de AWS AWS también envía un evento de AWS Salud, que puedes monitorizar y gestionar con Amazon EventBridge. Para obtener más información, consulta Monitorización de eventos en AWS Salud con Amazon EventBridge y Eventos programados para EC2 instancias de Amazon en la Guía del EC2 usuario de Amazon.

En cualquier momento, puedes reprogramar el evento para que se produzca en la fecha y hora específicas que más te convengan. El evento se puede reprogramar hasta la fecha límite del evento. Para obtener más información, consulta Reprogramar un evento programado para una EC2 instancia en la Guía del EC2 usuario de Amazon.

Uso de reservas de capacidad EC2 bajo demanda

Puede utilizar las reservas de capacidad EC2 bajo demanda para garantizar que el clúster tenga suficiente capacidad durante los períodos de mantenimiento. Puede reservar capacidad en una zona de disponibilidad específica durante cualquier período. Para obtener más información, consulta Reserva capacidad de cómputo con reservas de capacidad EC2 bajo demanda en la Guía del EC2 usuario de Amazon.

Para conocer los pasos para crear una reserva de capacidad, consulta Crear una reserva de capacidad en la Guía del EC2 usuario de Amazon.

> **Note**
>
> Si utiliza reservas de capacidad EC2 bajo demanda o hosts EC2 dedicados, le recomendamos que reserve un host de reserva para las cargas de trabajo esenciales. Si bien las reservas de capacidad garantizan el acceso a una cantidad específica de capacidad de EC2 instancia en una zona de disponibilidad determinada, disponer de un host libre proporciona un nivel adicional de redundancia que es fundamental para las cargas de

trabajo esenciales. En el caso de los hosts dedicados, disponer de un host libre garantiza el mantenimiento del entorno para las cargas de trabajo esenciales, incluso si el host principal requiere mantenimiento o tiene algún problema.

Prepararse para la programación y los eventos AWS `system-maintenance` `instance-retirement`

AWS programa dos tipos de `system-maintenance` eventos: mantenimiento de la red y mantenimiento de la energía.

- Durante el mantenimiento de red, las instancias programadas pierden la conectividad de red durante un breve periodo de tiempo. La conectividad de red normal a la instancia se restaurará una vez completado el mantenimiento.
- Durante el mantenimiento de energía, las instancias programadas se desconectan durante un breve periodo y, a continuación, se reinician. Cuando se realiza un reinicio en instancias EC2 completas, no se conservan los datos del volumen del almacén de instancias.

AWS programa EC2 `instance-retirement` eventos cuando se detecta una degradación del hardware subyacente que aloja EC2 las instancias.

Para corregir cualquier `system-maintenance` suceso, sustituya el host que ha fallado por uno nuevo mediante la consola Amazon EVS o AWS CLI un SDDC Manager antes de que se produzca el evento de mantenimiento. `instance-retirement` Si espera a que se produzca el evento de mantenimiento y sea necesario reiniciar la EC2 instancia, perderá los datos de vSAN que están almacenados en el volumen del almacén de instancias. Para ver los pasos detallados, consulte the section called “Sustituir un host de Amazon EVS”.

> **Important**
>
> La EC2 consola no debe usarse para administrar el estado de los hosts de Amazon EVS, incluidos los de parada, inicio y terminación. No intente iniciar, detener ni finalizar las EC2 instancias que despliega Amazon EVS. Esta acción provoca la pérdida de datos de vSAN.

Sustituir un host de Amazon EVS

Siga este procedimiento para reemplazar un host de Amazon EVS.

> **Warning**
>
> Los hosts de Amazon EVS utilizan un complemento de proveedor personalizado para proporcionar una funcionalidad de host importante. Cuando añada un host a su entorno, tendrá la última versión disponible del complemento personalizado de Amazon EVS. Si su entorno usa hosts con una versión adicional anterior, agregar un host al clúster de vSphere provocará un error en la corrección de la imagen del clúster. Para ver los pasos para solucionar este problema, consulte. the section called “Solucione el problema de un error al añadir el host debido a una imagen de clúster incompatible”

> **Warning**
>
> Si ha actualizado la versión de ESX después de la implementación, es posible que el administrador del SDDC no funcione durante la validación del host VCF en la etapa de comisionamiento de los anfitriones. Para ver los pasos para solucionar este problema, consulte. the section called “El administrador del SDDC no pasa la validación del host VCF durante la puesta en servicio del host”

> **Note**
>
> Asegúrese de que el número de hosts de Amazon EVS por cuota de entorno de EVS esté configurado correctamente para garantizar que la creación del host se ha realizado correctamente. Se produce un error en la creación de hosts si este valor de cuota es inferior al número de hosts que intenta aprovisionar en un único entorno de Amazon EVS. Es posible que deba solicitar un aumento de cuota para las operaciones de mantenimiento que requieran la sustitución del host. Para obtener más información, consulte Cuotas de servicio.

Example

Amazon EVS console and SDDC Managuer UI

1. Ve a la consola Amazon EVS.
2. En el panel de navegación, elija Entorno.
3. Seleccione el entorno que contiene el host que se va a reemplazar.

4. Seleccione la pestaña Hosts.
5. Elija Create host (Crear alojamiento).
6. Especifique los detalles del anfitrión y elija Crear anfitrión.
7. Para comprobar que se ha completado, compruebe que el estado del host ha cambiado a Creado.
8. Recupere las credenciales de la contraseña root de ESX de AWS Secrets Manager. Para obtener más información sobre cómo recuperar secretos, consulte Obtener AWS secretos de Secrets Manager en la Guía del usuario de AWS Secrets Manager.
9. Vaya a SDDC Manager.
10. Instale el nuevo host en SDDC Manager con las credenciales raíz de ESX que obtuvo en un paso anterior. Para obtener más información, consulte Comisionar anfitriones en la documentación de VMware Cloud Foundation.
11. Agregue el nuevo host al clúster. Para obtener más información, consulte Cómo agregar un host ESX a su clúster de vSphere mediante el flujo de trabajo de inicio rápido en la documentación de vSphere.
12. Quite el host anterior de SDDC Manager que desee eliminar de SDDC Manager. Para obtener más información, consulte Retirar los hosts en la documentación de Cloud Foundation. VMware
13. Regrese a la consola Amazon EVS.
14. En la pestaña Hosts, seleccione el host fallido y elija Eliminar > Eliminar host.

AWS CLI and SDDC Manager UI

1. Abra una nueva sesión de terminal.
2. Cree un nuevo host. Consulte el comando de ejemplo que aparece a continuación como referencia.

```
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 las credenciales de la contraseña root de ESX de AWS Secrets Manager. Para obtener más información sobre cómo recuperar secretos, consulte Obtener AWS secretos de Secrets Manager en la Guía del usuario de AWS Secrets Manager.
4. Vaya a SDDC Manager.
5. Instale el nuevo host en SDDC Manager con las credenciales raíz de ESX que obtuvo en un paso anterior. Para obtener más información, consulte Comisionar anfitriones en la documentación de VMware Cloud Foundation.
6. Agregue el nuevo host al clúster que contiene el host dañado.
7. Retire el host averiado en el administrador del SDDC. Para obtener más información, consulte Retirar los hosts en la documentación de Cloud Foundation. VMware
8. Regrese a la terminal.
9. Elimine el host que ha fallado. Consulte el ejemplo de comando que aparece a continuación como referencia.

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

Resolución de problemas

Para obtener ayuda sobre la solución de problemas, consulte Resolución de problemas. Si sigue teniendo problemas después de revisar la guía de solución de problemas, póngase en contacto con AWS Support para obtener más ayuda.

Configurar una tabla de enrutamiento personalizada para las subredes de Amazon EVS

Amazon EVS admite el uso de una tabla de enrutamiento personalizada solo después de crear el entorno de Amazon EVS. Para permitir la creación correcta del entorno, debe configurar la tabla de enrutamiento principal para permitir el tráfico a los servicios dependientes, como el DNS y los sistemas locales. Esto se debe a que las subredes VLAN de Amazon EVS se asocian implícitamente a la tabla de enrutamiento principal de nuestra VPC durante la implementación del entorno.

Tras la implementación del entorno, debe asociar de forma explícita cada una de las subredes de VLAN de Amazon EVS a una tabla de enrutamiento de la VPC. La conectividad de NSX falla si las subredes de VLAN no están asociadas explícitamente a una tabla de enrutamiento de VPC.

Le recomendamos encarecidamente que asocie las subredes de forma explícita a una tabla de enrutamiento personalizada. Una tabla de enrutamiento personalizada proporciona un control más detallado sobre el enrutamiento del tráfico de red dentro de la VPC, lo que permite establecer reglas de enrutamiento personalizadas para subredes o puertas de enlace específicas. Para obtener más información sobre cómo crear una tabla de enrutamiento personalizada, consulte Crear una tabla de enrutamiento para su VPC en la Guía del usuario de Amazon VPC.

Configurar una lista de control de acceso a la red para controlar el tráfico de subred de VLAN de Amazon EVS

Una lista de control de acceso (ACL) de red permite o deniega el tráfico entrante o saliente específico en el nivel de subred. Puede utilizar la red ACLs para controlar el tráfico entrante y saliente de las subredes de VLAN de Amazon EVS. Para obtener más información, consulte Crear una ACL de red para su VPC en la Guía del usuario de Amazon VPC.

Important

EC2 los grupos de seguridad no funcionan en las interfaces de red elásticas que están conectadas a las subredes de VLAN de Amazon EVS. Para controlar el tráfico hacia y desde las subredes VLAN de Amazon EVS, debe usar una lista de control de acceso a la red.

Warning

Amazon EVS requiere acceso a su implementación de VCF. Debe configurar los grupos de seguridad y las listas de control de acceso a la red (ACLs) para permitir que Amazon EVS se comunique con:

- Servidores DNS a través TCP/UDP del puerto 53.
- Subred VLAN de administración de hosts a través de HTTPS y SSH.
- Administración de la subred VLAN de VM a través de HTTPS y SSH.

Si sus grupos de seguridad y su red ACLs no permiten este acceso, la implementación del entorno Amazon EVS fallará y los entornos existentes podrían tener un estado de conformidad degradado.

Ciclo de vida de administración secreta

Amazon EVS utiliza AWS Secrets Manager para crear, cifrar y almacenar información confidencial en su cuenta durante la implementación inicial del entorno. Estos secretos contienen las credenciales de VCF necesarias para instalar y acceder a los dispositivos de administración de VCF, como vCenter Server, NSX y SDDC Manager, así como la contraseña raíz del host ESX. Amazon EVS también elimina los secretos gestionados en su nombre cuando se elimina el entorno de EVS.

Usted es responsable de la gestión del ciclo de vida de los secretos, incluida la rotación de los secretos. Amazon EVS no ofrece una rotación administrada de los secretos. Te recomendamos que cambies los secretos con regularidad en una ventana de rotación establecida para asegurarte de que los secretos no duren mucho tiempo. Para obtener más información, consulte los programas de rotación en la Guía del usuario de AWS Secrets Manager.

Crear un host de Amazon EVS

Tras la implementación de un entorno Amazon EVS, puede añadir hosts para aumentar la capacidad y la resiliencia de la carga de trabajo. Amazon EVS admite de 4 a 16 hosts por entorno. Esta acción solo se puede utilizar después de implementar el entorno Amazon EVS.

> **Note**
>
> Debe asignar y poner en marcha el host desde la interfaz de usuario del SDDC Manager.

Para crear un host de Amazon EVS

Siga estos pasos para crear un host de Amazon EVS.

> **Warning**
>
> Los hosts de Amazon EVS utilizan un complemento de proveedor personalizado para proporcionar una importante funcionalidad de alojamiento. Cuando añada un host a su entorno, tendrá la última versión disponible del complemento personalizado de Amazon EVS. Si su entorno usa hosts con una versión adicional anterior, agregar un host al clúster de vSphere provocará un error en la corrección de la imagen del clúster. Para ver los pasos para solucionar este problema, consulte. the section called “Solucione el problema de un error al añadir el host debido a una imagen de clúster incompatible”

Warning

Si ha actualizado su versión de ESX después de la implementación del entorno Amazon EVS, es posible que el administrador del SDDC no funcione durante la validación del host de VCF en la etapa de comisionar los anfitriones. Para ver los pasos para solucionar este problema, consulte. the section called “El administrador del SDDC no pasa la validación del host VCF durante la puesta en servicio del host”

Note

Asegúrese de que el número de hosts de Amazon EVS por cuota de entorno de EVS esté configurado correctamente para garantizar la creación correcta del host. Se produce un error en la creación de hosts si este valor de cuota es inferior al número de hosts que intenta aprovisionar en un único entorno de Amazon EVS. Para aumentar la cuota, puede solicitar un aumento de cuota. Para obtener más información, consulte Cuotas de servicio.

Note

Si no especifica una versión de ESX al añadir hosts a su entorno, Amazon EVS utiliza automáticamente la versión de ESX predeterminada asociada a la versión de VCF de su entorno. Para obtener más información, consulte the section called “Versiones e instancias de VCF EC2 ”.

Important

Al agregar un host ESX, seleccione una versión de ESX que coincida con el clúster de vSphere de destino. Si la misma versión no está disponible, implemente una versión anterior y actualícela con vSphere Lifecycle Manager. Para obtener más información, consulte the section called “El administrador del SDDC no pasa la validación del host VCF durante la puesta en servicio del host”. Las actualizaciones pueden requerir el rearranque del host y aumentar el tiempo que tarda en ponerse en marcha el host.

Un host con una versión de ESX más reciente que la versión ESX de la imagen de clúster de vSphere no se puede degradar. Deberá eliminar el host y volver a crearlo con la versión de ESX correcta.

Example

Amazon EVS console and SDDC Managuer UI

1. Ve a la consola Amazon EVS.
2. En el panel de navegación, elija Entorno.
3. Seleccione el entorno en el que desee crear el host.
4. Seleccione la pestaña Hosts.
5. Elija Create host (Crear alojamiento).
6. Especifique los detalles del anfitrión y elija Crear anfitrión.
7. Para comprobar que se ha completado, compruebe que el estado del host ha cambiado a Creado.
8. Vaya al administrador del SDDC.
9. Ponga en marcha el nuevo host en SDDC Manager. Para obtener más información, consulte Comisionar anfitriones en la documentación de VMware Cloud Foundation.
10. Agregue el nuevo host al clúster mediante SDDC Manager. Para obtener más información, consulte Cómo agregar un host ESX a su clúster de vSphere mediante el flujo de trabajo de inicio rápido en la documentación de vSphere.

AWS CLI and SDDC Manager UI

1. Abra una nueva sesión de terminal.
2. Cree un nuevo host. Consulte el comando de ejemplo que aparece a continuación como referencia.

```
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. Vaya al administrador del SDDC.
4. Ponga en marcha el nuevo host en SDDC Manager. Para obtener más información, consulte Comisionar anfitriones en la documentación de VMware Cloud Foundation.
5. Agregue el nuevo host al clúster mediante SDDC Manager. Para obtener más información, consulte Cómo agregar un host ESX a su clúster de vSphere mediante el flujo de trabajo de inicio rápido en la documentación de vSphere.

Eliminar un host de Amazon EVS

Puede eliminar un host de Amazon EVS de su entorno cuando ya no lo necesite. Amazon EVS requiere que su entorno tenga un mínimo de cuatro hosts. Amazon EVS no admite entornos con menos de cuatro hosts.

> **Warning**
>
> Si se elimina un host sin retirarlo, se dejarán datos obsoletos en el vCenter y en el SDDC Manager y es posible que sea necesario realizar esfuerzos adicionales de limpieza. Asegúrese de que sus hosts estén retirados del servicio antes de eliminarlos de la consola o API de Amazon EVS.

> **Warning**
>
> Utilice siempre la consola o la API de Amazon EVS para eliminar los hosts de Amazon EVS. Eliminar los hosts de la EC2 consola puede dejar el entorno en un estado incoherente.

Para eliminar un host de Amazon EVS

Siga estos pasos para eliminar un host de Amazon EVS.

Example

SDDC Managuer UI and Amazon EVS console

1. Vaya al administrador del SDDC.

2. Elimine el clúster del administrador del SDDC.
3. Retire el host del SDDC Manager. Para obtener más información, consulte Retirar los hosts en la documentación de Cloud Foundation. VMware
4. Ve a la consola Amazon EVS.
5. En el panel de navegación, elija Entorno.
6. Seleccione el entorno que contiene el host que desea eliminar.
7. Seleccione la pestaña Hosts.
8. Seleccione Eliminar anfitrión.
9. Seleccione el anfitrión y elija Eliminar en la pestaña Hosts. Repita este paso para cada host que desee eliminar.

SDDC Manager UI and AWS CLI

1. Vaya al administrador del SDDC.
2. Elimine el clúster del administrador del SDDC.
3. Retire el host del SDDC Manager. Para obtener más información, consulte Retirar los hosts en la documentación de Cloud Foundation. VMware
4. Abra una nueva sesión de terminal.
5. Elimine el host. Consulte el comando de ejemplo que aparece a continuación como referencia.

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

Seguridad en Amazon Elastic VMware Service

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Amazon Elastic VMware Service (Amazon EVS), consulte Servicios de AWS Alcance by Compliance Program.
- Seguridad en la nube: su responsabilidad viene determinada por lo Servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Amazon EVS. Le muestra cómo configurar Amazon EVS para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayuden a supervisar y proteger sus recursos de Amazon EVS.

Contenido

Protección de datos en Amazon EVS

El modelo de responsabilidad AWS compartida se aplica a la protección de datos en Amazon Elastic VMware Service. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecuta toda la AWS nube. Usted es responsable de mantener el control sobre el contenido que se aloja en esta infraestructura, incluidos los componentes de VMware

Cloud Foundation (VCF). También eres responsable de las tareas de configuración y administración de la seguridad Servicios de AWS que utilices. Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener más información sobre la protección de datos en Europa, consulte la publicación de blog AWS Shared Responsibility Model and GDPR en el blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management. De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Úselo SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.

> **Note**
>
> Amazon EVS no registra la actividad de los usuarios que no sean AWS componentes, como la actividad dentro de su entorno de VCF. Estas actividades se registran en varias VMware consolas, como vSphere y NSX Manager. Si desea un registro centralizado del VCF, puede configurar soluciones de monitoreo del VCF, como VMware Aria Operations o VMware Tanzu Observability, para lograr este resultado. Para obtener más información, consulte VMware Cloud Foundation con VMware Tanzu y VMware Aria Suite Lifecyle en modo VMware Cloud Foundation en la documentación de VCF.

- Usa soluciones AWS de cifrado, junto con todos los controles de seguridad predeterminados. Servicios de AWS
- Utilice servicios de seguridad gestionados avanzados Amazon Macie, como los que ayudan a descubrir y proteger los datos confidenciales almacenados en ellos Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un terminal FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Le recomendamos encarecidamente que nunca coloque información de identificación confidencial, como las direcciones de correo electrónico de sus clientes, en etiquetas o campos de texto de formato libre, como un campo de nombre. Esto incluye cuando trabaja con Amazon EVS u otro dispositivo Servicios de AWS mediante la consola, la API o AWS SDKs. AWS CLI Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Amazon EVS implementa EC2 instancias i4i.metal que utilizan un cifrado AES-256 transparente de forma predeterminada para los datos almacenados en el volumen del almacén de instancias. Amazon EVS no admite el cifrado del volumen de arranque de EBS en este momento.

Volumen de arranque de Amazon EBS

Las instancias i4i.metal de Amazon EVS utilizan un volumen de arranque de Amazon EBS. El volumen de arranque contiene el sistema operativo y otros archivos necesarios para que la EC2 instancia arranque y se ejecute. El volumen de arranque no está cifrado. Amazon EVS no admite el cifrado del volumen de arranque en este momento. El volumen de arranque no contiene datos de usuario de sus máquinas virtuales.

Volumen de almacén de instancias

EC2 Las instancias Amazon EVS i4i.metal incluyen almacenamiento NVMe SSD local, que forma parte del hardware de la instancia. Amazon EVS utiliza volúmenes de almacenes de NVMe instancias como discos para los almacenes de datos de vSAN. El almacén de datos de vSAN almacena las máquinas virtuales de administración y carga de trabajo después de implementar el entorno Amazon EVS.

Los datos de los volúmenes del almacén de NVMe instancias se cifran mediante un cifrado XTS-AES-256, implementado en un módulo de hardware de la instancia. Las claves que se utilizan para cifrar los datos que se escriben en los dispositivos de almacenamiento conectados localmente NVMe son por cliente y por volumen. Para obtener más información, consulta Encriptación en reposo en la Guía del EC2 usuario de Amazon.

Tras implementar el entorno Amazon EVS, puede habilitar el cifrado de data-at-rest vSAN para todos los datos almacenados en el almacén de datos de vSAN, para las máquinas virtuales individuales

VMs () o para los archivos individuales que se encuentran en él. VMs Este control granular puede resultar útil cuando algunos VMs requieren cifrado y otros no, o cuando es necesario cifrar discos o archivos específicos de una máquina virtual. Para obtener más información, consulte Cómo funciona el Data-At-Rest cifrado de vSAN en la documentación de vSAN VMware .

Cifrado en tránsito

Amazon EVS no cifra el tráfico en tránsito de forma predeterminada. Para cifrar los datos en tránsito que atraviesan Amazon EVS, puede utilizar el cifrado de capa de aplicación con un protocolo como Transport Layer Security (TLS). Para obtener más información sobre el cifrado del tráfico de EC2 instancias, consulta Encryption in Transit en la Guía del EC2 usuario de Amazon.

> **Note**
>
> El cifrado de red Nitro no se aplica a las EC2 instancias que despliega Amazon EVS. Amazon EVS no admite el cifrado en tránsito del tráfico entre hosts.

Opciones de cifrado en tránsito para la conectividad local

Para cifrar el tráfico entre su centro de datos local y Amazon EVS, puede combinar el uso de Direct AWS Connect y AWS Site-To-Site VPN con Transit Gateway AWS . Esta combinación proporciona una conexión privada IPsec cifrada que también reduce los costes de red, aumenta el rendimiento del ancho de banda y proporciona una experiencia de red más uniforme que las conexiones VPN basadas en Internet. Para obtener más información, consulte AWS Site-to-Site VPN de IP privada con AWS Direct Connect.

> **Note**
>
> Amazon EVS no admite la conectividad a través de una interfaz virtual privada (VIF) de AWS Direct Connect ni a través de una conexión AWS Site-to-Site VPN que termine directamente en la VPC subyacente. Amazon EVS admite la terminación de IPSec VPN en la puerta de enlace de nivel 0 o 1 de NSX Edge. Para obtener más información, consulte Añadir un IPSec servicio VPN de NSX en la documentación de NSX. VMware

MAC Security (MACsec) es un estándar IEEE que proporciona confidencialidad, integridad y autenticidad del origen de los datos. Puede utilizar las conexiones de AWS Direct Connect que

MACsec permiten cifrar los datos desde el centro de datos corporativo a la ubicación de AWS Direct Connect. Para obtener más información, consulte Seguridad MAC en AWS Direct Connect en la Guía del usuario de AWS Direct Connect.

Cifrado en tránsito para datos VMware de red

Una vez implementado el entorno Amazon EVS, tiene varias opciones para aplicar el cifrado de los datos en tránsito en la capa VMware VCF:

- VMware Firewall distribuido vDefend: le permite implementar una segmentación de red detallada y aplicar el cifrado entre máquinas virtuales. TLS/SSL Para obtener más información, consulte Configurar los ajustes de seguridad del firewall distribuido mediante la interfaz de usuario en la documentación de VCF. VMware
- data-in-transitCifrado de vSAN: se puede utilizar para cifrar todos los datos y metadatos entre los hosts del clúster de vSAN. Para obtener más información, consulte Data-In-TransitCifrado de vSAN en la documentación de vSAN VMware .
- vSphere vMotion cifrado: protege la confidencialidad, integridad y autenticidad de los datos que se transfieren con vSphere vMotion. Para obtener más información, consulte Qué es vSphere vMotion cifrada en la documentación de vSphere.

Administración de claves y secretos

Durante la implementación del entorno Amazon EVS, Amazon EVS utiliza AWS Secrets Manager para crear, cifrar y almacenar los secretos que contienen las credenciales de VCF necesarias para instalar y acceder a los dispositivos de administración de VMware VCF, así como la contraseña raíz de ESX. Amazon EVS también elimina los secretos gestionados en su nombre cuando se elimina el entorno de EVS. Para obtener más información, consulte Qué hay en un secreto de Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Secrets Manager utiliza el cifrado de sobres con AWS KMS claves y claves de datos para proteger cada valor secreto. A menos que se especifique lo contrario, se utiliza la clave AWS gestionada predeterminada de Secrets Manager. Como alternativa, puede especificar una clave gestionada por el cliente durante la creación del entorno para cifrar sus secretos. Para obtener más información, consulte Cifrado y descifrado AWS secretos en Secrets Manager en la Guía del usuario de AWS Secrets Manager.

> **Note**
>
> Hay cargos de uso adicionales para las claves administradas por el cliente. La clave AWS gestionada predeterminada se proporciona sin coste alguno. Para obtener más información, consulte los precios en la Guía del usuario de AWS Secrets Manager.

Amazon EVS no sincroniza las credenciales entre AWS Secrets Manager y su software VCF después de la implementación. Usted es responsable de garantizar que los secretos asociados a su entorno de Amazon EVS se mantengan sincronizados con las credenciales de SDDC Manager para evitar que la contraseña de VCF caduque y se pierda el acceso al software de VCF.

Amazon EVS no divulga secretos en su nombre. Usted es responsable de divulgar los secretos asociados a su entorno. Te recomendamos encarecidamente que cambies tus datos secretos tan pronto como se cree el entorno e implementes un programa de rotación para actualizar tus datos secretos de forma periódica. Para obtener más información sobre la rotación de AWS los secretos de Secrets Manager, consulte Rotation by Lambda function en la Guía del usuario de AWS Secrets Manager. Para obtener más información sobre la administración de contraseñas de VCF, consulta la sección Administración de contraseñas en la documentación de VMware Cloud Foundation.

> **Important**
>
> Amazon EVS no sincroniza las credenciales entre AWS Secrets Manager y su software VCF después de la implementación. Si utiliza AWS Secrets Manager después de la implementación, debe mantener sincronizadas las credenciales entre AWS Secrets Manager y SDDC Manager para evitar problemas de caducidad de la contraseña de VCF. Puede perder el acceso al software VCF si las credenciales del SDDC Manager no se mantienen actualizadas.

> **Note**
>
> Amazon EVS no ofrece la rotación gestionada de secretos.

> **Note**
>
> El uso de una función de Lambda para la rotación de AWS secretos de Secrets Manager conlleva costes. Para obtener más información, consulte los precios en la Guía del usuario de AWS Secrets Manager.

Privacidad del tráfico entre redes

Amazon EVS utiliza una VPC proporcionada por el cliente para crear límites entre los recursos del entorno de Amazon EVS y controlar el tráfico entre ellos, la red local e Internet. Para obtener más información sobre la Amazon VPC seguridad, consulte Garantizar la privacidad del tráfico entre redes en la Guía del usuario. Amazon VPC Amazon VPC

De forma predeterminada, Amazon EVS crea subredes de VLAN privadas durante la creación del entorno que deniegan el acceso directo a Internet. Para añadir otro nivel de seguridad a la VPC, puede crear una lista de control de acceso a la red personalizada para la VPC con reglas que restrinjan aún más la conectividad a Internet. Para obtener más información, consulte Crear una ACL de red para su VPC en la Guía del usuario de Amazon VPC.

> **Important**
>
> EC2 los grupos de seguridad no funcionan en las interfaces de red elásticas que están conectadas a las subredes de VLAN de Amazon EVS. Para controlar el tráfico hacia y desde las subredes VLAN de Amazon EVS, debe usar una lista de control de acceso a la red.

Si es administrador de NSX, puede configurar las siguientes funciones de NSX para proteger el tráfico de red:

- VMware Firewall vDefend Gateway: protege el perímetro de la red y lo protege de amenazas externas (tráfico norte-sur). Para obtener más información, consulte Agregar una política y una regla de firewall de puerta de enlace en la VMware documentación de NSX.
- VMware Firewall distribuido vDefend: protege contra los ataques que se originan en una red interna (tráfico de este a oeste). Para obtener más información, consulte Agregar un firewall distribuido en la VMware documentación de NSX.

Administración de identidades y accesos para Amazon Elastic VMware Service

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAM los administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Amazon Elastic VMware Service (Amazon EVS). IAM es una Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Amazon EVS.

Usuario del servicio: si utiliza el servicio Amazon EVS para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de Amazon EVS para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador.

Si no puede acceder a una función de Amazon EVS, consultethe section called “Solución de problemas de identidad y acceso a Amazon EVS”.

Administrador de servicios: si está a cargo de los recursos de Amazon EVS en su empresa, probablemente tenga acceso total a Amazon EVS. Es su trabajo determinar a qué funciones y recursos de Amazon EVS deben acceder los usuarios del servicio. A continuación, debe enviar

solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Amazon EVS, consultethe section called "Cómo funciona Amazon EVS con IAM".

IAM administrador: si es IAM administrador, puede que le interese obtener más información sobre cómo redactar políticas para gestionar el acceso a Amazon EVS. Para ver ejemplos de políticas basadas en la identidad de Amazon EVS que puede utilizar, consulte. IAMthe section called "Ejemplos de políticas basadas en la identidad de Amazon EVS"

Autenticación con identidades

La autenticación es la forma de iniciar sesión para AWS usar sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario raíz de la AWS cuenta Usuario de IAM, o asumiendo un IAM rol.

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center (IAM Identity Center) los usuarios, la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal Consola de administración de AWS o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del usuario de AWS inicio de sesión.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte el proceso de firma de la versión 4 en la Referencia AWS general.

Independientemente del método de autenticación que utilice, es posible que también deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la Guía del usuario del AWS IAM Identity Center (sucesor del inicio de sesión AWS único) y Uso de la autenticación multifactorial (MFA) AWS en la Guía del usuario de IAM.

AWS usuario raíz de la cuenta

La primera vez que crea una Cuenta de AWS, comienza con una identidad de inicio de sesión única que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario raíz de la AWS cuenta y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja sus credenciales de usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía de referencia sobre administración de cuentas.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidad para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener información sobre el Centro de identidades de IAM, consulte ¿Qué es el Centro de identidades de IAM? en la guía del AWS usuario del IAM Identity Center (sucesor del AWS Single Sign-On).

Usuarios de IAM y grupos

Una Usuario de IAMes una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, te recomendamos Usuarios de IAM que utilices credenciales temporales en lugar de crearlas con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales de larga duración Usuarios de IAM, le recomendamos que rote las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un IAM grupo es una identidad que especifica una colección de Usuarios de IAM. No puede iniciar sesión como grupo. Puede usar grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un rol Usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

IAM roles

Un IAM rol es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos. Es similar a un Usuario de IAM, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el Consola de administración de AWS cambiando de rol. Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del usuario de IAM.

IAM los roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información sobre los conjuntos de permisos, consulte los conjuntos de permisos en la Guía del usuario del AWS IAM Identity Center (sucesor del AWS Single Sign-On).
- Usuario de IAM Permisos temporales: un usuario Usuario de IAM puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder el acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para

conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte En qué se diferencian las IAM funciones de las políticas basadas en recursos en la Guía del usuario de IAM.

- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones Amazon EC2 o almacene objetos en Amazon S3él. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a un servicio.
  - Permisos principales: cuando utilizas un rol Usuario de IAM o para realizar acciones en AWSél, se te considera principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones.
  - Función de servicio: una función de servicio es una IAM función que asume un servicio para realizar acciones en tu nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- Aplicaciones en ejecución Amazon EC2 : puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una Amazon EC2 instancia y que realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la Amazon EC2 instancia. Para asignar un AWS rol a una Amazon EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la Amazon EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a las aplicaciones que se ejecutan en Amazon EC2 instancias en la Guía del usuario de IAM.

Para saber si se deben usar IAM roles, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos de las políticas determinan si la solicitud está permitida o denegada. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

Todas las IAM entidades (usuarios o roles) comienzan sin permisos. De forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar su propia contraseña. Para conceder permiso a un usuario para hacer algo, el administrador debe asociar una política de permisos a un usuario. O bien el administrador puede agregar al usuario a un grupo que tenga los permisos necesarios. Cuando un administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

IAM las políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API Consola de administración de AWS AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en la identidad son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un Usuario de IAM rol o un grupo. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte Creación de políticas en la Guía IAM del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas integradas están integradas directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre

cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas de JSON que se adjuntan a un recurso, como un Amazon S3 bucket. Los administradores de servicios pueden utilizar estas políticas para definir qué acciones puede realizar una entidad principal especificada (miembro de cuenta, usuario o rol) en dicho recurso y bajo qué condiciones. Las políticas basadas en recursos son políticas insertadas. No existen políticas basadas en recursos que sean administradas.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) son un tipo de política que controla qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON. Amazon S3, AWS WAF, y Amazon VPC son ejemplos de servicios que admiten. ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (Usuario de IAM o función). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anula la autorización. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para IAM las entidades en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas.

El SCP limita los permisos de las entidades en las cuentas de los miembros, incluido cada usuario raíz de la AWS cuenta. Para obtener más información sobre Organizations SCPs, consulte la Guía del usuario de How SCPs work in the AWS Organizations.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon EVS con IAM

Antes de gestionar el acceso IAM a Amazon EVS, infórmese sobre IAM las funciones disponibles para su uso con Amazon EVS.

IAM función	Soporte de Amazon EVS
the section called “Políticas basadas en la identidad para Amazon EVS”	Sí
the section called “Políticas basadas en recursos en Amazon EVS”	No
the section called “Acciones políticas para Amazon EVS”	Sí
the section called “Recursos de políticas para Amazon EVS”	Parcial
the section called “Claves de condición de la política para Amazon EVS”	Sí

IAM función	Soporte de Amazon EVS
the section called “Listas de control de acceso (ACLs) en Amazon EVS”	No
the section called “Control de acceso basado en atributos (ABAC) con Amazon EVS”	Sí
the section called “Uso de credenciales temporales con Amazon EVS”	Sí
the section called “Sesiones de acceso directo para Amazon EVS”	Sí
the section called “Funciones de servicio para Amazon EVS”	No
the section called “Funciones vinculadas a servicios para Amazon EVS”	Sí

Para obtener una visión general de cómo funcionan Amazon EVS y otros IAM, consulte Servicios de AWS ese Servicios de AWS trabajo con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para Amazon EVS

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre todos los elementos que

se utilizan en una política de JSON, consulte la referencia sobre los elementos de la política de IAM JSON en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidad para Amazon EVS

Para ver ejemplos de políticas basadas en la identidad de Amazon EVS, consulte. the section called "Ejemplos de políticas basadas en la identidad de Amazon EVS"

Políticas basadas en recursos en Amazon EVS

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puedes especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para Amazon EVS

Soporta acciones Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una política IAM basada en la identidad describe la acción o las acciones específicas que la política permitirá o denegará. Las acciones políticas suelen tener el mismo nombre

que la operación de AWS API asociada. La acción se utiliza en una política para otorgar permisos para realizar la operación asociada.

Las acciones políticas en Amazon EVS utilizan el siguiente prefijo antes de la acción:. `evs:` Por ejemplo, para conceder permiso a alguien para crear un entorno con la operación de la `CreateEnvironment` API Amazon EVS, debes incluir la `evs:CreateEnvironment` acción en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Amazon EVS define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

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

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción:

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

Para ver una lista de las acciones de Amazon EVS, consulte Acciones definidas por Amazon EVS en la Referencia de autorización de servicio.

Recursos de políticas para Amazon EVS

Admite recursos de políticas: en forma parcial

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter asterisco (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Amazon EVS y sus tipos de recursos ARNs, consulte Recursos definidos por Amazon Elastic VMware Service en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon Elastic VMware Service.

Algunas acciones de la API de Amazon EVS admiten varios recursos. Por ejemplo, se puede hacer referencia a varios entornos al solicitar la acción de la `ListEnvironments` API. Para especificar varios recursos en una sola sentencia, sepárelos ARNs con comas.

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

Por ejemplo, el recurso del entorno Amazon EVS tiene el siguiente ARN:

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

Para especificar los entornos `my-environment-1` y `my-environment-2` en su declaración, utilice el siguiente ejemplo: 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 los entornos que pertenecen a una cuenta específica, utilice el comodín (*):

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

Claves de condición de la política para Amazon EVS

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Condition` elemento (o `Condition` bloque) permite especificar las condiciones en las que entra en vigor una declaración. El elemento `Condition` es opcional. Puedes crear expresiones

condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una sola clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un Usuario de IAM permiso para acceder a un recurso solo si está etiquetado con su Usuario de IAM nombre. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del usuario de IAM.

Amazon EVS define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Todas Amazon EC2 las acciones admiten las claves de `ec2:Region` condición `aws:RequestedRegion` y. Para obtener más información, consulte Ejemplo: restricción del acceso a una región específica.

Para ver una lista de claves de condición de Amazon EVS, consulte Claves de condición de Amazon EVS en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Amazon EVS.

Listas de control de acceso (ACLs) en Amazon EVS

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con Amazon EVS

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar

etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designe las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Puede adjuntar etiquetas a los recursos de Amazon EVS o pasarlas en una solicitud a Amazon EVS. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/<key-name>`, `aws:RequestTag/<key-name>` o `aws:TagKeys`. Para obtener más información sobre las acciones con las que puede utilizar etiquetas en las claves de condición, consulte Acciones definidas por Amazon EVS en la Referencia de autorización de servicio.

Uso de credenciales temporales con Amazon EVS

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas Consola de administración de AWS mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para Amazon EVS

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en él AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Funciones de servicio para Amazon EVS

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Funciones vinculadas a servicios para Amazon EVS

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la gestión de funciones vinculadas a los servicios de Amazon EVS, consulte. the section called “Cómo utilizar roles vinculados a servicios”

Ejemplos de políticas basadas en la identidad de Amazon EVS

De forma predeterminada, Usuarios de IAM los roles no tienen permiso para crear o modificar los recursos de Amazon EVS. Tampoco pueden realizar tareas mediante la AWS API Consola de administración de AWS AWS CLI, o. IAM El administrador debe crear IAM políticas que concedan permiso a los usuarios y roles para realizar operaciones de API específicas en los recursos específicos que necesitan. A continuación, el administrador debe adjuntar esas políticas a los Usuarios de IAM grupos que requieran esos permisos.

Para obtener información sobre cómo crear una política de IAM basada en la identidad utilizando estos ejemplos de documentos de política de JSON, consulte Creación de políticas mediante el editor de JSON en la Guía del usuario de IAM.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de Amazon EVS de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la Guía del usuario de IAM.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo

CloudFormation. Para obtener más información, consulte Elementos de la política de IAM JSON: condición en la Guía del usuario de IAM.

- Úselo IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y a las IAM mejores prácticas. IAM IAM Access Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación IAM Access Analyzer de políticas en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si se presenta una situación en la que se Usuarios de IAM requieren usuarios root en su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Uso de la consola Amazon EVS

Para acceder a la consola Amazon EVS, un director de IAM debe tener un conjunto mínimo de permisos. Estos permisos deben permitir al director enumerar y ver detalles sobre los recursos de Amazon EVS de su Cuenta de AWS propiedad. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades principales que tengan esa política adjunta.

Para garantizar que sus directores de IAM puedan seguir utilizando la consola de Amazon EVS, cree una política con su propio nombre único, como. `AmazonEVSAdminPolicy` Adjunte la política a las entidades principales. Para obtener más información, consulte Agregar de permisos a un usuario en la Guía del usuario de 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"
                }
            }
        }
    ]
}
```

No es necesario conceder permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la misma. AWS En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo se puede crear una política que Usuarios de IAM permita ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la AWS CLI API o. 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": "*"
        }
    ]
}
```

Cree y gestione un entorno Amazon EVS

Este ejemplo de política incluye los permisos necesarios para crear y eliminar un entorno de Amazon EVS y añadir o eliminar hosts una vez creado el entorno.

Puede sustituirlo por Región de AWS el entorno en el Región de AWS que desee crear un entorno. Si su cuenta ya tiene el rol `AWSServiceRoleForAmazonEVS`, puede quitar la acción `iam:CreateServiceLinkedRole` de la política. Si alguna vez ha creado un entorno de Amazon EVS en su cuenta, ya existe un rol con estos permisos, a menos que lo haya eliminado.

```
{
    "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": "*"
        }
    ]
}
```

Obtenga y enumere los entornos, hosts y VLANs

Este ejemplo de política incluye los permisos mínimos necesarios para que un administrador obtenga y publique todos los entornos y hosts de Amazon EVS y VLANs dentro de una cuenta determinada en el Región de AWS us-east-2.

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

Solución de problemas de identidad y acceso a Amazon EVS

Utilice la siguiente información para ayudarle a diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con Amazon EVS y IAM.

Temas

- AccessDeniedException
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon EVS

AccessDeniedException

Si recibes una `AccessDeniedException` al llamar a una operación de AWS API, significa que las credenciales principales de IAM que utilizas no tienen los permisos necesarios para realizar esa llamada.

```
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
```

En el mensaje de ejemplo anterior, el usuario no tiene permisos para llamar a la operación de la `CreateEnvironment` API de Amazon EVS. Para proporcionar permisos de administrador de Amazon EVS a un director de IAM, consulte. the section called “Ejemplos de políticas basadas en la identidad de Amazon EVS”

Para obtener más información general sobre IAM, consulte Controlar el acceso a AWS los recursos mediante políticas en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon EVS

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede utilizar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon EVS admite estas funciones, consultethe section called “Cómo funciona Amazon EVS con IAM”.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a uno Usuario de IAM en otro Cuenta de AWS que sea de su propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información acerca de cómo ofrecer acceso a la identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer la diferencia entre el uso de funciones y políticas basadas en recursos para el acceso entre cuentas, consulte En qué se diferencian las IAM funciones de las políticas basadas en recursos en la Guía del usuario de IAM.

AWS políticas gestionadas para Amazon EVS

Una política AWS gestionada es una política independiente creada y administrada por. AWS AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes. Para obtener más información, consulta las políticas AWS gestionadas en la Guía del IAM usuario.

AWS política gestionada: Amazon EVSService RolePolicy

No puede asociar `AmazonEVSServiceRolePolicy` a sus entidades IAM. Esta política se adjunta a una función vinculada al servicio que permite a Amazon EVS realizar acciones en su nombre. Para obtener más información, consulte the section called “Cómo utilizar roles vinculados a servicios”. Cuando crea un entorno con un director de IAM que tiene el `iam:CreateServiceLinkedRole` permiso, el rol `AWSServiceRoleforAmazonEVS` vinculado al servicio se crea automáticamente para usted con esta política adjunta.

Esta política permite que el rol `AWSServiceRoleForAmazonEVS` vinculado al servicio actúe en su nombre. Servicios de AWS

Detalles de los permisos

Esta política incluye los siguientes permisos que permiten a Amazon EVS completar las siguientes tareas.

- `ec2`- Descubra los componentes de red de VPC, incluidas las subredes y. VPCs Cree, modifique, etiquete y elimine las interfaces de red elásticas que se utilizan para establecer una conexión persistente entre Amazon EVS y el dispositivo SDDC Manager de VMware Virtual Cloud Foundation (VCF) en la subred de VPC. Esta conectividad es necesaria para que Amazon EVS despliegue, gestione y supervise la implementación de VCF.

- `ec2`- Elimine las instancias de EC2 que Amazon EVS crea al realizar una solicitud de eliminación de un host de EVS. Describa y modifique los atributos de la instancia de EC2 para que la protección por defecto de terminación y parada de la instancia de EC2 se pueda deshabilitar si es necesario para permitir la eliminación del host de EVS.
- `ec2`- Gestione los volúmenes de EBS para la instalación y limpieza de Cloud Builder. Durante la creación del entorno, Cloud Builder se instala en uno de los hosts implementados por Amazon EVS para realizar cambios en la configuración de VCF. Una vez finalizado, Amazon EVS elimina Cloud Builder separando y eliminando el volumen de EC2 en el que está almacenado.
- `ec2`- Elimine las subredes VLAN de EVS en su nombre si solicita la eliminación del entorno.
- `secretsmanager`- Elimine las contraseñas VCF que Amazon EVS crea y almacena en AWS Secrets Manager durante la creación del entorno. Amazon EVS elimina todos los secretos que el servicio crea en su cuenta si se produce un error en la creación del entorno o si usted solicita la eliminación del entorno. Recupere las credenciales de vCenter de AWS Secrets Manager al configurar un conector de vCenter proporcionando un ARN secreto. El permiso incluye una condición de etiqueta de recurso `EvsAccess=true` para garantizar que Amazon EVS solo acceda a los secretos etiquetados explícitamente para el acceso a Amazon EVS vCenter.
- `kms`- Descifre los secretos y describa las claves de KMS cuando las credenciales de vCenter almacenadas en Secrets Manager se cifran con claves de KMS. El permiso está sujeto a una condición de etiqueta de recurso `EvsAccess=true` para garantizar que Amazon EVS solo acceda a las claves de KMS etiquetadas explícitamente para el acceso a vCenter.
- `cloudwatch`- Publica métricas AWS de uso CloudWatch para los recursos de Amazon EVS que tengan cuotas.

Para ver más detalles sobre la política, incluida la última versión del documento de política de JSON, consulta Amazon EVSService RolePolicy en la Guía de referencia de políticas AWS gestionadas.

Amazon EVS actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon EVS desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial de revisión.

Cambio	Descripción	Fecha
Amazon EVSServiceRolePolicy : política actualizada	Amazon EVS actualizó la política para permitir que el servicio recupere las credenciales de vCenter de Secrets AWS Manager y descifre los secretos cifrados con claves de KMS. Para obtener más información, consulte the section called “AWS política gestionada: Amazon EVSService RolePolicy”.	23 de marzo de 2026
Amazon EVSServiceRolePolicy : política actualizada	Amazon EVS actualizó la política para añadir capacidades integrales de administración de recursos, incluida la administración de instancias EC2, las operaciones de volumen de EBS y la integración de AWS Secrets Manager. Para obtener más información, consulte the section called “AWS política gestionada: Amazon EVSService RolePolicy”.	14 de agosto de 2025
Amazon EVSServiceRolePolicy : política actualizada	Amazon EVS actualizó la política para permitir que el servicio elimine las subredes de VLAN de EVS y publique las métricas de uso de Amazon EVS en. CloudWatch Para obtener más información, consulte the section called	14 de julio de 2025

Cambio	Descripción	Fecha
	“AWS política gestionada: Amazon EVSService RolePolicy”.	
Amazon EVSService RolePolicy — Se ha añadido una nueva política	Amazon EVS agregó una nueva política que permite al servicio conectarse a una subred de VPC en la cuenta del cliente. Esta conexión es necesaria para que el servicio funcione. Para obtener más información, consulte the section called “AWS política gestionada: Amazon EVSService RolePolicy”.	09 de junio de 2025
Amazon EVS comenzó a rastrear los cambios	Amazon EVS comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	9 de junio de 2025

Uso de funciones vinculadas a servicios para Amazon EVS

Amazon Elastic VMware Service utiliza funciones AWS vinculadas al servicio Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon EVS. Amazon EVS predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración de Amazon EVS, ya que no es necesario añadir manualmente los permisos necesarios. Amazon EVS define los permisos de sus funciones vinculadas a servicios y, a menos que se defina lo contrario, solo Amazon EVS puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus recursos de Amazon EVS porque no puede retirar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Amazon EVS

Amazon EVS utiliza el rol vinculado al servicio denominado. `AWSServiceRoleForAmazonEVS` El rol permite a Amazon EVS gestionar los entornos de su cuenta. La política adjunta permite al rol administrar los siguientes recursos: interfaces de red elásticas de EVS, subredes de VLAN de EVS, hosts de EVS y métricas. VPCs CloudWatch

El rol vinculado al servicio `AWSServiceRoleForAmazonEVS` depende de los siguientes servicios para asumir el rol:

- `evs.amazonaws.com`

La política de permisos de roles permite a Amazon EVS realizar las siguientes acciones en los recursos especificados:

- AmazonEVSServiceRolePolicy

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Amazon EVS

No necesita crear un rol vinculado a servicios de manera manual. Cuando crea un entorno en la Consola de administración de AWS AWS CLI o la AWS API, Amazon EVS crea el rol vinculado al servicio automáticamente.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea un entorno, Amazon EVS vuelve a crear el rol vinculado al servicio para usted.

Edición de un rol vinculado a un servicio para Amazon EVS

Amazon EVS no le permite editar el rol vinculado al `AWSServiceRoleForAmazonEVS` servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para Amazon EVS

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol. Para ver los pasos para eliminar un entorno de Amazon EVS con hosts, consultethe section called “Eliminar los hosts y el entorno de Amazon EVS”.

> **Note**
>
> Si el servicio Amazon EVS utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Eliminar manualmente el rol vinculado al servicio

Utilice la consola de IAM, la AWS CLI o la AWS API para eliminar el rol vinculado al `AWSServiceRoleForAmazonEVS` servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para las funciones vinculadas al servicio de Amazon EVS

Amazon EVS admite el uso de funciones vinculadas a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte los puntos de enlace y las cuotas de Amazon Elastic VMware Service en la Guía de referencia AWS general.

Resiliencia en Amazon EVS

La infraestructura AWS global se basa Regiones de AWS en distintas zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que se conectan a través de redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Los entornos de Amazon EVS están disponibles en una única zona de AWS disponibilidad. Para garantizar la alta disponibilidad de la infraestructura Single-AZ de Amazon EVS, Amazon EVS ofrece las siguientes funciones:

> **Note**
>
> Por el momento, Amazon EVS solo admite implementaciones Single-AZ.

- Amazon EVS admite el uso de AWS Elastic Disaster Recovery para automatizar la copia de seguridad y la recuperación de sus datos.
- Amazon EVS implementa un clúster de Active/Standby NSX Edge con dos nodos de NSX Edge según los requisitos de VCF. Los nodos de NSX Edge se ejecutan en diferentes hosts para garantizar una alta disponibilidad y permitir una rápida conmutación por error en el raro caso de que un nodo de NSX Edge falle.
- Amazon EVS implementa un entorno mínimo de cuatro hosts ESX, que VCF requiere. Se pueden agregar hosts adicionales después de la implementación. Este es un requisito de VMware diseño para garantizar el quórum adecuado de vSAN y mantener la disponibilidad durante las operaciones de mantenimiento y los errores del host. Para obtener más información, consulte vSphere Cluster Design for VMware Cloud Foundation en la documentación de VMware Cloud Foundation.
- Amazon EVS admite el uso de un grupo de ubicación de EC2 particiones o un grupo de ubicación de clústeres para los EC2 hosts. El grupo de ubicación de particiones distribuye las EC2 instancias entre particiones lógicas, de modo que los grupos de instancias de una partición no comparten el hardware subyacente con grupos de instancias de particiones diferentes. Esta estrategia ayuda a reducir la probabilidad de que se produzcan fallos de hardware correlacionados en el caso de grandes cargas de trabajo distribuidas. Los grupos de ubicación de clústeres se utilizan para colocar EC2 las instancias en el mismo rack físico a fin de garantizar una baja latencia. Para

obtener más información, consulte los grupos de ubicación de particiones en la Guía del Amazon EC2 usuario.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

VMware resiliencia de los componentes

Los clientes de Amazon EVS son responsables de configurar los VMware componentes que se ejecutan en Amazon EVS para garantizar la alta disponibilidad de sus máquinas virtuales (VMs) y la resiliencia de la carga de trabajo.

Amazon EVS admite las siguientes funciones de resiliencia de VMware Cloud Foundation (VCF):

- vSphere Replication: proporciona una replicación asíncrona y basada en el host VMs para fines de recuperación ante desastres y migración de cargas de trabajo. Para obtener más información, consulte Cómo funciona vSphere Replication en la documentación de VMware vSphere Replication.
- Protección de datos de vSAN: le permite VMs recuperarse rápidamente de un fallo operativo provocado por ataques de ransomware mediante instantáneas nativas almacenadas localmente en el clúster de vSAN. Para obtener más información, consulte Uso de vSAN Data Protection en la documentación de vSAN.
- vSphere HA: proporciona una conmutación por error automática en caso de que se produzca un error VMs en el host. Para obtener más información, consulte Diseño de alta disponibilidad para vCenter Server for VMware Cloud Foundation en la documentación de VCF.
- vSphere Fault Tolerance (FT): proporciona disponibilidad continua para tareas críticas VMs mediante la creación y el mantenimiento de otra máquina virtual idéntica y disponible de forma continua para sustituirla en caso de una situación de conmutación por error. Para obtener más información, consulte Cómo funciona la tolerancia a errores en la documentación de vSphere.
- Error de tolerancia de vSAN (FTT): configuración de vSAN que determina cuántos errores de host puede soportar una máquina virtual antes de que quede inaccesible. Esto define el nivel de redundancia y tolerancia a errores de las máquinas virtuales del clúster de vSAN. Para obtener más información, consulte Tolerar errores adicionales con el dominio de errores en el clúster de vSAN en la documentación de vSAN.

Uso de Amazon EVS con otros servicios AWS

Amazon EVS está integrado con otros Servicios de AWS para ofrecer soluciones adicionales. En este tema se identifican algunos de los servicios con los que trabaja Amazon EVS para añadir funcionalidad.

Temas

- Cree recursos de Amazon EVS con AWS CloudFormation
- Ejecute cargas de trabajo de alto rendimiento con Amazon FSx for ONTAP NetApp

Cree recursos de Amazon EVS con AWS CloudFormation

Amazon EVS está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y gestionar sus recursos e infraestructura. Crea una plantilla que describe todos los AWS recursos que desea, por ejemplo, un entorno Amazon EVS, y AWS CloudFormation se encarga de aprovisionar y configurar esos recursos por usted.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los recursos de Amazon EVS de forma coherente y repetida. Simplemente describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varias Cuentas de AWS regiones.

Amazon EVS y plantillas AWS CloudFormation

Para aprovisionar y configurar recursos para Amazon EVS y los servicios relacionados, debe conocer AWS CloudFormation las plantillas. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus AWS CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulta ¿Qué es AWS CloudFormation Designer? en la Guía AWS CloudFormation del usuario.

Amazon EVS admite la creación de entornos en AWS CloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para sus entornos, consulte la referencia de tipos de recursos de Amazon EVS en la Guía del AWS CloudFormation usuario.

Obtenga más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario
- AWS CloudFormation Guía del usuario de la interfaz de línea de comandos

Ejecute cargas de trabajo de alto rendimiento con Amazon FSx for ONTAP NetApp

Amazon FSx for NetApp ONTAP es un servicio de almacenamiento que te permite lanzar y ejecutar sistemas de archivos ONTAP totalmente gestionados en la nube. ONTAP NetApp es la tecnología de sistema de archivos que proporciona un conjunto ampliamente adoptado de capacidades de acceso y gestión de datos. FSx for ONTAP ofrece las funciones, el rendimiento y APIs los sistemas de NetApp archivos locales con la agilidad, la escalabilidad y la sencillez de un servicio totalmente gestionado. AWS Para obtener más información, consulte la Guía del usuario de FSx ONTAP.

Amazon EVS admite el uso de Amazon FSx for NetApp ONTAP como NFS/iSCSI almacén de datos y como almacenamiento conectado como huésped para VMware máquinas virtuales que se ejecutan en Amazon EVS.

Configurar FSx NetApp ONTAP como almacén de datos NFS

El siguiente procedimiento detalla los pasos mínimos necesarios FSx para configurar NetApp ONTAP como almacén de datos de NFS para Amazon EVS mediante la FSx consola y la interfaz de cliente de VMware vSphere que se ejecuta en Amazon EVS.

Requisitos previos

Antes de utilizar Amazon EVS con Amazon FSx for NetApp ONTAP, asegúrese de haber completado las siguientes tareas previas.

- Se implementa un entorno de Amazon EVS en su Virtual Private Cloud (VPC). Para obtener más información, consulte Introducción.
- Tiene acceso a su cliente vSphere que se ejecuta en Amazon EVS.
- Usted o su administrador de almacenamiento deben tener los permisos necesarios para crear y administrar FSx los sistemas de archivos ONTAP en su VPC. Para obtener más información, consulte Gestión de identidad y acceso para Amazon FSx for NetApp ONTAP.

Su director de IAM tiene los permisos adecuados para crear y gestionar FSx los sistemas de archivos de ONTAP en su VPC. Para obtener más información, consulte the section called “Cree y gestione un entorno Amazon EVS”.

Cree un sistema de archivos FSx para ONTAP NetApp

1. Ve a la FSx consola de Amazon.
2. Seleccione Crear sistema de archivos.
3. Selecciona Amazon FSx para NetApp ONTAP.
4. Elija Siguiente.
5. Selecciona Creación estándar.
6. Para el tipo de implementación, seleccione una opción de implementación Single-AZ.

> **Note**
>
> Por el momento, Amazon EVS solo admite despliegues Single-AZ.

7. Para la capacidad de almacenamiento SSD, especifique 1024 GiB.
8. En Capacidad de rendimiento, elija Especificar capacidad de rendimiento. Elija al menos 512 MB/s para Single-AZ 1 o al menos 768 MB/s para Single-AZ 2.
9. Seleccione la VPC de Amazon EVS que tenga conectividad con las subredes de VLAN de Amazon EVS.
10. Seleccione un grupo de seguridad que permita todo el tráfico NFS necesario FSx para ONTAP a la subred de VLAN de VMkernel administración de hosts de Amazon EVS.
11. Seleccione la subred de acceso al servicio Amazon EVS en la que se implementará el sistema de archivos. Para obtener más información, consulte the section called “Subred de acceso a servicios”.
12. En Ruta de cruce, especifique un nombre significativo `/vol1` para identificar este volumen en vSphere.
13. En la configuración de volumen predeterminada, establezca la eficiencia del almacenamiento en Habilitada.
14. Deje el resto de los ajustes en sus valores predeterminados y seleccione Siguiente.
15. Revise los atributos del sistema de archivos y elija Crear sistema de archivos.

Recupere el nombre DNS de NFS de la máquina virtual de almacenamiento

1. Ve a la FSx consola de Amazon.
2. En el menú de la izquierda, selecciona Sistemas de archivos.
3. Elige el sistema de archivos recién creado.
4. Seleccione la pestaña Máquinas virtuales de almacenamiento.
5. Elija la máquina virtual de almacenamiento.
6. Seleccione la pestaña Endpoints.
7. Copie el nombre DNS del sistema de archivos de red (NFS) para usarlo más adelante en VMware Vsphere.

Cree un almacén de datos NFS en vSphere mediante el volumen for ONTAP FSx

Siga las instrucciones de Crear un almacén de datos NFS en el entorno de vSphere para configurar Amazon FSx for NetApp ONTAP como almacenamiento externo para vSphere. VMware Para la configuración del servidor en la interfaz de cliente de vSphere, utilice el nombre DNS NFS de la máquina virtual de almacenamiento (SVM) que copió en el paso anterior.

Configurar FSx NetApp ONTAP FSx como almacén de datos iSCSI

El siguiente procedimiento detalla los pasos mínimos necesarios para configurar NetApp ONTAP como almacén de datos iSCSI FSx para Amazon EVS mediante la consola VMware y FSx la interfaz de cliente de vSphere que se ejecuta en Amazon EVS.

Requisitos previos

Antes de utilizar Amazon EVS con Amazon FSx for NetApp ONTAP, asegúrese de haber completado las siguientes tareas previas.

- Se implementa un entorno de Amazon EVS en su Virtual Private Cloud (VPC). Para obtener más información, consulte Introducción.
- Tiene acceso a su cliente vSphere que se ejecuta en Amazon EVS.
- Usted o su administrador de almacenamiento deben tener los permisos necesarios para crear y administrar FSx los sistemas de archivos ONTAP en su VPC. Para obtener más información, consulte Gestión de identidad y acceso para Amazon FSx for NetApp ONTAP.

Cree un sistema de FSx archivos para NetApp ONTAP

1. Ve a la FSx consola de Amazon.
2. Seleccione Crear sistema de archivos.
3. Selecciona Amazon FSx para NetApp ONTAP.
4. Elija Siguiente.
5. Selecciona Creación estándar.
6. Para el tipo de implementación, seleccione una opción de implementación Single-AZ.

> **Note**
>
> Por el momento, Amazon EVS solo admite despliegues Single-AZ.

7. Para la capacidad de almacenamiento SSD, especifique 1024 GiB.
8. En Capacidad de rendimiento, elija Especificar capacidad de rendimiento. Elija al menos 512 MB/s para Single-AZ 1 o al menos 768 MB/s para Single-AZ 2.
9. Seleccione la VPC de Amazon EVS que tenga conectividad con las subredes de VLAN de Amazon EVS.
10. Seleccione un grupo de seguridad que permita todo el tráfico iSCSI FSx de ONTAP necesario a la subred de VLAN de administración de VMkernel hosts de Amazon EVS.
11. Seleccione la subred de acceso al servicio Amazon EVS en la que se implementará el sistema de archivos. Para obtener más información, consulte the section called “Subred de acceso a servicios”.
12. En la configuración de volumen predeterminada, establezca la eficiencia del almacenamiento en Habilitada.
13. Deje el resto de los ajustes en sus valores predeterminados y seleccione Siguiente.
14. Revise los atributos del sistema de archivos y elija Crear sistema de archivos.

Configurar un adaptador iSCSI de software en vSphere para el almacenamiento en host ESX

Para cada host ESX, debe configurar el adaptador iSCSI de software para que los hosts ESX puedan usarlo para acceder al almacenamiento iSCSI. Para obtener instrucciones sobre cómo configurar el

adaptador iSCSI de software para los hosts ESX en vSphere, consulte Agregar o quitar el adaptador iSCSI de software en la documentación del producto vSphere. VMware

Después de configurar el adaptador iSCSI de software, copie el nombre cualificado de iSCSI (IQN) asociado a un adaptador iSCSI. Estos valores se utilizarán más adelante.

Creación de un LUN iSCSI

FSx para ONTAP le permite crear números de unidad lógica (LUNs) diseñados específicamente para el acceso iSCSI, lo que proporciona almacenamiento en bloques compartido a sus hosts ESX. Utilice la CLI de NetApp ONTAP para crear un LUN.

A continuación se muestra un ejemplo de comando.

> **Note**
>
> Se recomienda configurar el tamaño del LUN al 90% del tamaño del volumen.

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

Para obtener más información, consulte Creación de un LUN iSCSI en la Guía del usuario de FSx ONTAP.

Configurar y asignar un grupo de iniciadores al LUN iSCSI

Ahora que ha creado un LUN iSCSI, el siguiente paso del proceso consiste en crear un grupo de iniciadores (`igroup`) para conectar el volumen al clúster y asignar el LUN al grupo de iniciadores. Utilice la CLI de NetApp ONTAP para realizar estas acciones.

1. Configure el grupo de iniciadores.

   A continuación se muestra un ejemplo de comando. Para `--initiator` ello, utilice el adaptador iSCSI IQNs que copió en el paso 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 que `igroup` existe.

```
lun igroup show
```

3. Asigne el LUN al grupo iniciador. A continuación, se muestra un comando de ejemplo.

```
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. Utilice el `lun show -path` comando para confirmar que el LUN está creado, conectado y mapeado.

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

Para obtener más información, consulte Aprovisionamiento de iSCSI para Linux o Aprovisionamiento de iSCSI para Windows en FSx la Guía del usuario de ONTAP.

Configurar la detección dinámica del LUN iSCSI en vSphere

Para permitir que los hosts ESX vean el LUN iSCSI, debe configurar la detección dinámica para cada host de la interfaz de cliente de vSphere. En el campo del servidor iSCSI, introduzca el nombre DNS (NFS) que copió en el paso anterior. Para obtener más información, consulte Configurar la detección dinámica o estática para iSCSI e iSER en un host ESX en la documentación del producto vSphere VMware .

Cree un almacén de datos de VMFS en VMware vSphere mediante el LUN iSCSI

Los almacenes de datos del Sistema de archivos de máquinas virtuales (VMFS) sirven como repositorios para las máquinas virtuales. VMware Siga las instrucciones de Crear un almacén de datos de VMFS de vSphere para configurar el almacén de datos de VMFS en vSphere mediante el LUN iSCSI que configuró VMware anteriormente.

Resolución de problemas

En este capítulo se detallan algunos problemas comunes que se presentan al crear o administrar entornos de Amazon EVS.

Solucione problemas con las comprobaciones de estado del entorno que no

Amazon EVS realiza comprobaciones automatizadas en el entorno para identificar problemas. Puede ver el estado del entorno para identificar problemas específicos y detectables.

Revise la información de verificación del estado del entorno

Para investigar entornos deteriorados mediante la consola Amazon EVS

1. Abra la consola Amazon EVS.
2. En el panel de navegación, elija Entornos y, a continuación, seleccione su entorno.
3. Seleccione la pestaña Detalles para ver una descripción general del entorno.
4. Compruebe el estado del entorno. Pase el ratón sobre este campo para ampliar una ventana emergente con los resultados individuales de cada comprobación del estado del entorno.

Falló la comprobación de accesibilidad

La comprobación de accesibilidad verifica que Amazon EVS tenga una conexión persistente con SDDC Manager. Si Amazon EVS no puede llegar al entorno, se produce un error en esta comprobación.

Si esta comprobación produce un error, Amazon EVS ya no podrá comunicarse con SDDC Manager para validar el estado del entorno y ya no se podrán agregar hosts al entorno. Un error de accesibilidad también provocará que las comprobaciones de reutilización y cobertura de claves de licencia produzcan un error, y que la comprobación del recuento de hosts devuelva una respuesta desconocida.

Para garantizar la accesibilidad, compruebe lo siguiente:

- Asegúrese de que los certificados sean válidos y no hayan caducado. Puede usar la interfaz de usuario de SDDC Manager o el cliente de vSphere para administrar los certificados en un entorno

de VCF. Tras la implementación, se recomienda reemplazar todos los certificados del dominio de administración de VMware Cloud Foundation. Para obtener más información, consulta Cómo administrar los certificados en VMware Cloud Foundation en la documentación de VMware Cloud Foundation.

- Asegúrese de que se pueda acceder a sus servidores DNS desde la subred de acceso al servicio, que los registros DNS sean válidos y que no existan nombres de host o direcciones IP duplicados.
- Si desea crear sus propias reglas de firewall, siga estas instrucciones:
  - Permita el TCP/UDP acceso a los servidores DNS.
  - Permita el HTTPS/SSH acceso a la subred de VLAN de administración del host.
  - Permita el HTTPS/SSH acceso a la subred VLAN de la máquina virtual de administración.

Si sigues sin poder resolver el problema después de seguir estas instrucciones, te recomendamos que te pongas en contacto con AWS Support para obtener más ayuda.

Falló la comprobación del recuento de hosts

Esta comprobación verifica que su entorno tenga un mínimo de cuatro hosts, lo cual es un requisito para VCF 5.2.x.

Si esta comprobación produce un error, tendrá que agregar hosts para que el entorno cumpla con este requisito mínimo. Amazon EVS solo admite entornos con 4 a 16 hosts.

Falló la comprobación de reutilización de claves

Esta comprobación verifica que la clave de licencia de VCF no esté siendo utilizada por otro entorno de Amazon EVS. Las licencias de VCF solo se pueden usar para un entorno de Amazon EVS. Esta comprobación no se realiza correctamente si proporciona claves de licencia de VCF en una solicitud de creación de entornos que ya están siendo utilizadas por otro entorno.

Si esta comprobación produce un error, recibirá una respuesta de error indicando que no se pudo crear el entorno de Amazon EVS. Para solucionar el problema, revise la configuración de las licencias en SDDC Manager y reemplace las licencias utilizadas anteriormente por licencias no utilizadas.

> **Important**
>
> Utilice la interfaz de usuario de SDDC Manager para gestionar la solución VCF y las claves de licencia de vSAN. Amazon EVS requiere que mantenga claves de licencia de vSAN y de

solución VCF válidas en SDDC Manager para que el servicio funcione correctamente. Si bien las claves se deben asignar a los hosts y al clúster de vSAN mediante vSphere Client, debe asegurarse de que esas claves también aparezcan en la pantalla de licencias de la interfaz de usuario del SDDC Manager.

No se pudo comprobar la cobertura de las claves

Esta comprobación verifica que la clave de licencia de VCF asignada a vCenter Server asigne suficientes núcleos de vCPU y capacidad de almacenamiento (TiB) de vSAN para todos los hosts implementados.

Si esta comprobación produce un error, recibirá una respuesta de error indicando que no se pudo crear el entorno de Amazon EVS. La falta de cobertura de claves puede indicar uno de los siguientes problemas:

- Las licencias de VCF no están asignadas correctamente a vCenter Server. Debe asignar una licencia a vCenter Server antes de que caduque su periodo de evaluación o antes de que caduque la licencia actualmente asignada. Si este es el problema, revise las asignaciones de licencias en SDDC Manager.
- Las licencias de VCF actuales no cubren las necesidades de núcleo de vCPU ni de capacidad de almacenamiento de vSAN. La clave de solución de VCF debe tener al menos 256 núcleos. La clave de licencia de vSAN debe tener al menos 110 TiB de capacidad de vSAN. Si este es el problema, agregue licencias de vSAN en SDDC Manager hasta satisfacer sus necesidades de uso.

Si las acciones anteriores no resuelven el problema, ponte en contacto con AWS Support para obtener más ayuda.

Important

Utilice la interfaz de usuario de SDDC Manager para gestionar la solución VCF y las claves de licencia de vSAN. Amazon EVS requiere que mantenga claves de licencia de vSAN y de solución VCF válidas en SDDC Manager para que el servicio funcione correctamente. Si bien las claves se deben asignar a los hosts y al clúster de vSAN mediante vSphere Client, debe asegurarse de que esas claves también aparezcan en la pantalla de licencias de la interfaz de usuario del SDDC Manager.

El agente de vSphere HA en este host no pudo acceder a la dirección de aislamiento

En la interfaz de usuario de vCenter, con el host ESX seleccionado, aparece el mensaje «El agente de vSphere HA en este host no pudo alcanzar la dirección de aislamiento < dirección>». IPv6

Este mensaje de error indica que el agente de vSphere HA de un host no puede alcanzar la dirección de IPv6 aislamiento predeterminada que vSphere HA utiliza para las comprobaciones de latidos. El mensaje de error no indica un problema y solo se produce porque Amazon EVS no es compatible IPv6 en este momento. La ausencia de IPV6 soporte para Amazon EVS no afecta a la funcionalidad principal de vSphere HA.

Las comprobaciones previas de actualización de vSAN fallan en el clúster de hosts ESX

Al intentar actualizar el clúster de hosts de ESX mediante SDDC Manager, es posible que no se realicen las comprobaciones previas relacionadas con el disco de vSAN. Esto se debe a que Amazon EVS utiliza la arquitectura de almacenamiento vSAN Express (ESA) y las comprobaciones previas de actualización no se aplican a vSAN ESA. Para obtener más información, consulte el artículo de la base de conocimiento de Broadcom sobre este tema.

Error al agregar el host debido a una imagen de clúster incompatible

Problema

Cuando agrega un host a su entorno, el host tiene la última versión disponible del complemento personalizado del proveedor de EVS. Si su entorno utiliza hosts con una versión complementaria anterior, se produce un error al agregar nuevos hosts y se produce un error que indica que el nuevo host no es compatible con la imagen de clúster. Para solucionar este problema, debe usar vSphere Lifecyle Manager para extraer la última versión del complemento disponible del host recién agregado.

Solución

Siga estos pasos.

1. Vaya al inventario de hosts y clústeres en VMware vCenter Server.

2. Extraiga el complemento del host recién agregado mediante la creación de un clúster vacío temporal.
3. En Conceptos básicos, seleccione Importar imagen desde un host existente en el inventario de vCenter y cree el clúster. Deje todas las demás configuraciones como predeterminadas.
4. Una vez creado este clúster temporal con la imagen extraída, puede eliminar el clúster temporal. El complemento ahora estará disponible en su almacén de vSphere Lifecycle Manager.
5. Vaya al clúster de su entorno y seleccione la pestaña Actualizaciones.
6. Edite la imagen del clúster y cambie la versión del complemento por la versión recién extraída.
7. Seleccione Save.
8. En el administrador del SDDC, vuelva a intentar la tarea fallida de agregar el host. Esto solucionará los hosts del clúster y actualizará todos los hosts a la última versión complementaria. La corrección de la imagen del clúster requerirá que se reinicie el host.

El administrador del SDDC no pasa la validación del host VCF durante la puesta en servicio del host

Problema

Si ha actualizado su versión de ESX después de la implementación del entorno Amazon EVS, es posible que el administrador del SDDC no funcione durante la validación del host de VCF en la etapa de comisionar los anfitriones. Para solucionar este problema, tendrá que usar vSphere Lifecyle Manager para actualizar ESX en el host recién agregado.

Solución

Siga estos pasos.

> **Important**
>
> Estos pasos requieren agregar temporalmente el host a vCenter fuera de SDDC Manager. El uso de vSphere Lifecyle Manager para cualquier operación distinta de las actualizaciones de ESX puede inutilizar el host y requerir que elimine y cree un nuevo host de Amazon EVS.

1. Vaya al inventario de hosts y clústeres en VMware vCenter Server.

2. Agregue el host temporalmente a su centro de datos virtual y asegúrese de seleccionar administrar el host con una imagen. El host se eliminará en un paso posterior, una vez completada la actualización de ESX. Para obtener más información, consulte Cómo agregar un host a su carpeta o centro de datos de vSphere en la documentación de vSphere.
3. Una vez que se haya agregado el host a vSphere, actualice la versión de ESX en el host. Esto se puede hacer en la pestaña Actualizaciones de su host. Edite la imagen del host para que coincida con la versión ESX de su clúster.
4. Una vez completada la actualización, elimine el host del inventario de vCenter. Para obtener más información, consulte Cómo eliminar un host ESX de la instancia de vCenter Server en la documentación de vSphere.
5. Instale su host en el administrador de SDDC. Para obtener más información, consulta la documentación de Commission Hosts en VMware Cloud Foundation.
6. Una vez que se haya puesto en marcha el host, agréguelo a su clúster mediante SDDC Manager.

Registro de llamadas a la API de Amazon EVS mediante AWS CloudTrail

Amazon EVS está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario de IAM, un rol de IAM o un servicio AWS en Amazon EVS. CloudTrail captura todas las llamadas a la AWS API de Amazon EVS como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Amazon EVS y llamadas en código a las operaciones de la API de Amazon EVS. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon EVS. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon EVS, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía del AWS CloudTrail usuario.

> **Note**
>
> Amazon EVS no registra la actividad de los usuarios que no sean AWS componentes, como la actividad dentro de su entorno de VCF. Estas actividades se registran en varias VMware consolas, como vSphere y NSX Manager.
> Si desea un registro de VCF centralizado, puede configurar soluciones de supervisión de VCF, como VMware Cloud Foundation Operations, para lograr este resultado.

Información sobre Amazon EVS en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en Amazon EVS, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su AWS cuenta. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de Amazon EVS, cree una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a

todas AWS las regiones. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones
- Recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de Amazon EVS se registran CloudTrail y se documentan en la referencia de la API de Amazon EVS. Por ejemplo, las llamadas a `GetEnvironment` y `DeleteEnvironment` las acciones generan entradas en los archivos de CloudTrail registro. `CreateEnvironment`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o de AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de registro de Amazon EVS

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Cuotas de servicio de Amazon EVS

Amazon EVS se ha integrado con Service Quotas, y puede utilizarla para ver y gestionar sus cuotas desde una ubicación central. Servicio de AWS Para obtener más información, consulte ¿Qué son las Service Quotas? en la Guía del usuario de Service Quotas.

Con la integración de Service Quotas, puedes usar Consola de administración de AWS o AWS CLI para buscar el valor de tus cuotas de Amazon EVS y solicitar un aumento de cuota para las cuotas ajustables. Para obtener más información, consulte Solicitar un aumento de cuota en la Guía del usuario de Service Quotas y request-service-quota-increaseen la Referencia de AWS CLI comandos.

Para obtener más información sobre las cuotas de servicio de Amazon EVS, consulte las cuotas de Amazon EVS en la Guía de referencia AWS general.

Important

Asegúrese de que su cuota de instancias estándar en EC2 ejecución bajo demanda refleje la cantidad de v CPUs que necesita para todas las EC2 instancias que utilizará en Amazon EVS. Cada instancia de i4i.metal utiliza 128 v. CPUs Para obtener información sobre cómo aumentar las cuotas de EC2 servicio, consulta Solicitar un aumento en la Guía del EC2 usuario de Amazon.

Note

Si planea utilizar hosts EC2 dedicados para su entorno de Amazon EVS, asegúrese de que su cuota de hosts i4i EC2 dedicados refleje el número de hosts dedicados que pretende utilizar en la región deseada. Para obtener información sobre cómo aumentar las cuotas de EC2 servicio, consulta Solicitar un aumento en la Guía del EC2 usuario de Amazon.

Note

Si configuras la conectividad a Internet de HCX, tu cuota de IPAM para la longitud de la máscara de red de bloques IPv4 CIDR públicos contiguos proporcionada por Amazon debe ser de /28 o superior. Para obtener más información, consulta Cuotas de tu IPAM.

> **Note**
>
> Amazon CloudWatch recopila métricas AWS de uso de los recursos de Amazon EVS que tienen cuotas (entorno y hosts). Para obtener más información, consulta las métricas CloudWatch de uso en la Guía del CloudWatch usuario de Amazon.

Consulte las cuotas de servicio de Amazon EVS en la Consola de administración de AWS

1. Abra la consola de Service Quotas.
2. En el panel de navegación izquierdo, seleccione AWS servicios.
3. En la lista de AWS servicios, busca y selecciona Amazon Elastic VMware Service.
4. Elija Visualización de las cuotas.

   En la lista de cuotas de servicio, puede ver el nombre de la cuota de servicio, el valor aplicado (si está disponible), la cuota AWS predeterminada y si el valor de la cuota es ajustable.
5. Para ver información adicional sobre una cuota de servicio, como, por ejemplo, la descripción, elija el nombre de cuota.
6. (Opcional) Para solicitar un aumento de cuota, selecciona la cuota que deseas aumentar, selecciona Solicitar aumento a nivel de cuenta, introduce o selecciona la información requerida y selecciona Solicitar.

Para trabajar más con las cuotas de servicio mediante el Consola de administración de AWS, consulte la Guía del usuario de Service Quotas. Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas.

Consulte las cuotas de servicio de Amazon EVS con la CLI AWS

Ejecuta el siguiente comando para ver tus cuotas de 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**
>
> La cuota devuelta es la cantidad de entornos o hosts de Amazon EVS que se pueden crear en esta cuenta en la AWS región actual.

Para trabajar más con las cuotas de servicio mediante la AWS CLI, consulte service-quota en la Referencia de comandos de la AWS CLI. Para solicitar un aumento de cuota, consulte el request-service-quota-increasecomando en la Referencia de comandos de la AWS CLI.

Historial de documentos de la Guía del usuario VMware de Amazon Elastic Service

En la siguiente tabla se describen las versiones de documentación de Amazon Elastic VMware Service.

Cambio	Descripción	Fecha
Amazon actualizado EVSService RolePolicy	Amazon EVS ha actualizado la política gestionada `AmazonEVSServiceRolePolicy` para permitir que el servicio recupere las credenciales de vCenter de Secrets AWS Manager y descifre los secretos cifrados con claves de KMS administradas por el cliente.	23 de marzo de 2026
Amazon actualizado EVSService RolePolicy	Amazon EVS ha actualizado la política gestionada `AmazonEVSServiceRolePolicy` para añadir funciones integrales de administración de recursos, incluida la gestión de instancias EC2, las operaciones de volumen de EBS y la integración de AWS Secrets Manager. Para obtener más información, consulte las actualizaciones de Amazon EVS a las políticas AWS gestionadas.	14 de agosto de 2025

Amazon actualizado EVSService RolePolicy	Se actualizó la política AWS gestionada de Amazon EVSServiceRolePolicy.	4 de agosto de 2025
Publicó la cuota de recuento de entornos por AWS cuenta	Amazon EVS publicó el recuento de entornos por cuota de AWS cuenta. La cuota de recuento de entornos por AWS cuenta representa el número máximo de entornos de Amazon EVS que se pueden crear en una cuenta y región determinadas.	8 de julio de 2025
Amazon EVS lanzado en la región de Europa (Irlanda)	Amazon EVS se lanzó en la región de Europa (Irlanda).	18 de junio de 2025
Lanzado Amazon EVSService RolePolicy	EVSServiceRolePolicy Se publicó la política AWS gestionada Amazon.	9 de junio de 2025
Versión inicial de la guía del usuario	Se publicó la guía del usuario de Amazon Elastic VMware Service. La guía del usuario de Amazon EVS describe todos los conceptos de Amazon EVS y proporciona instrucciones sobre el uso de las distintas funciones tanto con la consola como con la interfaz de línea de comandos.	9 de junio de 2025

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.